DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Review of the Status of Department of Homeland Security Efforts to Address Its Major Management Challenges

Office of Audits

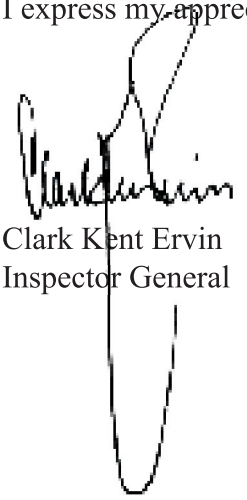
OIG-04-21 March 2004

Preface

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

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein, if any, have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.



Clark Kent Ervin
Inspector General

Contents

Appendices

Introduction

On March 1, 2004, it was one year since almost 180,000 employees and 22 disparate agencies combined to form the Department of Homeland Security (DHS) in one of the largest government reorganizations ever. The reorganization had elements of a merger, divestiture, acquisition, and startup. Because of the size and complexity of the effort, the existing challenges already faced by the incoming components, and the importance of the department's mission, the General Accounting Office (GAO) designated the implementation and transformation of DHS as a "high risk." GAO also noted that successful transformations of large organizations under even less complicated situations could take from 5 to 7 years.

The Office of Inspector General (OIG), as one of its first tasks, consulted with the legacy OIGs whose staffs OIG inherited and identified major management challenges facing the department. These challenges were then used in setting OIG priorities for audits, inspections, and evaluations of DHS programs and operations, and developing OIG's performance plans. As part of OIG's fiscal year (FY) 2004 performance plan, which may be found on OIG's web site, we included an assessment of the department's progress in addressing these challenges. This report presents that assessment, and includes the status of key recommendations still open at the beginning of the period; observations from OIG audits and inspections completed or nearing completion; and discussions with DHS officials on major DHS program initiatives and accomplishments during the year.

Much of the information presented in this report is based on information provided by DHS officials, and which OIG has not had a chance to verify. Consequently, the report does not constitute an audit according to generally accepted government auditing standards, nor does the report contain specific recommendations, other than those made in OIG reports cited herein. Nevertheless, OIG believes this document provides a valuable compendium of issues related to, and DHS' progress in addressing, the major management challenges facing DHS.

Results in Brief

DHS has made significant progress in addressing all of its management challenges. However, some of the planned improvements will take years to develop and implement, and much remains to be done. For example:

- DHS has taken steps to consolidate many of its support service operations, including financial management, contracting, and human resources, but the operations are still not under central control, and contracts management and information technology present formidable challenges.

- DHS has taken steps to consolidate its preparedness grant programs under one component, and generally has been timely in awarding "first responder" funds; however, state and local grant recipients have been slow in spending the funds, and an effective grants management system is needed.

- Financial management functions provided by 19 separate service providers during FY 2003 are now provided by 10 service providers, including 4 outside DHS; however, development and implementation of a single, integrated financial management system are still years away.

- DHS has developed and distributed for public comment proposed human resource regulations that will dramatically affect DHS employees and could serve as a model for the whole federal government; however, finalizing and implementing these regulations will be challenging.

- DHS has made major strides in protecting U.S. borders, including beginning implementation of the United States Visitor and Immigrant Status Indication Technology System (US-VISIT) program, which will provide the capability to record entry and exit information on foreign visitors who travel through U.S. air, sea, and land ports of entry. However, the challenges are immense, and it will take years to address them fully.

Two of the greatest homeland security challenges facing DHS over the past year have been the ongoing effort to implement the Aviation and Transportation Security Act of 2001 (ATSA) and the Maritime Transportation Security Act of 2002 (MTSA). To this end, the Transportation Security Administration (TSA) and the United States Coast Guard (Coast Guard) have made great progress in implementing critical components of the legislation and, as a result, our nation's defense against international terrorism has never been stronger. Despite the

progress that has been made over the past year, tight legislative deadlines, funding difficulties, a shortage of trained and qualified personnel to oversee and implement the legislation, delays in the acquisition and implementation of technological solutions, and a shortage of critical infrastructure to support homeland security initiatives, continue to challenge the department.

Information technology (IT) also remains a major management challenge for DHS. IT systems and tools are fundamental to supporting programs and activities across the department—from counter-terrorism, to border protection, to internal department operations. Effectively managing the IT assets is not only critical to achieving performance goals and the greatest possible returns on investments, it is also required by law. With central responsibility for ensuring effective IT management pursuant to the Clinger-Cohen Act and related statutes, the Chief Information Officer (CIO) is working to establish department-wide IT strategies and a consolidated framework for meeting mission needs. Key areas of focus include IT security, integrating systems, and ensuring effective information sharing.

In February 2004, DHS issued its first strategic plan, with goals and objectives directly linked to accomplishing the three objectives of the President's National Strategy for Homeland Security. These goals and objectives, together with specific measures of effectiveness, which are still being developed, will provide an important impetus for further progress in meeting DHS' management challenges.

The OIG will continue to track the department's progress in these areas. Our FY 2004 performance plan, which addresses many aspects of DHS' management challenges, can be found on our website at www.dhs.gov.

Consolidating the Department's Components

Perhaps the biggest challenge facing DHS is integrating 22 separate components into a single, effective, efficient, and economical department. DHS has made notable progress in this area, but there is much to be done, and OIG has concerns that structural and resource problems are inhibiting progress in certain support functions.

Support Functions

On March 1, 2003, DHS faced the daunting task of supporting 22 different components receiving services from nine different parent agencies. To provide

continuity of service, DHS signed Memoranda of Understanding (MOU) with each of the parent agencies to continue that support. Then, on May 1, the Under Secretary for Management established a transition team to consolidate support services throughout the department. The team identified 255 unique services in the 22 components and DHS headquarters resulting in 3,457 separate services requirements. The services were catalogued under eight lines of business: administrative services, human resources, information technology, procurement, financial management, civil rights, legal, and security.

According to DHS officials, by October 2003, the department was supporting 1463 of the 3457 services, and they expect that most of the services will be provided by DHS by the end of FY 2004. In addition, DHS has made significant progress in consolidating services under fewer service providers within the department:

- 19 financial management service providers were reduced to 10;
- 13 separate contracting offices were reduced to 8;
- 22 human resource offices were reduced to 7;
- 8 different payroll systems were reduced to 3, and the DHS expects to pay all of its employees using one system by the end of the year; and
- 22 property management systems have been consolidated to 3.

Of particular note was the establishment in July 2003 of an integrated project team to realign and transform support services for the 68,000 mission delivery employees assigned to the Bureau of Immigration and Customs Enforcement (ICE), the Bureau of Customs and Border Protection (CBP), and the Bureau of Citizenship and Immigration Services (CIS). This was especially difficult because ICE was highly decentralized, and CBP was highly centralized. The team was to develop a basis for shared services, consolidate services where appropriate to realize economies of scale, and ensure accountability. The result was that CIS, ICE, and CBP each became primary service providers for selected services. For example, CBP provides facilities acquisition and management, ICE provides supervisory leadership training, and CIS provides records management. For some services, however, the three components remain self-supporting. Those services include procurement, personal property, budget, and labor and employee relations. Among the next steps in implementing the tri-bureau shared services arrangement are implementation of a governance charter, establishment of performance

metrics and performance reporting systems, and establishment of "continuous improvement" teams.

Further, DHS has undertaken a new resource transformation initiative called "eMerge^2"[1]. This effort is to result in a consolidated enterprise solution for DHS administrative functions, including accounting, acquisition, budgeting, and procurement. IT management challenges are discussed later in this report.

OIG is concerned, however, that structural and resource problems are inhibiting progress in the areas of financial management, contracts management, and information technology, as discussed in the related sections below.

Program Integration

The Federal Emergency Management Agency (FEMA) was the only existing federal agency that was integrated in its entirety into DHS. While the newly created directorate is titled "Emergency Preparedness and Response" (EP&R), it consists primarily of FEMA. In many respects, moving the entire agency into the department made integration easier; however, there have been problems. FEMA's primary missions have been preparedness for, mitigation of, response to, and recovery from natural and man-made disasters. Almost all of FEMA's efforts have been focused on natural disasters. Transition to DHS meant that EP&R had to maintain its ability to respond to natural disasters and, in addition, increase its ability to respond to terrorist attacks.

EP&R has been successful in maintaining its mission to respond to natural disasters. On September 24, 2003, the Deputy Inspector General testified before the Subcommittee on Clean Air, Climate Change, and Nuclear Safety, Committee on Environmental and Public Works that FEMA has not missed a step in responding to disasters since becoming part of the department.

In shifting toward terrorism preparedness, EP&R has increased its emphasis on activities unique to dealing with terrorist attacks. For example, it has trained and equipped the 28 urban search and rescue task forces to respond to weapons of mass destruction attacks. OIG has not yet reviewed EP&R's efforts in these areas, but we will begin a review of the urban search and rescue response system this year.

[1] "eMerge^2" is the Electronically Managing Enterprise Resources for Government Effectiveness & Efficiency program.

EP&R also acquired other agencies' preparedness and response assets when DHS was created. These assets include the strategic national stockpile, the national disaster medical system, nuclear incident response teams, domestic emergency support teams, and the National Domestic Preparedness Office. According to a senior EP&R official, the largest integration challenge has been integrating the Department of Health and Human Services (HHS)'s strategic national stockpile into EP&R. As shown by the financial statement audit, responsibility for the stockpile is bifurcated and unclear. DHS proposes to return the stockpile to HHS. OIG will continue to monitor integration of these assets into EP&R.

One agency profoundly affected by the creation of DHS was the Immigration and Naturalization Service (INS), previously housed within the Department of Justice (DOJ). As a result of the Homeland Security Act of 2002 (HSA), INS was abolished and legacy components of INS now reside in ICE, CIS, and CBP. OIG is conducting evaluations of ICE and CIS, and we have extensive audit work under way in CBP. We will evaluate the effectiveness of their respective programs, and those of the other component organizations within DHS, as part of our performance plan.

Contract Management

A major challenge for the department is the identification and management of its procurements. DHS has made progress in reducing the number of contracting offices, and has taken numerous steps to promote efficient and effective procurements.

For example, DHS has established a Strategic Sourcing Group (SSG) to implement a department-wide approach to acquiring goods and services. The SSG established commodity councils that are identifying the department's needs for each commodity and developing more efficient purchasing mechanisms to address those needs. So far, DHS has established 14 commodity councils, covering among other things, office supplies, weapons and ammunition, uniforms, electricity, and airport services.

DHS also established the Investment Review Board (IRB), chaired by the Deputy Secretary, as the executive review board that provides acquisition oversight over the department's investments and conducts portfolio management. The IRB conducts systematic reviews of investment preparations and approves key decisions. It also serves as a forum for discussing investment issues and resolving problems requiring senior management attention.

DHS has won awards for its Federal Technical Data Solution program. This program is a part of the Integrated Acquisition Environment E-Gov Program and represents a partnership among the General Services Administration, the Department of Defense, the Office of Management and Budget (OMB), and DHS. This program will be used to disseminate all Sensitive But Unclassified (SBU) information associated with an active acquisition or solicitation to approved business partners, promoting full competition in a secured environment.

Nevertheless, formidable challenges remain. DHS needs to begin integrating the procurement functions of its component organizations to ensure that good management controls are consistently applied. Several of the incoming procurement organizations have lacked important management controls. For example, during its first year of operation, TSA relied extensively on contractors to accomplish its mission, but some contracts were written without clearly defined deliverables, and TSA lacked the staff to provide adequate 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. Also, FEMA has just recently discovered that it has not been reporting or tracking procurements let by its disaster field offices.

Other components of the department have some 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 the Coast Guard's Deepwater Capability Replacement Project will cost $17 billion and take two to three decades to complete. Further, to support the aforementioned US-VISIT program, DHS will soon award a contract for the development of an automated system for tracking and controlling the entry and exit of all aliens entering and leaving the country through air, land, and sea ports. It is anticipated that this will be a multi-billion dollar program implemented over the next 10 years. OIG will be reviewing these major procurements on an ongoing basis.

DHS has also struggled to prepare a sufficiently detailed and accurate listing of its procurements. The data DHS has received to date has come from 22 different sources, does not provide total contract award information, and has not been independently validated. While efforts are under way to bring all of DHS' procurements under the umbrella of one comprehensive reporting system, data for FY 2003 and FY 2004 have not been reported in detail sufficient to manage the procurement universe and have not been independently validated to assure accuracy and consistency.

Grants Management

DHS inherited a variety of grant programs that provide money for disaster preparedness, response, recovery, and prevention. Significant shortcomings had 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, OIG reported that many items authorized for purchase under the program are also authorized for purchase under the State Homeland Security Grant Program.[2] In addition, preparedness grant programs were located in different department directorates, creating challenges related to inter-departmental coordination, performance accountability, and fiscal accountability. Furthermore, DHS program managers needed to develop meaningful performance measures to determine whether the grant programs have actually enhanced state and local capabilities to respond to terrorist attacks and natural disasters.

DHS has made significant strides in this area, particularly in consolidating the preparedness grant programs. However, problems remain, and means must be found to ensure that first responder funds are being used effectively and getting to those who need them in a timely manner.

Consolidation of Preparedness Grants

DHS has taken steps to consolidate the two principal offices responsible for administering the grant awarding process for emergency responders and state and local coordination: the Office of Domestic Preparedness, and the Office of State and Local Government Coordination. This consolidation addresses the need to tie all DHS terrorism preparedness programs together into a cohesive overall national preparedness program. We applaud this effort.

DHS is also in the process of creating the Grants Management Council. It is intended to be a group of senior DHS managers to provide advice on issues regarding DHS grant programs. It will include identifying innovative approaches to promote effective business practices that ensure the timely delivery and proper stewardship of federal assistance funds. The first meeting was held on February 10, 2004. We support this effort and will participate in an advisory role.

Preparedness and First Responder Grants

Based on the FY 2001 through FY 2005 budget requests, over $14 billion in assistance will be made available for grant programs during the 5-year period.

[2] Assistance to Firefighters Grant Program (Audit report number OIG-ISP-01-03, September 2003)

DHS estimates that there are more than 80 grant programs[3] now under its managerial control, and many of them fund preparedness and first responders. We recently completed fieldwork related to a review of Office for Domestic Preparedness (ODP) first responder grant distribution and spending. We found that states, local jurisdictions, and first responder organizations have been slow to spend ODP first responder grant funds, although, in many cases, the funds have been obligated. In many cases the states have specific plans in place and know who will get the money and what they will buy. In addition, state and jurisdiction officials agreed that spending the funds wisely was more important than spending them quickly. Nevertheless, there is room for improvement.

We found that, as of February 10, 2004, the majority of the $2.4 billion in FY 2002 and 2003 first responder grant funds awarded have not been drawn down. The 56 states and territories that had been awarded the funds had drawn down only 36% of FY 2002 awards and about 13% of FY 2003 awards.

In addition to delays caused by planning requirements, we identified numerous other reasons for delayed spending. For example, local governments' processes for grant approval and procurement often cause delays. Some delays, such as equipment delivery backlogs, are unavoidable.

For the most part, delays were not due to ODP's processing and approving grant applications, and states generally were pleased with ODP's performance. However, DHS needs to require more meaningful reporting by grantees, and develop performance standards, so that it can track their progress more accurately; work with grantees to collect and identify best practices and strategies that speed spending; and assist state planning efforts by accelerating the development of federal guidelines for first responder capabilities, equipment, training, and exercises.

OIG is planning a continuing series of audits of preparedness and first responders grant programs to assess states' management of the grants.

Further, DHS is tasked with producing a detailed national assessment of the terrorist threat as a basis for federal spending and regularly updating the assessment in the future. By January 31, 2004, ODP collected homeland security strategies from each of the states. However, it remains to be determined how the data in these state strategies can be used to obtain a national picture of the terrorist

[3] The number of programs is surprisingly large due in part to separate appropriations in the same and different years and name changes that all get counted as separate grants, even though they are for the same or similar purposes.

threat, as well as, how reliable the data behind the strategies is. OIG will conduct an audit of the homeland security strategies data collection this year.

Grants Management System

DHS is faced with developing an effective, integrated grants management and accounting system, but is still a long way from accomplishing that objective. While grants managed by the Science and Technology (S&T) Directorate, ICE, the Information Analysis and Infrastructure Protection (IAIP) Directorate, and ODP fire grants, are processed under MOUs with FEMA, other components' grants are managed by outside agencies:

- DOJ processes the ODP grants, except for fire grants.
- The Federal Aviation Administration (FAA) processes the TSA aviation grants.
- The Department of Energy (DOE) processes S&T grants and contracts with Oak Ridge National Labs.

DHS' Grants Policy and Oversight Office has been inventorying DHS grants, no small task, as well as collecting the regulations and relevant laws for each, and identifying awarding offices, servicing offices, grants management systems, and administrative staff. This office was also spearheading the e-grants initiative until DHS' Resource Management Transformation Office took over that responsibility in September 2003.

Progress in this area may have been hampered by inadequate resources. About 63 FY 2002 grants and more than 83 FY 2003 grants were integrated into DHS, yet the Grants Policy and Oversight Office was staffed by only one full-time person for much of the past year. The problem is receiving additional attention and funding in FY 2004. OIG will continue to monitor DHS' progress in this regard.

Financial Management

The most immediate financial management challenge for DHS has been the orderly transition of the financial operations of its inherited components and the development of plans for its own integrated financial management system. As noted above, DHS has made significant progress in these areas. Further, DHS was presented with the challenge of preparing its first set of financial statements for audit, and met that challenge under difficult circumstances. Finally, DHS has

the challenge of collecting more than $22 billion in duties, excise taxes, fines, penalties, and other revenues.

Integration and Reporting of Financial Information

OIG's audit contractor, KPMG LLP (KPMG), recently completed an audit of DHS' financial statements as of September 30, 2003, and for the 7 months then ended, as required by the Accountability of Tax Dollars Act of 2002. Despite limited staff with many other responsibilities, DHS officials agreed to accept the challenge of a financial statement audit, even though it added strain on its relatively limited resources. They recognized that an audit would establish a solid baseline from which DHS could plan for and build good financial management processes. With this audit, DHS now has that solid baseline for measuring improvement.

KPMG gave a qualified opinion on the consolidated balance sheet and statement of custodial activity, meaning that, except for certain items described below, they were presented fairly and free of material misstatements. KPMG was unable to provide an opinion on the remaining statements for the reasons discussed below. The qualification on the balance sheet related to:

- The lack of sufficient documentation provided prior to the completion of KPMG's audit procedures to support $2.9 billion in property, plant, and equipment at the Coast Guard;
- KPMG's inability to observe sufficient physical counts of operating materials and supplies at Coast Guard or otherwise verify the valuation of operating materials reported in the amount of $497 million; and
- The lack of sufficient, actuarial documentation provided prior to the completion of KPMG's audit procedures to support retirement benefits recorded at $3.3 billion at the Secret Service and post-employment benefits recorded at $201 million at the Coast Guard.

The Coast Guard's financial statements had never been audited at the level of detail required at DHS, where the Coast Guard became a larger bureau relative to its executive department. It is not uncommon for a large established agency such as the Coast Guard to require additional time to get its processes and systems in place to facilitate a financial statement audit at this level of detail. The Secret Service has obtained actuarial report on its retirement benefits liability, and

believes it has recorded the correct amount. Coast Guard has likewise done the same for its post-employment benefits liability.

KPMG was unable to provide an opinion on the consolidated statements of net cost and changes in net position, the combined statement of budgetary resources, and the consolidated statement of financing for several reasons. First, several "legacy" agencies (agencies from which component entities or functions were transferred to DHS) submitted accounting and financial information over which DHS had limited control. Consequently, the auditors were unable to complete procedures relating to revenue, costs, and related budgetary transactions reported by the legacy agencies to DHS. In addition, KPMG was unable to complete audit procedures over certain revenues, costs, and related budgetary transactions at the Coast Guard, prior to the completion of the DHS consolidated audit.

DHS inherited 18 material weaknesses from the Customs Service, the INS, FEMA, and TSA. KPMG determined that nine of the material weaknesses were corrected or partially corrected. The remaining ones were consolidated into seven DHS material weaknesses or reclassified to a reportable condition or other matter for management's attention. The seven material weaknesses included the following

- Financial Management and Personnel: DHS' Office of the Chief Financial Officer (OCFO) needs to establish financial reporting roles and responsibilities, assess critical needs, and establish standard operating procedures (SOPs). These conditions were not unexpected for a newly created organization, especially one as large and complex as DHS. The Coast Guard and the Strategic National Stockpile had weaknesses in financial oversight that have led to reporting problems, as discussed further below.

- Financial Reporting: Key controls to ensure reporting integrity were not in place, and inefficiencies made the process more error prone. At the Coast Guard, the financial reporting process was complex and labor-intensive. Several DHS bureaus lacked clearly documented procedures, making them vulnerable to the loss of key people.

- Financial Systems Functionality and Technology: The auditors found weaknesses across DHS in its entity-wide security program management and in controls over system access, application software development, system software, segregation of duties, and service continuity. Many

bureau systems lacked certain functionality to support the financial reporting requirements.

- Property, Plant, and Equipment (PP&E): The Coast Guard was unable to support $2.9 billion in PP&E due to insufficient documentation provided prior to the completion of KPMG's audit procedures, including documentation to support its estimation methodology. TSA lacked a comprehensive property management system and adequate policies and procedures to ensure the accuracy of its PP&E records.

- Operating Materials and Supplies (OM&S): Internal controls over physical counts of OM&S were not effective at the Coast Guard. The Coast Guard also had not recently reviewed its OM&S capitalization policy, leading to a material adjustment to its records when an analysis was performed.

- Actuarial Liabilities: The Secret Service did not record the pension liability for certain of its employees and retirees, and when corrected, the auditors had insufficient time to audit the amount recorded. The Coast Guard also was unable to provide, prior to the completion of KMPG's audit procedures, sufficient documentation to support $201 million in post-service benefits.

- Transfers of Funds, Assets, and Liabilities to the Department: DHS lacked controls to verify that monthly financial reports and transferred balances from legacy agencies were accurate and complete.

Other reportable conditions included the following:

- Drawback Claims on Duties, Taxes, and Fees: The CBP's accounting system lacked automated controls to detect and prevent excessive drawback claims and payments.

- Import Entry In-bond: CBP lacked an effective compliance measurement program to compute an estimate of underpayment of related duties, taxes, and fees.

- Acceptance and Adjudication of Immigration and Naturalization Applications: The CIS' process for tracking and reporting the status of applications and related information was inconsistent and inefficient. CIS did not perform cycle counts of its work in process that would facilitate

the accurate calculation of deferred revenue and reporting of related operational information.

- Fund Balance with Treasury (FBWT): The Coast Guard did not perform required reconciliations for FBWT accounts and lacked written SOPs to guide the process, primarily as the result of a new financial system that substantially increased the number of reconciling differences.

- Intra-governmental Balances: Several DHS bureaus had not developed and adopted effective SOPs or established systems to track, confirm, and reconcile intra-governmental balances and transactions with their trading partners.

- Strategic National Stockpile (SNS): The SNS accounting process was fragmented and disconnected, largely due to operational challenges caused by the laws governing the SNS. A $485 million upwards adjustment had to be made to value the SNS in DHS' records properly.

- Accounts Payable and Undelivered Orders: CIS, ICE, TSA, and the Coast Guard had weaknesses in their processes for accruing accounts payable and /or reporting accurate balances for undelivered orders.

Further, KPMG identified weaknesses in the DHS' reporting process for the Federal Managers' Financial Integrity Act of 1982 and instances of non-compliance with the Federal Information Security Management Act. KPMG also noted instances where DHS was not in full compliance with Office of Management and Budget Circular A-133, subpart D – *Federal Agencies and Pass-Through Entities* and Appendix B, *Compliance Supplement*.

Revenue Collection

CBP is not only responsible for border security and narcotics interdiction, it is also responsible for enforcing trade regulations and collecting associated revenues. Annually, the United States collects more than $24 billion in customs duties, excise taxes, fines, penalties and other revenue. While it is paramount that DHS ensure that the nation's ports are secure from terrorist activities, it is also important that the revenue base is protected.

CBP's compliance measurement program targets importers to assess trade compliance and project the revenue base, along with the associated revenue gap. The revenue gap is the difference between the dollar amount of import duties,

taxes, and fees that CBP could have collected under current operations had all goods been entered in full compliance, and the actual amount of revenue collected by CBP. Using this information, CBP estimated the revenue gap to be $170 million for FY 2003. However, the reliability of the compliance measurement data is questionable. We identified discrepancies in the data used to establish the compliance rate, for example import data varied depending on the database accessed. Accordingly, the compliance rate may be imprecise.

The Treasury OIG had conducted a review of CBP's international mail operations. Each year a huge volume of international mail transported by foreign postal administrators - approximately 160 million letters and parcels - enters the United States at 13 international mail branches (IMB). These IMBs are dispersed throughout the country, but are often co-located with international airports, seaports, and land ports. In addition to examining the mail for implements of terror and other contraband, CBP examines the mail to identify dutiable parcels. Treasury OIG reported that information on values from the mail declarations is often inaccurate and reliance on such information has resulted in CBP's losing revenue. CBP has taken measures to improve the collectability of mail revenue. These measures include:

- Using the mail survey results to target where the greatest potential for revenue in mail packages is located based on type of mail, country of origin, etc.;
- Revising its International Mail Operations and Enforcement Handbook to standardize operations at all IMBs; and,
- Monitoring incoming mail to ensure that international mail is delivered to CBP for inspection.

However, since receipt of the mail at the IMB is the primary mission of the United States Postal Service (USPS), CBP must work cooperatively with the Postal Service to ensure that adequate processes are in place at the IMBs to ensure that all mail is delivered to CBP for inspection, and outstanding duties are collected from the USPS.

Both ICE and CIS perform an integral role in collecting and accounting for the more than $1 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 must perform regular data calls

to obtain information on its pending application inventory, which is important in measuring performance. This situation and the lack of regular cyclical inventories of this work-in-process has caused CIS to halt normal business operations for up to two weeks in past years in order to report deferred revenue accurately. "Deferred revenue" is a financial measure of pending applications and is material to the Department's financial statements. Also, DHS' financial statement audit found that CIS lacks standard operating procedures to track and report the status of applications and related information. The challenge for CIS is to move from paper based and non-integrated processes to an integrated case management system, which CIS is planning to implement.

CBP processes drawback claims on duties, taxes, and fees. "Drawback" is a remittance of duties, taxes, or fees previously paid by an importer. Drawback typically occurs when the imported goods on which duties, taxes, or fees have been previously paid, are subsequently exported from the U.S., or destroyed prior to entering the U.S. commerce. The Automated Commercial System (ACS), which accounts for the revenue, lacks controls to detect and prevent excessive drawback claims and payments. Additionally, ACS does not have the capability to compare, verify, and track essential information on drawback claims to the entries or export documentation upon which the drawback claim is based. Further, drawback review policies do not require drawback specialists to review all related drawback claims against the associated entries to determine whether, in the aggregate, an excessive amount was claimed. Accordingly, CBP must rely on a manual sampling approach to compare, verify, and match entries and export documentation to drawback claims submitted by importers. As a result, the inherent risk of fraudulent claims or claims made in error is high.

CBP is also responsible for collecting user fees from air passengers and commercial vessels arriving in the United States, as required by Consolidated Omnibus Reconciliation Act. The retailer of the passengers' tickets must collect the user fee and remit payment to CBP quarterly. The fees are designed to pay for the costs of inspection services provided by CBP, which now includes INS and the Animal and Plant Health Inspection Service (APHIS) inspection processes. CBP tracks the fees in a database and follows up with delinquent carriers. However, the list of retailers that are liable for payment cannot be reconciled with the user fees that are due. CBP has no viable method to identify all parties selling tickets subject to the fee. Accordingly, CBP cannot impose penalties on the ticket seller not collecting the fee.

To comply with the reporting requirements of the ATSA, CBP mandated the use of Advanced Passenger Information System (APIS) to target people who could threaten homeland security. However, the APIS is utilized only by the enforcement branch of CBP, and the information gathered on arriving passengers, which includes the country of origin, is not shared with the financial staff responsible for collecting the user fees. CBP collects information regarding the number of passengers on each vessel by reviewing flight or ship manifest information that is entered into the Entry Clearance Arrival Record (ECAR) system. The information entered in ECAR does not include information regarding country of origin, and thereby does not specify the fee required from the passenger. As a result, CBP may not be collecting all the passenger user fees mandated by law from people entering the U.S.

Between FY 1998 and FY 2002, the former 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 important that CBP ensure that the appropriate revenues are collected and are adequate to cover the costs of services provided.

Similarly, TSA is also required by statute to impose a fee on passengers of air carriers and may impose a fee on air carriers for the difference between TSA's costs of providing civil aviation security services, and the amount of passenger fees collected. These fees are designed to pay for the costs of providing civil aviation security services including: costs of screening personnel and their supervisors; equipment; federal law enforcement officers; and civil aviation security research and development. TSA should also ensure that the appropriate revenues are collected and are adequate to cover the costs of services provided.

Information Technology Management

IT remains a major management challenge for the Department. IT systems and tools are fundamental to the programs and activities across the department used to accomplish its wide-ranging missions—from counter-terrorism to border protection to supporting internal department operations. Effectively managing the IT assets is not only critical to successfully achieving performance goals and maximizing returns on investments, it is also required by legislation. With central responsibility for ensuring effective IT management pursuant to the Clinger-Cohen Act and related legislation, the CIO is working to establish department-wide IT strategies and a consolidated framework for meeting mission needs. Key

areas of focus include IT security, integrating systems, and ensuring effective information sharing.

Securing the IT Infrastructure

To meet requirements of the Federal Information Security Management Act (FISMA), the CIO is charged with developing and implementing a department-wide information security management program that addresses the risks and vulnerabilities facing DHS' IT systems. Based on its annual FISMA evaluation, OIG reported in September 2003 that DHS has made some progress in establishing a framework for an IT systems security program. Such progress includes establishing IT security policies and procedures and creating an organizational unit headed by a Chief Information Security Officer to govern information security department-wide. DHS also has instituted an Information Systems Security Board to ensure systems security and effective IT portfolio management as part of its overall capital planning and investment control process.

Currently, DHS must rely on its component organizations to follow its established policies and procedures for implementing the IT security program. However, as part of its 2003 FISMA evaluation, OIG reported that none of the DHS components had a fully functioning IT security program, and there were a number of key security areas that required management attention. Specifically, while 42% of DHS' systems had security plans, only 37% of the systems had been certified and accredited and only 39% had been assessed for risk. Further, only 21% of DHS' system controls had been tested and evaluated, and only 11% of its systems had contingency plans. Based on these findings, OIG recommended in its evaluation report that the CIO designate information security a material weakness at DHS. OIG made 5 additional recommendations in its FISMA evaluation to assist DHS in establishing an effective information security program.

To address its information security needs, DHS has developed an information technology security program strategic plan, with identified major program areas, goals, and objectives, for migrating to a unified information security infrastructure over the next 5 years. The plan outlines eight distinct security program areas: program management and integration; compliance and oversight; security architecture; continuity planning for critical department assets; information security, training, education, and awareness; security policy; security operations; and national security systems and computer security management. DHS considers the first four of these security program areas as material weaknesses and

anticipates completing specific initiatives and achieving mature capabilities in all program areas by the end of FY 2005.

Systems Integration

Another challenge for the CIO is in establishing a department-wide IT infrastructure for effective communications and information exchange among its approximately 180,000 employees, largely drawn from the 22 legacy agencies. In this context, the CIO is charged with identifying IT assets and consolidating and/or integrating hundreds of systems from the transferred agencies.

Taken together, DHS organizational elements have over 100 disparate, redundant, and non-integrated systems used to support a range of administrative functions, such as accounting, acquisition, budgeting, and procurement. To address these issues, DHS has established the "eMerge^2" program, scheduled for implementation by September 2006. Program goals include implementing DHS-wide enterprise solutions to increase efficiency and effectiveness significantly, while optimizing investments. Based upon recent OIG discussions with management officials, the program's design and acquisition phase is on schedule, and DHS has identified requirements, and has issued a request for proposals, for enterprise-wide solutions to meet mission requirements.

Further, the CIO must ensure that individual technology investments are aligned with an overarching, department-wide framework for IT. To this end, the CIO has a stated goal of implementing "one network, one infrastructure" by December 2005. To establish the network, the CIO has established the Enterprise Infrastructure Board that meets periodically to discuss strategies for connecting the department networks, which include local area networks, metropolitan area networks, and wide area networks. The Enterprise Infrastructure Board is comprised of a number of project teams, such as the Network Security Board, which is tasked with implementing an initiative to institute the firewalls, routers, switches, and other technologies needed to secure DHS networks. DHS is enhancing ICE's "backbone" to create the department-wide network that establishes data communications between all of its organizational elements.

With release of the first version of enterprise architecture in September 2003, the CIO made progress toward the goal of one DHS infrastructure. However, this version only outlines a very general transition strategy that must be broken down further for the architecture to be implemented. Nonetheless, the enterprise architecture team is working with several large project offices, e.g., ACE and US-VISIT, to determine alignment to its transition strategy so that these project

offices can begin building to the target architecture. Work is currently under way on version 2 of the enterprise architecture. One of the objectives of DHS' enterprise architecture team is to make the transition strategy in version 2 more detailed and easier to implement.

Information Sharing

Interagency coordination and information sharing are critical to support DHS counter-terrorism, law enforcement, and emergency preparedness and response activities—several of the core reasons for which DHS was founded. In some instances, systems enhancements and integration are required to facilitate the communications and exchange across federal, state, and local government and industry lines. For example, DHS faces a major challenge of working with intelligence and law enforcement agencies to standardize and consolidate multiple terrorist watch lists to control and protect U.S. borders and apprehend terrorists in the homeland. Traditionally, terrorist watch list information has been compiled and maintained in disparate federal agency databases, with no assurance that any one list contains all of the identified names of potential terrorists. State and local law enforcement officials typically have not had access to terrorist watch list information.

Following the terrorist attacks of September 11, 2001, the Congress passed, and the President signed, several pieces of legislation, including the Enhanced Border Security and Visa Entry Reform Act of 2002 and the USA PATRIOT Act of 2001, which requires terrorist information sharing, as well as standardization and consolidation of individual agency watch list systems.

DHS also has a key role in terrorist watch list consolidation. Specifically, the CIO has the primary responsibility within the department for ensuring that the Terrorist Screening Center's (TSC) technical requirements are compatible with the various systems that DHS currently uses or is developing to thwart terrorist activities. The CIO has been coordinating with TSC representatives since the mid-October 2003 to provide requirements, technology, and communications support to the TSC. The CIO will have ongoing involvement in this effort, as DHS plans and implements changes to the screening and intelligence systems it uses to access the TSC database. One goal is to implement "real-time" connections between the systems that DHS and the TSC use in the terrorist screening process. Ultimately, biometric identifiers are to be introduced to support the terrorist screening process.

A number of DHS components, including TSA, CBP, CIS, and ICE, are major customers of TSC and also have significant roles in the consolidation efforts. If and when implemented, TSA's Computer-Assisted Passenger Prescreening System (CAPPS II) will enhance DHS' name-checking capabilities. CAPPS II will eventually connect with TSC systems. Together with officials from the Information Analysis and Infrastructure Protection (IAIP) directorate who are assisting the TSC, these DHS organizations have a vested interest in addressing the various concerns that have arisen related to consolidation of the terrorist screening process. These concerns include ensuring that the new system is designed to accommodate the various mission requirements of participating agencies, and that the flow of terrorist information data is not interrupted or delayed as new processes and systems are implemented.

Human Capital Management

HSA gave DHS special authorization to design a human capital management system that fit its unique missions. On April 1, 2003, DHS announced that it would assemble a diverse team of employees from across DHS, the Office of Personnel Management (OPM), and representatives of the major unions to design DHS' human capital management system. This team developed a range of options for pay and classification, performance management, labor relations, discipline and employee appeals that was presented to the Secretary and the Director of OPM.

The decisions of the Secretary and the Director were published as proposed regulations in the Federal Register on February 20, 2004, with a request for public comment within 30 days. These new regulations will affect not only DHS employees, but possibly the entire civilian workforce, as the DHS system is used as a model for other civil service personnel systems.

Intelligence Matters

DHS challenges include establishing effective working relationships with the Terrorist Threat Information Center (TTIC) and TSC; fully staffing the IAIP directorate; developing common standards for information sharing with relevant federal, state, local, and "first responder" entities; and identifying, validating, cataloguing, and prioritizing critical U.S. infrastructure protection. OIG will examine these areas as part of its FY 2004 performance plan.

Agency Roles

HSA[4] made the Under Secretary for IAIP responsible for, among other things, accessing, receiving, and analyzing law enforcement information, intelligence information, and other information from agencies of the federal government, state and local government agencies, including law enforcement agencies, and private sector entities, and integrating such information in order to: identify and assess the nature and scope of terrorists threats to the homeland; detect and identify threats of terrorism against the United States; and understand such threats in light of actual and potential vulnerabilities of the homeland.

The TTIC and TSC were created after IAIP was established. The TTIC is managed and funded by the Director of Intelligence and TSC is managed and funded by the FBI. While the TTIC and the TSC are working toward building an integrated intelligence analysis capability, there is still confusion within the federal government and among state and local governments about the respective roles of the TTIC, TSC, and the Information Analysis (IA) component of IAIP.

IAIP officials told OIG that, as a full member of the Intelligence Community (IC), IA is committed to working with and through TTIC and the TSC both to obtain and to make threat related information concerning the homeland accessible to the appropriate parties. IA officials stated that it is currently fulfilling its mandate to provide independent analysis of domestic threat related information provided to it by its fellow members of the Intelligence Community (including TTIC) and other DHS components. IA officials stated also that it is fulfilling its responsibility to use that analysis to coordinate with Infrastructure Protection (IP) so as to protect potential targets and create information products to warn relevant state and local government officials and private sector leaders.

IAIP officials said that TTIC is responsible for collecting all threat related information concerning the homeland from the IC and creating "broad picture" reports, while the TSC is responsible for maintaining the database of known or suspected terrorists submitted by a number of federal agencies. These missions, while different, do require a great deal of communication and cooperation between the entities. No one party is responsible for establishing clear guidance on the role of each organization in establishing information and collection requirements. Rather, the parties must work together to develop understanding as to their respective roles and as best practices.

[4] Homeland Security Act of 2002 section 201.

To protect and advance DHS equities, the deputies of both the TTIC and TSC are DHS employees. Additionally, analysts from DHS are assigned to both the TTIC and the TSC. These analysts and the Deputy Directors represent DHS interests within each organization, meet with senior leadership, and share with DHS/IA threat related information, as well as areas of concern and suggestions for improvement.

As part of OIG's FY 2004 performance plan, we will evaluate the challenges and results to date from DHS' efforts to standardize and consolidate the various agencies' terrorists watch lists. We will also assess DHS' role in TTIC and TSC and the degree to which DHS IAIP needs are met through those organizations.

IAIP Directorate Staffing

The IAIP is understaffed. IAIP inherited positions from five legacy organizations at its inception, many of which were vacant. IAIP began to hire new employees in May 2003, and put into place an aggressive hiring strategy, recruiting talent both from the government and the private sector. During FY 2004, IAIP expects to complete hiring to its initial authorization, and simultaneously to begin to hire its FY 2004 staffing complement. Those positions will be both internal to IAIP and external placements, which have been verified as requirements, e.g., the TTIC, TSC, and field positions.

Information Sharing

In addition to producing intelligence, DHS must develop common standards for information sharing. Standards must include, at a minimum, a definition of the communications methods and protocols for sharing information and a set of common and consistent policies for retaining and disseminating shared data.

DHS, through IAIP and the Science and Technology (S&T) directorate, are developing approaches for acquiring and implementing information sharing systems. DHS is currently working with various members of the IC to develop an existing product further that will allow for sharing and collaboration between organizations based on policies in a memorandum of agreement. Also, S&T is in the process of developing a Threat Vulnerability Integration System, using industry standard protocols through which each agency that provides intelligence to IAIP can submit information using its own format. Despite the differences in the underlying information sources, DHS expects the system to provide for an integrated analysis capability. Additionally, IAIP officials stated that a team is

researching systems to transfer data from unclassified to classified networks and will be reporting its findings soon.

Creating new processes and requirements creates a challenge. However, IAIP officials say that they are not facing obstacles that would prevent information sharing among DHS and its IC and law enforcement community partners. As DHS matures, processes will become more advanced and fluid. IA officials stated that they are currently receiving the threat related information needed to assess threats to the nation. Some major milestones as IA continues to grow are ensuring prompt access to all relevant internal and external information sources; developing robust outreach from IA to all IC and law enforcement partners and customers; establishing advanced exchange policies and procedures with all partner organizations; completing a collection management plan to engage federal, state and local entities in collecting and assembling information; and ensuring full IA decision-making participation with IC and law enforcement partners on intelligence requirements, tasking, and collection management.

Infrastructure Protection

Identifying, validating, cataloging, and prioritizing critical infrastructure, most of which is owned by the private sector, and key assets, such as national symbols and monuments, are vital to implementing a national infrastructure protection plan. Once the critical infrastructure and key assets are prioritized into a national list, the list will serve as a baseline for making decisions concerning which actions should be taken first to safeguard critical infrastructure and key assets.

The IAIP has solicited data from state and local partners on certain critical infrastructure and key assets and is compiling this data into a national asset database. IAIP officials told OIG that the effort to categorize and prioritize potential terrorist targets and develop lists of critical infrastructure is on schedule and due to be completed no later than July 1, 2004. The identification of the national asset list is an ongoing effort and will result in adjustments to priorities as terrorist tactics and capabilities evolve and interdependencies are identified. The course of action that is under way will aid the grant allocation process as other DHS components depend on prioritized critical infrastructure information to determine which assets to harden first and which homeland security technologies to develop. IAIP officials told OIG that the IAIP has already provided a critical assets list to ODP for two sets of grant allocations.

Border Security

CBP and ICE share responsibility for ensuring the security of our borders. CBP focuses on security at and between the ports of entry along the border, and 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 focuses 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 the formation of DHS, OIGs at DOJ and Treasury, as well as the GAO, identified numerous deficiencies in the systems used to track aliens, and in the deployment, use, and operational effectiveness of the equipment used to carry out the border security mission. To a great extent, these challenges remain, and are discussed below.

Entry/Exit Control Issues at Land Ports of Entry

Historically, development of a national entry-exit system has focused on establishing a process for air passengers at airport ports of entry (POEs). Airport POEs offer many logistical and control features that facilitate an entry/exit system that may not be duplicated at land POEs. Implementing the US-VISIT Program at land POEs will be a complex project that will have to identify operating requirements and develop integration and operability strategies with other systems. The sheer volume of daily traffic at the POEs also challenges the US-VISIT program at the land POEs. This traffic cannot be significantly impeded without causing significant economic and political problems.

US-VISIT is required to be implemented at the top 50 land POEs by December 31, 2004, and at remaining land POEs by December 31, 2005. The US-VISIT system is to provide the capability to record entry and exit information on foreign visitors who travel through United States air, sea and land ports, and will apply to non-immigrants holding non-immigrant visas. By reconciling entry and exit records, US-VISIT will identify visitors who have overstayed their period of admission.

US-VISIT officials anticipate that $330 million appropriated for US-VISIT implementation will be released soon. GAO has reviewed US-VISIT's expenditure plan and will report to Congress in March 2004. Once Congress approves the expenditure plan, the funds will be released.

An integrated project team (IPT) will be used in the implementation of US-VISIT at land border POEs. IPT members will come from CBP, ICE, TSA, and DOJ, information technology, and other areas. The IPT team, which should be in place by the end of March 2004, will finalize US-VISIT's draft deployment plan for bringing ports online through a phased rollout. The IPT team will address operational issues of implementing US-VISIT at land POEs. Also, a new federal regulation must be published to allow US-VISIT to be implemented at land POEs.

The US-VISIT Program Office has initiated a public relations effort to facilitate implementation of US-VISIT on both the northern and southern borders. The Border Guidance Network will enable US-VISIT officials to explain the US-VISIT process, provide implementation updates, debunk myths about US-VISIT, and allay fears. The network includes local chambers of commerce, trucking associations, bridge and tunnel operators, etc. Through the network, the US-VISIT Program Office will be able to work with and hear comments from groups that will be affected by the implementation of US-VISIT at land POEs.

Environmental assessments have been completed for the top 50 land POEs to clear the way for construction. While new lanes are not planned, land POEs may need upgrades to secondary inspection facilities, networking capabilities, and the installation of antennas for radio frequency (RF) technology in existing travel lanes.

The US-VISIT Program Office is working to finalize plans to expand RF technology to land border inbound and outbound travel lanes. While officials there would like to deploy RF technology in all lanes, funds are an issue, so the office is looking at having RF technology in at least one inbound and one outbound lane at each land POE. The RF token will record an individual's entry to and exit from the United States. US-VISIT is also trying to determine the best way to provide the RF token to the traveler e.g., attached to the Form I-94, attached to the passport, or attached to/integrated into the B1/B2/border-crossing cards (BCC). If the RF token is integrated into the B1/B2/BCC rather than creating a sticker to place on existing cards, a card replacement plan will be needed.

To facilitate travel through land POEs, US-VISIT will be deployed at secondary inspection areas for land POEs rather than at primary inspection areas like air and sea POEs. Non-immigrant visa holders are currently referred to secondary inspection for completion of the Form I-94 at land POEs. So, US-VISIT will not create an entirely new inconvenience for non-immigrants. Travelers using the Secure Electronic Network for Travelers' Rapid Inspection (SENTRI) Program

should not be affected by the implementation of US-VISIT at land POEs. These pre-registered, "low-risk" drivers and passengers will continue to use the same travel lanes, except US-VISIT will now be able to track their exits as well.

Neither Canadian nor Mexican citizens are likely to see a large increase in lines and waiting times at border crossings. Most Canadians are not required to have visas to enter the United States and will therefore not be subject to US-VISIT requirements. Only Canadian and Mexican citizens entering the United States under visas will be registered in US-VISIT. Mexican citizens carrying B1/B2/BCC cards will have to declare whether they are entering the United States under the provision of the B1/B2 visa or under the BCC. Mexican citizens entering under a BCC and not going more than 25 miles past the border will not be subject to US-VISIT requirements. US-VISIT will coordinate with CPB on the method for best ensuring that Mexican citizens properly declare their travel intentions at the POEs.

Primary Inspections at Air Ports of Entry

The goal of the primary inspection is to admit legitimate travelers into the U.S. quickly and refer high-risk travelers and inadmissible aliens to a secondary inspection for a more detailed review. The DOJ OIG reported that CBP needs to improve: (1) the operational capability to perform passenger analyses prior to flight arrival; (2) the lookout system capability to provide primary inspectors with critical information such as stolen passports; (3) control of passengers who were referred for secondary inspections to prevent them from leaving the airport without appearing; (4) enforcement of the requirement for primary inspectors to query lookout databases; and (5) training provided to inspectors. CBP has made progress in each of these areas, as discussed below.

- Lookout System. Crucial to the function of CBP is the ability to link immigration documents to people at POEs and to share data with other agencies in order to detect fraudulent documents. CBP uses the National Automated Immigration Lookout System (NAILS), a part of the Interagency Border Inspection System (IBIS), to provide information to inspectors at POEs. CBP is cooperating with the DOS and other DHS components to ensure the integrity of the data share system and in communicating policy changes to all employees.

- Passenger Analyses. CBP has increased the use of APIS to check passenger information against the combined federal law enforcement database, known as IBIS, which contains data from 22 federal agencies.

CBP also checks names against the FBI's National Crime Information Center (NCIC) wanted persons list. In conjunction with the new ATSA requirements, CBP also upgraded and expanded its APIS system. ATSA requires all airlines flying into the U.S. to provide CBP with advance passenger information, the passenger manifest, and personal name and record data. The airline must transmit this data electronically to CBP upon take-off from foreign airports. Using the data, CBP is better able to identify persons posing a potential threat prior to their arrival at U.S. airports. CBP officials state that they have moved aggressively to achieve compliance from all air carriers as soon as possible. In less than a year they achieved a 99% compliance rate. CBP, through its combined customs and immigration authorities, uses that information to evaluate and determine which arriving passengers pose a potential threat risk. In conjunction with the new legislative requirement, CBP also upgraded and expanded its systems to ensure that APIS could keep up with the expanded workflow.

- System Training/Use. Due to the increased need to process alien information into a number of intelligence databases, CBP has initiated the training of new and experienced inspectors on the lookout system. It is the intent of CBP that additional system training increase inspector proficiency. CBP reports that it has revised training given to inspectors for their passenger analytical unit, rover team, and counter-terrorism airport response teams. CBP officials also state that CBP is training personnel in the proper use of the former INS's Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) to identify previous immigration violators, criminals and terrorists. This is in addition to training on lookout and APIS computer intelligence systems.

- Secondary Inspections: The DOJ OIG reported the need for improving airport secondary inspection facilities. Since it is the responsibility of the airlines to provide suitable facilities for inspections, CBP should timely and substantively communicate to the airlines any deficiency in the workspace provided. CBP officials state that CBP commissioned a task force in December 2003 to look at air facilities of the future. This group, working with TSA and ICE, is working on recommendations to increase the physical security of the airport facility, and the technical requirements for a secure exit solution.

- Training. CBP is currently training personnel in the proper use of lookout and APIS computer intelligence systems, analyzing travel patterns and passenger identifications to determine trends, and educating inspectors on how to increase computer proficiency.

Deferred Inspections

People seeking entry into the U.S. are required to pass through a primary inspection where inspectors examine documents, perform immigration and customs database queries, and question travelers. If an immediate decision regarding admissibility cannot be made, inspectors have the discretion to defer the inspection. The person is then allowed into the country and must report to the appropriate INS district office at a later date to complete the inspection.

DOJ OIG reported that immigration officials failed to track these inspections to completion or to penalize people who fail to appear. Even though database systems existed that were capable of capturing and reporting the occurrences and outcomes of deferred inspections.

CBP has made progress in addressing some of the recommendations made in the DOJ OIG report. CBP has established tougher criteria for determining who is eligible for deferred inspection. Those in "high-risk" groups can no longer receive deferred inspections. For instance, people with criminal records, who were previously allowed to receive deferred inspections in some circumstances, can no longer defer inspection because those with criminal records are inadmissible. Also, the authority to grant deferred inspections has been raised to a higher level. In addition, CBP has emphasized that deferred inspections were designed to deal with cases involving resolution of minor administrative deficiencies, usually forms or other paperwork, of those who would otherwise be admissible into the U.S. Finally, different thresholds have been established for allowing deferred inspections based on the current Homeland Security Advisory System threat level (i.e., different procedures during orange vs. yellow threat level).

In tracking and documenting deferred inspections, CBP has revised Form I-546, the primary document for initiating, authorizing, and tracking deferred inspections, to require more information. The deferred inspection form is now electronic, rather than handwritten. Also, CBP moved many deferred inspection offices to port locations because prior locations are not part of DHS.

If a person fails to appear for deferred inspection, CBP creates a lookout in the NAILS, and the person's name and information is referred to ICE for investigation. If that person then attempts to re-enter the U.S. at a later date, the NAILS lookout will notify inspections personnel, and the person will not be allowed to enter.

Risk Management Approach for Inspecting Passengers at Sea Ports of Entry

A DOJ OIG report found that the current capabilities for collecting, analyzing, and sharing inspection data are insufficient for supporting an effective risk management strategy. Methods used at the time of the report to record and maintain inspection data made it difficult to conduct the type of analysis required by an effective risk management strategy, not only at sea POEs that use manual methods, but also at seaports using automated databases. In addition, the report found that not all inspection data is complete or accurate, limiting the extent to which immigration officials may be able to draw reliable conclusions about immigration risks within the seaport environment. Finally, the seaports cannot share or exchange inspection data easily. This further limits the ability to identify any regional or national trends regarding immigration risks and to develop subsequently an appropriate inspection strategy for addressing these risks.

Some cruise ship carriers voluntarily transmit passenger and crew manifest information electronically through APIS prior to arrival at the POE or destination. APIS is a nationwide automated system capable of performing database queries on passengers and crewmembers prior to their arrival in or departure from the United States. CBP, TSA, and the Coast Guard are coordinating APIS regulations that should be published in 30-60 days and will make the submission mandatory.

As APIS data is received, a sea passenger analysis unit at each POE queries against IBIS and the NCIC wanted persons database. The results of these queries are used to identify persons of interest to interview and inspect at the POE. CBP is sharing APIS data with the Coast Guard, and the two agencies are working together to integrate APIS with the Coast Guard's Electronic Notice of Arrival System. This integration is expected to be complete in FY 2004. This will enhance both agencies' ability to identify passengers, crewmembers, and cargo for more thorough inspection.

Integrated Fingerprint Systems

Considerable effort has been expended over a long period of time to integrate the IDENT and IAFIS into an effective tool to identify illegal aliens apprehended entering the country. The integrated tool will be especially useful to identify aliens with outstanding criminal warrants and those on terrorist watch lists. The most recent DOJ OIG report acknowledged that the integration project had made considerable progress, but that there were serious concerns regarding program management, lack of program prioritization, and weak long-range planning. The Justice Management Division within DOJ was the project manager for this effort, coordinating activities of INS and FBI. With the establishment of DHS, it is unclear what agency is acting as the project manager and where program responsibility lies within DHS. The previous DOJ OIG report identified this situation as potentially detrimental to future integration efforts and likely to result in further delays.

The DOJ Justice Management Division is anticipating full integration completion by the fall of 2008. This fully integrated IDENT system will be used by the US-VISIT program to process all visitors to the United States. Concern has been raised regarding the need for daily NCIC updates into the IDENT system and whether the FBI should have access to fingerprints collected by the US-VISIT biometric system.

As of February 18, 2004, 55 sites have been deployed with the recently upgraded version of the software (i.e., 10 fingerprints are captured once and processed simultaneously in one report from both IDENT and IAFIS). This includes 29 border patrol stations and 26 POEs. Ten prints capability has also been deployed to an additional 58 sites, including 30 ICE investigations offices, which allow them to capture and submit electronically prints to IAFIS only. There is also an effort to redeploy IAFIS stand alone units, originally deployed to Border Patrol and Inspections sites, to 20 ICE detention and removal locations to provide them connectivity to the FBI's IAFIS system.

In addition, the US-VISIT program has budgeted funds to continue deployment and use of the integrated IDENT/IAFIS functionality to support criminal identification and booking. However, the US-VISIT program has not initiated deployment with these funds, as there are concerns over the fingerprint image quality produced with the integrated version. In a joint effort, DOJ and DHS have been analyzing image quality data over the past few months in an effort to determine whether the increase in poorer quality images was the result of software, hardware, training, or physical set up. As part of this analysis, in

January 2004, DHS deployed a new scanner at a few sites that had no previous electronic ten print capabilities. The preliminary data has shown significant increase in image quality. DHS has directed the IDENT contractor to provide a software solution that is compatible with more scanners than the current version, which works with just one type of scanner. DHS is waiting for an estimate of how long this solution will take to implement.

Northern Border Issues

In February 2002 the DOJ OIG reported that northern border patrols required additional personnel, equipment and intelligence support to perform enforcement operations to the extent required for maximizing border security. CBP is responsible for the security of the U.S.-Canadian border that includes waterways and vast stretches of wilderness with minimal law enforcement presence. CBP operates and manages of 86 official POEs, as well as numerous unofficial crossings and public land straddled by national parks. Sufficient personnel, close lines of communication, collaboration, and adequate equipment, and its use are needed to ensure adequate security at the northern border.

CBP plans to increase the number of border patrol agents and inspectors on the northern border. Also, CBP has negotiated with Canada to allow the Royal Canadian Mounted Police to use the IBIS intelligence system when processing border crossings. Along with this, CBP plans to incorporate aerial surveillance and sensor technology that would increase the effectiveness of the border patrol agents and inspectors.

Student Visa Tracking

The concerns associated with visa violators, especially students, continue to be a national security issue. Previous DOJ OIG reports identified several issues associated with the Student and Exchange Visitor Information System (SEVIS) that included computer difficulties, the timeliness, accuracy and completeness of the data in the system, the certification of schools that accept foreign students, training of contractors and immigration and ICE personnel, oversight of contractors conducting school site visits, oversight of schools' compliance with SEVIS requirements, procedures for identifying and referring potential instances of student or school fraud, and resource levels for investigating potential fraud. The issues identified by the DOJ OIG reports indicate that there are potential areas where fraud or non-compliance with policies and procedures could lead to breaches of national security.

SEVIS is an automated process developed to collect, maintain, and manage information about international foreign students and exchange visitors during their stay in the United States. SEVIS was designed to respond to the national security concerns raised by the DOJ OIG, Congress and the law enforcement community by improving data accuracy and collection. SEVIS increases the ability of ICE to maintain up-to-date information on foreign students and exchange visitors to ensure that they arrive in the United States, show up and register at the designated school or exchange program, and properly maintain their status during their stay. It does so by combining input from government sources as well as schools specially certified to lawfully enroll foreign students.

The USA PATRIOT Act required that SEVIS be implemented at schools for new foreign students by January 1, 2003. Schools were given until August 1, 2003, to enter all current students into SEVIS and to report their enrollment.

Also, as part of the requirements of the SEVIS program, Congress has mandated that it be fully funded by user fees. ICE has proposed a fee regulation, with the fee set at a level designed to fund the Student and Exchange Visitors Program (SEVP) and compliance efforts related to SEVIS. The proposed regulation was signed by the Secretary on February 19, 2004, and is under review by the Office of Management and Budget. In addition to student fees, SEVP receives limited funding from fees paid by schools in conjunction with applications for school certifications (Form I-17). This fee is currently in place.

The DOJ OIG reviewed the INS' system for monitoring and tracking foreign students and reported that SEVIS would address many, but not all, of its problems.[5] DOJ OIG also evaluated INS' progress in implementing SEVIS and reported deficiencies in: capabilities for accessing the SEVIS system; the processes for certifying schools as eligible to accept foreign students; training of contractors, school and ICE personnel; oversight of contractors conducting school site visits; the timeliness, accuracy and completeness of data in the system; oversight of schools' compliance with SEVIS requirements; procedures for identifying and referring potential instances of student or school fraud; and resource levels for investigation of potential fraud.[6]

[5] "Contacts with Two September 11 Terrorists: A Review of the INS's Admissions of Mohamed Atta and Marwan Alshehhi, its Processing of their Change of Status Applications, and its Efforts to Track Foreign Students in the United States" DOJ OIG, May 2002

[6] "Follow-up Review on the Immigrations and Naturalization Service's Efforts to Track Foreign Students in the United States through the Student and Exchange Visitor Information System," DOJ OIG Report Number I-2003-003, March 2003.

Responsibility for SEVIS transferred to ICE on March 1, 2003. Following the transfer of SEVIS from CIS to ICE, SEVP was established in May 2003 and became operational in June 2003 with 10 full-time positions. The SEVP Office assumed responsibility for administering SEVIS at that time. ICE's Compliance Enforcement Unit (CEU) is responsible for enforcement investigations.

SEVP has addressed the access problems. All Department of State consular posts now have the capability to view SEVIS information. There is an interface between the SEVIS system and the Department of State's Consular Consolidated Database (CCD). Consular officers access CCD, which is populated with key SEVIS information. A nightly interface of data updates any changes to a student's SEVIS record. All POEs have access to SEVIS in secondary inspection areas. The SEVIS helpdesk is available to assist in resolving any computer problems that do arise.

While authority to issue school certifications currently lies with CIS, both CIS and ICE are working to formally transfer this authority to SEVP. Although a delegation of authority transferring complete adjudicatory authority to SEVP has not yet been signed, under a mutual agreement between CIS and ICE, SEVP began adjudication of certain school certification applications on November 1, 2003. The School Certification Unit (SCU) within the SEVP Office initially has 10 full-time positions, which officials believe to be enough for the short term. Once the student fee regulation is approved, managers will be able to staff this area fully. Ultimately, SEVIS will be fully fee funded. The school fee is currently being charged. The student fee will be charged following approval of the proposed fee regulation, which is now under Office of Management and Budget's final review.

Based on data provided by SEVP officials, as of January 30, 2004, approximately 700 schools are in the certification and approval process, over 8,900 schools have been certified as eligible to accept foreign students, and 750,558 active students' and exchange visitors' names are in SEVIS.

The SEVP Office is looking at ways to improve the school certification process. Under the current process, contractors are used to conduct on-site investigations at schools and government personnel evaluate both the contractor report and the application for certification in making a decision whether a school should be certified. The SEVP Office has developed a statement of work to ensure that an improved certification process is comprehensive, efficient, and effective. Once the contract is awarded, the contractor will have 6 months to complete the tasks laid out in the statement of work. These tasks include conducting an independent

assessment of the current certification process; reviewing and developing school certification criteria; developing a complete training package for contractors, school personnel and ICE/SEVP staff; developing a strategic plan for the certification process; and determining the charges for school certification and re-certification. To assist contractors in effectively conducting school site visits, the SEVP Office is looking at developing 10-12 different site visit checklists tailored for different types of schools. Currently only one checklist is used for all schools.

Currently, everyone in the SCU is located at headquarters; however, SEVP officials would like to move some school certification adjudicators into field locations eventually. This would allow adjudicators to become familiar with schools in a particular area, as well as with state laws, which must be taken into account when certifying schools. Also, a delegation of authority is necessary to give ICE the authority to adjudicate the school certification applications. Headquarters personnel are able to view information in SEVIS, but most are unable to adjudicate applications because the delegation of authority for adjudication remains with CIS. Only those adjudicators who were previously at CIS are currently able to adjudicate school applications.

Recertification is required for schools every 2 years and includes a site visit. The SEVP Office is looking at recertification procedures, including options for making the recertification site visit more interactive, with school staff having SEVIS responsibility rather than simply verifying that the school exists and is legitimate. Recertification may include a review of the school's SEVIS data for timeliness, accuracy and completeness and for compliance with SEVIS reporting requirements. A large recertification push will begin in May 2004 as many schools reach the two-year mark.

Schools were required to have all continuing students entered into SEVIS by August 1, 2003. The SEVIS response team, a 24-hour hotline, was activated in the month of August 2003 to provide customer support to incoming foreign students and POEs if information was not correct in or was missing from SEVIS. During the time the hotline was operational, the SEVIS team had 24-hour access to school representatives if necessary. The SEVIS response team was activated again for January 2004; however, some of the response team staff was released early because they were not needed. SEVP officials attributed this to the system's being used properly, people's being aware of and educated about SEVIS, the system's being accurate, and schools' complying with SEVIS requirements.

ICE's CEU is responsible for enforcement investigations, which include investigation of aliens suspected of failing to maintain the terms of their student

status, as reported in SEVIS. The SEVP Office is establishing an SEVP Liaison Program for working with the CEU to identify student violators. Investigators in the CEU pull reports from SEVIS weekly for a list of possible student violators. The list is then vetted to create a "credible leads" list. Currently, investigators in the CEU do final vetting of the list and often find, during the investigation, that administrative or technical errors resulted in someone's being placed on the list. Under the SEVP Liaison Program, an SEVP CEU liaison will do a "final scrub" of the data for administrative and/or technical errors before a final list is sent to the CEU for investigation. Standard operating procedures for the program are currently being finalized, and this revised process should begin in March 2004.

Identification, Location, and Removal Non-immigrant Overstays

Immigration officials have experienced significant problems identifying, locating, and removing non-immigrant aliens who have overstayed their visas, who have violated a notice to appear, or are otherwise reported to be out of status. Immigration officials have also been largely unsuccessful at removing non-detained aliens with final removal orders, removing only 13% of these aliens according to a report issued by the DOJ OIG (DOJ report number, I-2003-004, February 2003.) Moreover, INS was deficient at removing important subgroups, removing only 6% of the non-detained aliens from countries that sponsor terrorism, 35% of non-detained criminal aliens, and only 3% of non-detained aliens denied asylum. The 2003 report followed up on a DOJ OIG report, issued March 1996, I-96-03, which found INS removed 11% of non-detained aliens. Some of the key DOJ OIG recommendations included: establishing annual goals for apprehending and removing absconders and other non-detained aliens with final orders; identifying the resources needed to achieve annual and strategic performance goals, and ensure that resources are applied to all case types; completing the rulemaking titled *Requiring Aliens Ordered Removed from the United States to Surrender to the Immigration and Naturalization Service for Removal;* and implementing with the Executive Office for Immigration Review a shared data system, similar to IBIS, for case tracking to identify and process aliens with final orders.

ICE has taken steps to address the recommendations cited in the report. In FY 2003, ICE asserts that removal of all aliens increased over 21% from FY 2002, and absconder removals increased by over 46%. ICE developed a 6-year plan that aligns its long-term detention and removal strategies with the resources that are required to fulfill them. This plan was used to construct the FY 2005 President's Budget request. Once the FY 2005 budget is enacted, this 6-year plan will be

revised and ICE will then set annual performance targets and develop future budget requests.

Further, ICE's Compliance Enforcement Office is now tasked to identify and locate overstays by using information provided by SEVIS and the National Security Entry Exit Registration System (NSEERS) databases, and the office is expected to use similar data from US-VISIT. In addition, ICE has created a program element specifically for fugitive operations. Guidance was provided to field offices on the use of personnel for fugitive operations, and employee costs associated with the program are being tracked.

On May 9, 2002, INS published a second proposed rule, titled *Requiring Aliens Ordered Removed from the United States to Surrender to the Immigration and Naturalization Service for Removal*, that would broaden notification methods and require all properly notified aliens to surrender within 30 days. This new rule bars properly notified aliens who do not comply with the surrender requirements from applying for administrative relief from removal or from returning legally to the United States for 10 years. The rule applies to aliens currently in immigration proceedings. DOJ OIG reported that as of January 2003, the proposed rule was not final. ICE reports that a final version of the Surrender Rule is complete and awaiting approval from DHS for publication.

The proposed budget for FY 2005 supports an increase of over $100 million for ICE's Detention and Removal Program. This includes an additional $50 million to expand the program to apprehend alien fugitives and includes 236 new positions. However, even when these additional resources are obtained, ICE will face challenges in training and deploying the new agents as hiring and training this number of agents will be a lengthy process. It will take 6 months to a year of on-the-job training to prepare the new agents adequately to handle a normal caseload. ICE will have to determine where to locate personnel to maximize the impact on the outstanding casework with respect to national priorities. ICE also faces a challenge in integrating the information contained in a number of "stove-piped" databases that are utilized to identify and track the fugitives and overstays.

Institutional Removal Program (IRP)

Under immigration law, most criminal aliens, including aggravated felons, are deportable. In many cases, these aliens are incarcerated at federal, state and local facilities serving out criminal sentences. The IRP is a national program that aims to: identify removable criminal aliens in federal, state and local correctional facilities; ensure they are not released into the community; and remove them

Department of Homeland Security

Under Secretaries
Agency Heads
Chief of Staff, Deputy Secretary
DHS OIG Liaison

Office of Management and Budget

Homeland Bureau Chief
DHS OIG Budget Examiner

Congress

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 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 Department of Homeland, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.