Major Management Challenges Facing the Department of Homeland Security (DHS) March 2003

Over the course of the first few weeks of DHS' existence, I spent a significant percentage of my time meeting with those offices of Inspector General (OIG) and General Accounting Office (GAO) officials, who oversaw departments or parts thereof that are now incorporated into DHS. Each of them has detailed the applicable component's top management challenges and other significant issues relating to the effectiveness, efficiency, and/or economy of the components' respective programs and operations. Following, based largely on those inputs, is a consolidated list of management challenges. These challenges will be used in setting DHS OIG's own priorities for audits and inspections or evaluations of DHS programs and operations. In addition, to the extent there are relevant recommendations from "legacy" OIGs relating to such challenges, we will undertake to track compliance for them.

ESTABLISHING THE DEPARTMENT OF HOMELAND SECURITY

Perhaps the biggest challenge facing DHS is integrating 22 separate components into a single, effective department. Appropriate plans (including workforce plans), goals, objectives and meaningful performance measures must be established as soon as possible to guide that process and track progress. Complicating the process is the fact that some of the more important components were already undergoing transformation. For example, prior to 9/11, homeland security related matters consumed 14% of the Coast Guard's resources. After 9/11, that percentage rose to 58%. Congress has expressed a concern as to whether, with the transfer of the Coast Guard from the Department of Transportation (DOT) to DHS, its non-homeland security related missions (marine environmental protection, fisheries enforcement, aids to navigation, and illegal drug and migrant interdiction) will be neglected. DHS OIG is required to conduct an annual review of the Coast Guard, with a particularly focus on whether the Coast Guard is meeting such missions.

Further, combining these entities will present opportunities for integrating systems and operations for greater economy and efficiency. For example, DOT OIG recommended that DHS take advantage of the economies of scale that can come from combining the Transportation Security Administration (TSA), the Immigration and Naturalization Service (INS), and the Customs Service. Administrative services, such as contracting, budgeting, legal, human resources, and internal affairs, should be consolidated. Likewise, airport space requirements for functions like office space, break rooms, training facilities, and detention cells should be consolidated. Finally, TSA should work with other DHS agencies, the airports, and other federal, state, and local law enforcement agencies before expanding its law enforcement duties (such as the current proposal for extending the federal air marshal program to conducting surveillance and patrolling at airports).

CONTRACT AND GRANTS MANAGEMENT

Contract Management

DHS will be integrating the procurement functions of many constituent programs and component missions, some lacking important management controls. For example, as reported by GAO, Customs has not begun to establish process controls for determining whether acquired software products and services satisfy contract requirements before acceptance, nor to establish related controls for effective and efficient transfer of acquired software products to the support organization responsible for software maintenance. At TSA, where contracts totaled $8.5 billion at the end of calendar year 2002, the DOT OIG found that procurements were made in an environment where there was no pre-existing infrastructure for overseeing contracts. TSA had to rely extensively on contractors to support its mission, leading to tremendous growth in contract costs. A recent review by TSA of one subcontractor found that, out of $18 million in expenses, between $6 million and $9 million appeared to be attributed to wasteful and abusive spending practices.

Also, some agencies have large, complex, high-cost procurement programs under way that need to be closely managed. For example, Customs' Automated Commercial Environment (ACE) project will cost $5 billion, and Coast Guard's Deepwater Capability Replacement Project will cost $17 billion and take two to three decades to complete. This $17 billion, multi-year project to upgrade the Coast Guard's fleet of ships, aircraft and communication systems for use far off shore in an integrated package was planned before 9/11, but no changes were made in project requirements after 9/11 and before awarding the contract in June of last year. DOT OIG has argued that post 9/11 changes in the Coast Guard's mission requirements argue for re-evaluating aspects of the project (for example, whether to arm more of its helicopters, whether to add more secure information handling capability, and ensuring that its systems can communicate with other DHS systems). Any such re-evaluation should be done sooner rather than later, especially now that the DHS Act has passed, requiring that consideration be given to accelerating the timetable for Deepwater from 20-25 years to 10. In addition to re-evaluating requirements, the Coast Guard should stabilize and prioritize the requirements, lest Deepwater investments crowd out other needed investments (plugging gaps in Rescue 21, the 911 system for mariners in distress, modernizing aids to navigation, rehabilitating aged buildings, piers, and other shore facilities, and replacing boats used close to shore).

On its $1 billion IT infrastructure project, TSA did not issue a statement of work detailing its requirements. Instead, it asked vendors to bid based on a "statement of objective" containing no specific requirements. While this approach enabled TSA to select a vendor (Unisys) quickly, it places total reliance on contractors not only to deliver them but also to decide the agency's requirements. As a result, it may be difficult for the agency to evaluate the contractors' performance.

Further, some contracts, regardless of their earlier merits, may no longer be necessary in accomplishing DHS' mission.

Grants Management

Essentially, DHS will absorb five distinct emergency preparedness grant programs: (1) a $3.5 billion First Responder Program; (2) a $300 million Assistance to Firefighters Grant Program; (3) a $300 million Domestic Preparedness Grant Program; (4) a $500 million Public Health Emergency Preparedness Program; and (5) a $300 million Emergency Management Preparedness Grant Program. Previous FEMA and Department of Justice (DOJ) OIG reports have identified significant shortcomings in the pre-award process, cash management, monitoring, and grant closeout processes. Further, each of these programs has redundant or similar features, i.e., emergency planning, training, and equipment purchases and upgrades for emergency management personnel (state and local police, firefighters, and health care workers). Nevertheless, these programs are to be divided between two separate DHS directorates. Preparedness for terrorism will be placed in the Border and Transportation Security directorate, while other preparedness efforts will be located in the Emergency Preparedness and Response directorate. This bifurcation will create additional challenges related to inter-departmental coordination, performance accountability, and fiscal accountability. Furthermore, program managers have yet to develop meaningful performance measures necessary to determine whether the grant programs being absorbed by DHS have actually enhanced state and local capabilities to respond to terrorist attacks and natural disasters.

BORDER SECURITY

The INS has about 9,000 agents along the border with Mexico, augmented by fences and a substantial automated sensor and surveillance infrastructure. On the Canadian border, however, INS is under-resourced in both personnel, with approximately 500 agents, and equipment. GAO has estimated that it will take years before INS can fully implement its border strategy.

Entry/Exit Tracking: INS has no effective system to determine whether non-citizens who enter the country subsequently leave it. Many aliens enter under temporary visas and then remain past the expiration date ("visa overstays"). Prior INS efforts tracked only travelers entering and exiting at airports by collecting paper forms, which proved to be an expensive failure. DOJ OIG has found in its reviews that INS lacks project management skills and the information technology (IT) capability to ensure successful acquisition and deployment of such a system.

INS has initiated the National Security Entry-Exit Registration System (NSEERS), a targeted tracking system for male nationals from 25 designated countries that includes photographing, fingerprinting, and location reporting. The system is intended to enable INS to check the individual against criminal history and immigration record databases, to verify reported location and activities, and to determine whether the alien overstayed his/her visa. The Senate's Fiscal Year 2003 budget markup expressed a concern that INS'

claim of success for this program needs to be verified. (I would hope to undertake to do so early in my tenure.) In addition, the DOJ OIG has received indications that the program is unevenly administered and misapplied by INS personnel who do not fully understand the program's criteria.

Student Visa Tracking: INS is developing the Student & Exchange Visitor Information System (SEVIS), a computerized student tracking system designed to tighten INS monitor of foreign students. DOJ OIG's review expressed concerns over computer difficulties SEVIS has experienced, noted that the accreditation of schools involves only a superficial review with many schools yet to be reviewed, and pointed out that the success of SEVIS depends on schools' willingness to provide date relative to their foreign students.

Joint INS-FBI Fingerprinting Initiatives: INS has used 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 INS database. The INS and the FBI have been working for several years to integrate IDENT with the FBI's Integrated Automated Fingerprint Identification System (IAFIS), 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. DOJ OIG is beginning its fourth review of this project (focusing on the FBI angle); it was also one of the four major INS systems that GAO studied, reporting poor oversight and management.

High-Technology equipment: The Remote Video Inspection System (RVIS) is designed to expedite the clearance of low-risk travelers and to enhance security at remote northern border crossings. RVIS is designed to transmit images of the person, vehicle, documents, and passengers to an inspector located miles away at the main monitoring, 24-hour port of entry. As of September, 2001, only seven sites were capable of operating RVIS equipment. Poor contractor performance and a lack of strong oversight caused delays in the deployment of RVIS. Since 9/11, Customs has relied primarily on inspectors at these northern border sites.

Treasury OIG is in the process of completing audits on Customs' use of two other high-tech systems, trade detection equipment and radiation detection systems. With respect to the former, Treasury OIG has found that Customs was not effectively or efficiently using the equipment because management did not ensure that the detectors were placed in locations most conducive to their use, failed to maintain them adequately, and failed properly to train inspectors on their use. For radiation detection systems, Customs does not have a documented strategic plan to ensure proper acquisition and deployment of the equipment, and it has not been collecting data on the usage or performance of the equipment. Also, most of the radiation detection equipment currently being used by Customs inspectors is focused on detecting gamma radiation and is unable to detect neutron radiation.

The Advance Passenger Information System (APIS) is a border enforcement tool used by both Customs and INS at our nation's airports to identify and detain high risk travelers on

flights bound for the United States. The system is intended to collect biographical information such as name, date of birth, and country of residence from international airline passengers and crewmembers entering the United States at airports around the country. Prior to arrival, these people are matched against law enforcement databases to identify people who should be detained and examined for violation of American law. Treasury OIG is drafting an audit report on APIS. The report will conclude that the value of APIS is dependent on several factors beyond Customs' control. First, the authenticity of passenger and crew information is dependent on other governments' source documents (passports, visas, etc.), and the integrity of those documents is sometimes questionable. Second, Customs depends on INS to make referrals based on INS' initial screening of arriving passengers and crewmembers. Third, APIS depends on the FBI's National Crime Information Center (NCIC) and Interagency Border Inspection System (IBIS) data to match APIS data for "hits" to occur; however, NCIC and IBIS may require data, like birthdates, that APIS does not always contain.

INTERIOR ENFORCEMENT/DETENTION

INS is thinly positioned to fulfill its non-border enforcement responsibilities. The effectiveness of a system like SEVIS and NSEERS depends on INS' using 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 recent study that, on average, INS 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 INS 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 removed. INS has other daunting interior enforcement responsibilities that include investigating document fraud and counterfeiting, preventing the illegal employment of undocumented aliens, and attacking sweatshops and smuggling enterprises that exploit undocumented aliens.

On average last fiscal year, the INS had 188,547 aliens in detention facilities each day. In addition to its own facilities, INS houses detainees in state, local, and contractor operated jails, for which INS pays a daily rate to the facility. INS recently obtained clearance to pay a profit to state and local jails with which it does business. The practice is likely to cause a significant increase in its detention costs as other suppliers seek comparable treatment.

State and local correctional institutions also hold many aliens who are removable at the conclusion of their criminal sentence. INS' institutional removal program seeks to identify such persons and to conclude the INS removal process before these aliens are released from state or local prison. If INS does not conclude the removal process before the inmate's release, INS must detain such aliens in an INS facility until removal and absorb the costs of doing so. Avoidable detention costs could reach $200 million annually, according to DOJ OIG. DOJ OIG also found that INS lacked comprehensive information about deportable aliens, and, as a consequence, many of them can pass through detention facilities undetected. DOJ OIG found instances where inmates not

identified by the INS as potentially deportable went on to commit more crimes after being released into the community, including child molestation, aggravated assault, and cocaine trafficking.

DOJ OIG has also reviewed INS' implementation of its policies for escorting criminal aliens who are being removed from the United States. The report concluded that the INS has placed the traveling public at risk because it does not consistently follow its escort policy. Some INS field supervisors disregarded provisions of the policy, resulting in the transportation of violent aliens on commercial airlines without escorts.

INFORMATION TECHNOLOGY AND SECURITY

Information technology will be a major management challenge for DHS. Initially, the CIO will need to establish a department-wide IT infrastructure that will enable communications among approximately 180,000 employees. In addition, the CIO will face the challenge of identifying the agency's IT assets, determining what IT assets are needed to meet mission requirements, and consolidating hundreds of systems from transferred agencies. In addition, the CIO, as required by the Federal Information Security Management Act (FISMA), will have a major challenge in developing and implementing an agency-wide information security management program that addresses the risks and vulnerabilities facing the agency's IT systems.

For example, INS has 87 different computer systems that handle sensitive information. INS has not managed IT acquisition or deployment well. DOJ OIG audits have shown that INS has failed to establish cost baselines, conduct life-cycle development planning, and control costs and delivery schedules. INS also has often lacked comprehensive performance measures to ensure that completed projects meet intended goals and uses.

Another example is the ACE project. ACE is intended to enable Customs to release cargo more efficiently by integrating international law enforcement intelligence, commercial intelligence, and data mining results to focus attention on high-risk importers and accounts. Treasury OIG audit reports have concluded, among other things, that Customs did not have the people and systems in place adequately to manage the development of ACE. Because controls were not being implemented and base line reviews were not being performed, Customs could not identify problems in a timely manner. And, Customs was emphasizing scheduled completion dates at the expense of quality and completeness.

Computer security is a related concern. For example, DOJ OIG found numerous vulnerabilities in two key INS systems that were reviewed pursued to the Government Information Security Reform Act. Further, Customs has not established effective controls to protect its law enforcement related data against unauthorized modification, loss, or disclosure. Any compromise in the security of the law enforcement data contained in Customs' databases would have a detrimental effect on Customs' ability to perform its law enforcement duties.

FINANCIAL MANAGEMENT

The Department quickly must integrate and establish effective controls over the financial systems and operations of the incoming components, each of which brings with it longstanding weaknesses in need of correction. Some components have received unqualified audit opinions on their financial statements; however, they expend tremendous manual efforts and costs to prepare for their financial statements, and weaknesses exist in financial preparation and control. For example, INS has poor databases upon which to calculate accurate fees and to ensure that the fees are spent on the services for which they were paid. INS collects and processes its own fees, but it has been found to have poor cash collection processes at virtually every kind of intake facility. INS has had to halt normal business operations for up to two weeks each year in order to conduct manual counts of millions of applications to calculate its earned revenue figures for its annual financial statement.

In addition, the Customs Service is the second largest revenue producer for the federal government. Total net revenues (duties, excise taxes, user fees, licenses, and other revenue, less refunds, drawbacks and other credits) collected during fiscal year 2002 were $22.1 billion. Ongoing weaknesses in the design and operation of Customs' controls over trade activities and financial management and information systems continue to inhibit the effective management of these activities and protection of trade revenue. Also, Customs has been losing between $151 and $432 million per year in uncollected duties related to international mail. Further, Customs had difficulty in collecting outstanding duties already collected by the Postal Service, primarily due to problems in reaching agreement with the Postal Service on the amounts due.

TRANSPORTATION SECURITY

Gap between security costs and security funding: DHS has requested $4.8 billion for aviation security in fiscal year 2004. This is projected against fiscal year 2003 and 2004 passenger security fee revenues of about $1.7 billion annually and $300 million annually in contributions from the airlines. DOT OIG has recommended strongly against increasing passenger security fees further, noting that government taxes and fees already constitute 26% of airline ticket costs. DOT OIG also recommended against tapping the airport improvement grants program further, observing that doing so would negatively affect airports' ability to fund needed capacity enhancing projects. The alternative is to tap the general fund, at a time when it is already strained by competing demands throughout the federal government.

Screeners: Before 9/11, there were only about 28,000 screeners at the nation's airports. In the last year TSA has hired 62,000. Having augmented the numbers significantly, DOT OIG has recommended that TSA: (1) develop a screener performance measurement system and use it to target training resources to where they are most needed; (2) expand the skills of existing staff and keep them at peak performance levels; (3) determine the proper balance of training between existing and new staff; and (4) "transition" the 45% of screeners who are "temporary" employees into permanent positions or replace them with new employees (who will have additional training needs).

Checking Bags for Explosives: TSA's largely successful effort to implement the requirement that all checked bags be screened by explosives detection equipment by December 31, 2002 has cost $1.6 billion to date. Remaining to be done is: (1) deploying such equipment to the remaining airports where alternative screening methods are in use today; and (2) integrating explosives detection systems into baggage handling systems at the largest airports (at a cost of more than $3 billion); and (3) using research and development funds to develop and deploy more effective and economical equipment to address current and future threats and risks.

Other Transportation Modes: Appropriately, TSA focused its first year efforts on aviation security. This year more focus should be given to mass transit, rail, and intermodal containers. DHS needs to develop meaningful risk assessments and to target limited resources to the areas of greatest vulnerability. Progress is being made on the container vulnerability issue, but this will require implementation.

DOT's continuing responsibilities for transportation safety and efficiency, including transportation of hazardous materials (HAZMAT) will overlap with DHS responsibilities for transportation security, requiring close coordination between the two departments and between the departments and industry. As a start, DHS and DOT should finalize a Memorandum of Agreement outlining their respective security roles and responsibilities.

PORT SECURITY

While Customs has taken positive steps to address the terrorist threat, additional steps are needed. Specifically, Treasury OIG found that vessel containers were not properly secured from the time of entry into port until the time of release by Customs. Physical security at the port and terminals was lax. Customs did not maintain adequate control over targeted containers being delivered for examination. The time between targeting and examination was unduly long. Certain Customs identified security upgrades were not being adequately implemented. Examinations performed were not in accordance with established guidelines, and the results were not always properly recorded in Customs databases. Customs targeting units were either understaffed, poorly trained, and/or given many collateral duties that diverted focus from targeting.

Treasury OIG took note of new Customs initiatives in the area of port security, including CSI, C-TPAT, and ATS, suggesting that further OIG evaluative work in each area is advisable. CSI (Container Security Initiative) is a partnership with other governments to target and inspect high risk vessel containers in foreign ports before those containers are shipped to the United States. C-TPAT (Customs Trade Partnership Against Terrorism) is a joint government-business initiative designed to build cooperative relationships that strengthen overall supply chain and border security. Businesses ensure the integrity of their security practices and communicate their security guidelines to their business partners, thereby taking an active role in the war against terrorism. In return, Customs provides specific "benefits," such as a reduced number of inspections. Another initiative is to improve ATS, 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.

Treasury OIG has found that Customs management controls are not sufficient to mitigate the significant safety, smuggling, and terrorism risks associated with the importation of hazardous materials. Customs' ability to examine HAZMAT cargo is limited due to the inherent danger in handling these materials and the lack of training on the part of personnel. HAZMAT teams are not actively making internal risk assessments concerning dangerous cargo, visiting importers' premises, and providing advice on obtaining samples. Furthermore, both headquarters and port personnel have an aging Automated Commercial System (ACS) that does not provide the information necessary to best allocate HAZMAT resources or to determine which port or what type of HAZMAT shipments may be at highest risk for smuggling drugs or becoming implements of terrorism.

Since 9/11, Customs has expanded the use of high-tech equipment to search for radioactive materials, explosives, chemicals, and biological materials. These pieces of equipment- which includes various vehicle and rail x-ray systems, radiation detection systems, trace detection systems, video systems, and the like – permit Customs officials to inspect cargo and conveyances for contraband without having to perform the costly and time consuming process of unloading cargo or drilling through or dismantling conveyances.

Treasury OIG has been unable to determine whether use of the equipment is meeting Customs' goals. Customs had not developed performance measures or otherwise evaluated the effectiveness of the equipment. Moreover, Customs needed to do a better job of monitoring equipment utilization; the limited data available indicated that equipment was being underutilized. In addition, Treasury OIG found that Customs needed better to track and account for equipment and better plan deployment to avoid installation problems.

INTERNATIONAL MAIL

Each year a huge volume of international mail transported by foreign postal administrators - approximately 160 million letters and parcels - enters the United States at 14 international mail branches (IMB). These IMBs are dispersed throughout the country, but are often co-located with international airports, seaports, and land ports. All international mail is subject to Customs examination, and IBMs are staffed with Customs inspectors, mail specialists, and mail technicians - a total staff of 164 at the 14 locations- who inspect the mail for both contraband and duties owed. Customs uses automated screening equipment, such as x-ray and radiation detection devices and dogs, to assist inspectors in examining the mail.

Treasury OIG audits have found both enforcement and revenue problems. IMBs lacked controls for ensuring that all mail was delivered to Customs for inspection. In some locations, mail bypassed Customs before being delivered to addressees, and in other cases

mail was not being adequately safeguarded. Customs needs to take action to ensure that all mail is delivered to IMBs for inspection. Customs also needs to ensure adequate inspector resources and screening equipment is in place adequately to assess potential threats.

Clark Kent Ervin
Acting Inspector General