STATEMENT OF RICHARD L. SKINNER

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

JANUARY 26, 2005

Good morning Madam Chairman and Members of the Committee:

I am Richard L. Skinner, Acting Inspector General for the Department of Homeland Security (DHS). Thank you for the opportunity to be here today to discuss the work of the Office of Inspector General (OIG) regarding major management challenges facing DHS.

During its first 2 years of existence, DHS worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented an inordinate number of challenges to the department's managers and employees. The Government Accountability Office (GAO) has noted that successful transformations of large organizations, under even less complicated situations, could take from 5 to 7 years. While DHS has made great strides toward improving homeland security, it still has much to do to establish a cohesive, efficient, and effective organization.

The OIG, based, in part, on assessments by legacy OIGs, Congress, the department, GAO, and others, has identified "major management challenges" facing the department, for inclusion in the department's Performance and Accountability Report issued on November 15, 2004. These challenges are a major factor in setting our priorities for audits and inspections of DHS programs and operations. As required by the Reports Consolidation Act of 2000, we will update our assessment of management challenges annually.

Our latest major management challenges report covers a broad range of issues, including both program and administrative challenges. A copy of that report is being provided for the record. In its response to the report, the department recognized the challenges and the potential impact the challenges could have on the effectiveness and efficiency of its programs and operations if not properly addressed. The department anticipates that the results of initiatives to address the challenges during FY 2005 should enable it to report significant progress next year.

The Committee has asked us to focus today on challenges related to border security, transportation security, integration, intelligence, and preparedness. I would like to highlight the significant issues that we have reported in these areas, which deal primarily with border and transportation security, and some of the work that we have underway or planned.

Before I discuss the details of our work, however, I believe it is important that we give credit to the thousands of dedicated, hard working DHS employees who are genuinely committed to securing our homeland and making the department a model for the entire federal government. No one here can deny that our nation is more secure today than it was prior to September 11, 2001.

I also wish to point out that the deparment has been very responsive to and implemented a number of the recommendations made by our office. We look forward to establishing a positive working relationship with the new Secretary, and continuing the momentum already underway toward building an effective, efficient, and economical homeland security operation—one that is free of fraud, waste, and abuse.

BORDER SECURITY

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

Two organizations within BTS are responsible for enforcing the nation's immigration and customs laws. Customs and Border Protection (CBP) inspects visitors and cargoes at the designated U.S. ports of entry (POE) and is responsible for securing the borders between the POE. CBP's primary mission is to prevent terrorists and terrorist weapons from entering the U.S., while also facilitating the flow of legitimate trade and travel. Immigration and Customs Enforcement (ICE) is the investigative arm of BTS that enforces immigration and customs laws within the U.S. While CBP's responsibilities focus on activities at POE and along the borders, ICE's responsibilities focus primarily on enforcement activities related to criminal and administrative violations of the immigration and customs laws of the U.S., regardless of where the violation occurs. CBP and ICE also have employees assigned outside the U.S. to enhance the security of our borders.

In December 2004, the Heritage Foundation recommended merging CBP and ICE and eliminating the Border and Transportation Security directorate. According to the Foundation, the merger would bring together all of the tools of effective border and immigration enforcement – Inspectors, Border Patrol Agents, Special Agents, Detection and Removal Officers, and Intelligence Analysts – and realize the objective of creating a single border and immigration enforcement agency. Eliminating BTS would remove a middle management layer allowing the combined CBP-ICE to report directly to the Secretary via the Deputy Secretary. Insofar as we have not studied the implications that such a reorganization would have on the department's border security initiatives, we are not in a position to address the pros and cons of such a reorganization.

The third organization within BTS that plays a major role for protecting the borders of the U.S. and safeguarding its transportation infrastructure is the Transportation Security Administration (TSA). TSA's primary security improvements have focused on aviation, with the hiring of over 60,000 passenger and baggage screeners, installing electronic passenger and baggage screening technology at the nation's airports, and greatly expanding the Federal Air Marshals Program, which is now organizationally located in ICE.

Other organizations within BTS have border security related responsibilities as well, such as the US-VISIT Program Office and the Federal Law Enforcement Training Center (FLETC). The US-VISIT Program Office is responsible for the development and fielding of the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). FLETC, also a BTS component, provides career-long law enforcement training to 81 federal partner organizations and numerous state, local, and international law enforcement agencies.

Also, although not organizationally housed within BTS, the U.S. Citizenship and Immigration Services (USCIS) plays an important part in DHS border security. USCIS is responsible for reviewing and approving applications for immigration benefits. While not a law enforcement agency, USCIS ensures that only eligible aliens receive immigration benefits and identifies cases of immigration benefit fraud and other immigration violations that warrant investigation.

Needless to say, DHS faces several formidable challenges in securing the nation's borders. Our audit and inspection program has attempted to address some of the challenges. These include: developing effective overseas operations; preventing terrorist weapons from entering the U.S.; and tracking the entry and exit of foreign visitors.

International Operations

As the Heritage Foundation's report aptly pointed out, our nation's homeland security does not stop at America's geographic borders. DHS faces international challenges in protecting our borders. Provisions in the visa issuance process and other programs to promote international travel create potential security vulnerabilities that may allow terrorists, criminals, and other undesirables to enter the U.S. undetected.

For example, DHS must address security concerns identified in the Visa Waiver Program (VWP). The VWP enables citizens of 27 countries to travel to the U.S. for tourism or business for 90 days or less without obtaining a visa. These travelers are inspected at a U.S. POE, but have not undergone the more rigorous background investigations associated with visa applications. In an April 2004 Inspection, we reported our concerns regarding the exclusion from the US-VISIT program of travelers under the VWP. In September 2004, BTS began requiring travelers from VWP countries to enroll in the US-VISIT program, and renewed its efforts to conduct required country reviews.

However, DHS continues to experience problems in identifying and detecting aliens presenting lost and stolen passports from VWP countries at ports of entry. Shortcomings in procedural and supervisory oversight permitted some aliens presenting stolen Visa Waiver Program passports to enter the United States even after their stolen passports were reported, watch-listed, and detected. New information on lost and stolen passports provided by Visa Waiver Program governments was not routinely checked against U.S.

entry and exit information to determine whether the stolen passports have been used to enter the U.S. In addition, there was no formal protocol for providing information concerning the use of stolen passports to ICE for investigation and apprehension of the bearer.

In addition, lost and stolen passport problems are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify *mala fide* travelers using stolen Visa Waiver Program passports even when the theft has been reported and the information is available in DHS lookout systems. This occurs because stolen passports are reported using the passports' inventory control numbers (ICNs), which are entered into the lookout systems. However, inspectors routinely enter just the passports' issuance numbers into the lookout systems, and therefore do not match the reported stolen ICNs, resulting in undetected stolen passports. While we applaud BTS' efforts to promote a change in the International Commercial Aviation Organization (ICAO) standard to a one-number passport system, it will take years once the new standard is adopted for the two-number passports to be removed from service. Interim measures are needed to reduce this vulnerability. In response to our concerns regarding the use of stolen Visa Waiver Program passports to enter the United States, BTS has taken steps to conduct systematic reviews of admission records to check for previous uses of newly stolen passports.

Further, DHS also must address issues identified with its visa security program, which stations DHS officers at U.S. embassies and consular offices overseas to review visa applications and perform other law enforcement functions. Because of its limited resources, BTS used temporary duty officers who often did not have the required background or training, including language skills, to perform effectively as visa security officers. For example, nine of the ten temporary duty officers who have served or are serving in Saudi Arabia did not read or speak Arabic. This limits their effectiveness and reduces their contribution to the security of the visa process. In response to our report, BTS advised that it would: stop using temporary duty officers and begin using permanently assigned officers at its visa security offices; develop a staffing model to ensure only qualified officers serve in these positions; and develop a training program for visa security officers. While BTS agreed with us in principle regarding the need for language training, BTS officials said that, because of funding concerns, it would provide language training "as necessary and to the extent possible."

As a result, the full intelligence and law enforcement value that Visa Security Officers could add to the existing inter-agency country teams has not been achieved. In response to our report, DHS advised that it has developed a near-term plan for deploying visa security officers for FY 2005 and was planning for additional deployments.

With respect to international travelers, two major border security challenges confront the department: the divergency in the biometric systems used to identify travelers, and the substantial differences in the levels of scrutiny given to different classes of travelers.

Biometric Systems. We have all seen the glaring deficiencies of name-based lookout lists: for every known terrorist there are many innocent people with the same name. And for every name, there are variants and misspellings. Biometric identifiers are the only reliable and practical way to tell people apart.

The FBI uses ten rolled fingerprints in the IAFIS to document criminal activities. The former INS, now within DHS, used only two index finger prints to create retrievable records for travelers in its Automated Biometric Identification System (IDENT). As has been widely reported, the two systems have not yet been integrated, so some travelers are run through one system, and then sometimes the other, at ports of entry. The CBP agents are required to check both systems when possible illegal aliens are apprehended.

The international standards for passports are developed through ICAO. The United States is one of several countries whose citizens are not routinely fingerprinted for licenses or identification cards. In the past, the U.S. has lobbied ICAO to use facial recognition rather than fingerprints as the required primary biometric identifier in passports. Public accounts suggest that the experiments to date using facial recognition (at Logan Airport, among others) yielded meager results. At our borders, meanwhile, we increasingly rely upon fingerprint scans to tell people apart. The difficulties in achieving international consensus on this subject are daunting. More daunting and far more obvious, however, is the fact that the United States cannot afford to implement both biometric capabilities at each port of entry, it must settle on one. We – the United States Government – need to decide soon which biometric is the most reliable. Then we need to apply that standard to our own identity and travel documents, as well as for foreign travelers. We cannot do this in a vacuum, however; we need international cooperation to establish a global standard.

Levels of Scrutiny. The second challenge relates to the inconsistent levels of scrutiny to which travelers are subjected. Everyone knows that some nonimmigrants need visas, but many do not. Less well known is that some do not even require passports. Immigrants, some of whom spend little time in the U.S., receive medical examinations and background checks, but nonimmigrants, some of whom remain legally for many years, do not.

Usually, travelers from visa waiver countries do not require visas, but, depending on the claimed purpose of their trip, they sometimes do. Most citizens of Canada and Mexico do not need visas or passports to enter the United States, and we do not always record their names, or check them against our databases, though we do check their automobile license plates at land POEs. During FY 2002, 104 million visa exempt Mexicans constituted 24 percent, and 52 million visa-exempt Canadians constituted 12 percent, of all admissions.

U.S. citizens reenter the country with the least scrutiny of all, and frequently require no passport. Foreign travelers who can successfully pretend to be Americans get the same special treatment, of course, as documented by the GAO in its May 2003 report,

"Counterfeit Documents Used to Enter The United States From Certain Western Hemisphere Countries Not Detected" (03-713T).

The US-VISIT system screens only nonimmigrants with visas, or visitors using the provisions of the Visa Waiver Program. According to fiscal year 2002 statistics, the approximately 15 million VWP visitors accounted for 3 percent of U.S. admissions, while 19 million travelers with nonimmigrant visas accounted for 5 percent. In essence, US-VISIT screens fewer than 9 percent of the people entering the United States. At land borders, where travelers with visas or using the VWP are a rarity, the percentage of crossers screened by US-VISIT is also very small: less than 3 percent.

No one designing a border security system from the ground up would create such a hodge-podge of processes with so many potential security gaps. If we are to be serious about border security, we will need to rationalize our border crossing processes. People are not always who they claim to be, and terrorists and criminals will try to assume whichever false identity will get them the least scrutiny as they enter and depart our country.

Preventing Terrorist Weapons from Entering the U.S.

Since September 11, 2001, CBP's priority mission is detecting and preventing terrorists and terrorist weapons from entering the U.S. A major component of its priority mission is to ensure that oceangoing cargo containers arriving at the seaports of entry are not used to smuggle illegal and dangerous contraband. To test controls over importing weapons of mass destruction, ABC News was successful in two attempts at smuggling depleted uranium into the country. On September 11, 2002, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium was shipped from Europe to the U.S. undetected by CBP. On September 11, 2003, ABC News reported that the same cylinder was smuggled to the U.S. from Jakarta, Indonesia, again undetected.

In the first smuggling event, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium, which was shielded with lead, was placed in a suitcase and accompanied by ABC News reporters by rail from Austria to Turkey. In Istanbul, Turkey, the suitcase was placed inside an ornamental chest that was crated and nailed shut. The crate containing the suitcase was then placed alongside crates of huge vases and Turkish horse carts in a large metal shipping container, and then loaded onto a ship that left Istanbul. Based on data contained in the Automated Targeting System, the crate was targeted as high-risk for screening by the U.S. Customs Service (Customs). ABC News broadcast on September 11, 2002, that Customs failed to detect the depleted uranium carried from Europe to the U.S.

During the second smuggling event, ABC News placed the same cylinder of depleted uranium into a suitcase, and then placed the suitcase into a teak trunk. The trunk, along with other furniture, was loaded into a container in Jakarta, Indonesia, and then transshipped to the U.S. from Tanjung Pelepas, Malaysia. This shipment was also

targeted as high-risk for screening and subsequently inspected by CBP personnel, but was then allowed to proceed from the port by truck.

In a classified September 2004 report, we cited several weaknesses that occurred at the time of the two incidents that made the container inspection process ineffective. The protocols and procedures that CBP personnel followed at the time of the two smuggling incidents were not adequate to detect the depleted uranium. CBP has since enhanced its ability to screen targeted containers for radioactive emissions by deploying more sensitive technology at its seaports, revising protocols and procedures, and improving training of CBP personnel.

During FY 2005, we plan to conduct a follow-up audit on the issue of radiation detection. The audit will determine to what extent CBP has a complete and workable plan for deploying and effectively operating radiation portal monitors at major U.S. seaports, and how the new technologies that CBP is deploying will impact operations at the ports.

Tracking the Entry and Exit of Foreign Visitors

Keeping track of people entering and leaving the U.S. is necessary to prevent terrorism, narcotics smuggling, and illegal alien smuggling, and to enforce trade laws and collect revenue, all while facilitating international travel. Over the next five years, DHS will invest billions of dollars to modernize the passenger processes and systems inherited from the legacy agencies, including the US-VISIT system. Concerted efforts are now being made to realign certain operations and systems within the newly created DHS.

However, DHS did not conduct an analysis and reexamination of its strategy, processes, technology, and organization for the overall federal passenger processing requirements, i.e., business-process reengineering, before proceeding with US-VISIT. Further, DHS did not have an overall modernization acquisition strategy for the legacy Customs, INS, TSA, and APHIS systems related to passenger processing. An acquisition strategy based on a re-engineered vision of how DHS will process international travelers, in alignment with the department's enterprise architecture, should result in better and more definitive contract requirements.

We recommended that BTS initiate a business process reengineering effort to establish a clear vision of the overall federal operations that will be used to clear people entering and leaving the U.S., and based on the results, work with the Chief Acquisition Officer (CAO) and Chief Information Officer (CIO) to develop an overall departmental acquisition strategy for passenger information technology systems. BTS advised that it plans to initiate a business process reengineering effort, and develop an overall department acquisition strategy in coordination with the CAO and CIO.

Finally, in a report issued in June 2004, we raised concerns about the Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program. This program permits pre-screened and enrolled low risk travelers to enter the U.S. from Mexico in designated lanes with minimal inspection by CBP officers, thereby avoiding the lengthy waiting

times in the regular inspection lanes. The SENTRI program is open to both U.S. citizens and certain non-citizens. We determined that the program is generally achieving the two basic objectives for which it was established: accelerating the passage of participating travelers through land ports of entry; and maintaining border integrity, security, and law enforcement responsibilities.

However, we noted inconsistencies in the way land ports of entry applied eligibility criteria for criminal offenses, financial solvency, and residency, and approved or denied applications. In addition, we noted weaknesses in the procedures by which SENTRI system records are kept current, and how alerts are disseminated to CBP officers. Taken as a whole, our findings indicate weak program management that could jeopardize the program's integrity and border security. In response to these concerns, CBP has moved to merge all of its trusted travelers programs and centralize the enrollment process to standardize enrollment procedures and criteria.

TRANSPORTATION SECURITY

DHS faces significant challenges in ensuring the security of the nation's transportation systems. TSA and the Coast Guard spearhead the department's transportation security efforts. While TSA has made progress in implementing the Aviation and Transportation Security Act (ATSA) and securing the nation's airways, improvements are still needed in aviation, rail, and transit security. Similarly, the Coast Guard has made progress in securing the nation's maritime transportation system, but the deteriorating condition of its aircraft and cutter fleets places the Coast Guard's current and future mission performance at risk.

Aviation Security

The success of TSA in fulfilling its aviation security mission depends heavily on the quality of its staff and the capability and reliability of the equipment to screen passengers and cargo to identify terrorists and terrorists' weapons, while minimizing disruption to public mobility and commerce.

Personnel. Providing qualified and trained personnel has been a substantial challenge for TSA. ATSA mandated that the TSA hire and train thousands of screeners for the nation's 429 commercial airports by November 19, 2002. As a result, TSA hired over 60,000 screeners. Our undercover audits of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports, or do not enter the checked baggage system. Also, the ability of TSA screeners to stop prohibited items from being carried through the sterile areas of the airports fared no better than the performance of screeners prior to September 11, 2001. We attributed the test failures to four areas that were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA is enhancing its screener training programs along with management and supervision of screener activities. We are

currently evaluating TSA's revised training programs and will continue to monitor TSA's progress in improving screeners' performance. We plan to complete another round of undercover tests within the next 2 months.

Equipment. Providing capable and reliable equipment has also been a substantial challenge for TSA. TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives detection systems. However, deployment of the equipment does not ensure effective security. We reported that TSA has not resolved some of the problems that arise when explosive detection equipment breaks down, there are workforce shortages, or high baggage volume overloads the system. Fallback alternatives are inconsistently applied and inadequately controlled, leaving gaps in the screening process.

Furthermore, TSA has come under criticism for not moving quickly enough to address the vulnerability of the nation's air traffic to suicide bombers. For example, the 9-11 Commission recommended that TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. TSA is in the process of testing several of these technologies, including backscatter x-ray, vapor detection, and document scanner machines, to address concerns regarding detection of explosives on individuals. Until these advanced technologies are tested and deployed, TSA has instituted a process of more extensive pat-down procedures to find explosives hidden on a traveler. The use of these more thorough examination procedures have been protested by travelers and interest groups, and have already been refined by TSA. We are currently reviewing the implementation of these procedures to ensure they are strictly followed, as well as TSA's process for responding to passenger complaints.

TSA is currently piloting explosives trace detection document scanners at four airports to assess the viability and effectiveness of the technologies. We are monitoring TSA's progress regarding these issues as well as reviewing TSA's process for screening air cargo.

Rail and Transit Security

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across the other modes of transportation. About 6,000 agencies provide transit services through buses, subways, ferries, and light-rail services to about 14 million Americans. Madrid's and Tokyo's terrorist experiences highlight potential vulnerabilities in transit systems. Recently, several congressional leaders expressed concern that the federal government has not taken strong enough action to respond to the threat to public transit. Furthermore, the 9/11 Commission reported that over 90% of the nation's $5.3 billion annual investment in TSA goes to aviation, and that current efforts do not yet reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits so that transportation security resources can be allocated to the greatest risks in a cost effective way. TSA's FY 2005 budget still focuses its resources on aviation.

TSA has lead responsibility for coordinating the development of a transportation sector plan, which is expected to be completed later this year. TSA, however, has not finalized the memoranda of understanding with various Department of Transportation agencies to determine how they will coordinate work in the future. We are evaluating TSA's actions to assess and address potential terrorist threats to the mass transit systems of major U.S. metropolitan areas.

Maritime Security

The Coast Guard's willingness to work hard and long hours, use innovative tactics, and work through partnerships in close inter-agency cooperation has allowed it to achieve mission performance results goals. However, to improve and sustain its mission performance in the future, the Coast Guard faces significant barriers, most importantly the deteriorating readiness of its fleet assets. The Coast Guard faces three major barriers to improving and sustaining its readiness to perform its legacy missions:

1. The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance.

2. The workload demands on the Coast Guard will continue to increase as it implements the Maritime Transportation Security Act of 2002 (MTSA). This complex work requires experienced and trained personnel; however, the Coast Guard has in recent years suffered from declining experience levels among its personnel.

3. Sustaining a high operating tempo due to growing homeland security demands, such as added port, waterway, and coastal security patrols, will tax the Coast Guard's infrastructure including its aging cutter and aircraft fleet.

The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to define a performance management system that includes all the input, output, and outcomes needed to gauge results and target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crises or major terrorist attacks. For example, for search and rescue, the number of mariners in distress saved is a good indicator of outcome; however, resource hours under-represent the effort put into this mission by omitting the many hours of watch standing at stations. Without more complete information, the Coast Guard has limited ability to identify and target cost effective improvements to mission performance.

The workload demands on the Coast Guard will continue to increase as it implements the MTSA. Under MTSA, the Coast Guard must conduct risk assessments of all vessels and facilities on or near the water; develop national and area maritime transportation security plans; and approve port, facility, and vessel security plans. This complex work requires

experienced and trained personnel, presenting a major challenge for the Coast Guard, which has in recent years suffered from declining experience levels among its personnel. Since the Coast Guard largely relies on experienced senior personnel to coach and train junior personnel and new recruits on the job, mission performance is at risk.

In addition to implementing MTSA, growing homeland security demands, such as added port, waterway, and coastal security patrols, result in a continued high operating tempo. Sustaining this high operating tempo will be a major challenge for Coast Guard personnel and will tax its infrastructure, especially its aged cutter and aircraft fleet. The Coast Guard reported that mission sustainment is at risk due to cutters and aircraft that are aging, technologically obsolete, and require replacement and modernization. Currently, the Coast Guard is experiencing serious cracking in the hulls of the 110 foot cutters and engine power loss on the HH-65 Dolphin helicopters, resulting in operating restrictions. These problems adversely affect the Coast Guard's mission readiness and ultimately mission performance.

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

As an example, the number of in-flight loss of power mishaps involving the HH-65 helicopter grew from about a dozen mishaps annually before September 11, 2001, to more than 150 in FY 2004, requiring the immediate re-engining of the entire HH-65 fleet. The Coast Guard recently accelerated its acquisition of the Multi-Mission Cutter Helicopter under development by the Integrated Deepwater System acquisition project, in addition to initiating engine replacement for its HH-65 helicopter fleet. Also, in 2003, the Coast Guard experienced 676 unscheduled maintenance days for its cutters—a 41% increase over 2002. This was the equivalent of losing the services of over three and a half cutters. These lost cutter days include the coastal patrol boats that are suffering from accelerated hull corrosion and breached hull casualties.

INTEGRATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components into a single, effective, efficient, and economical department remains one of DHS' biggest challenges. To meet this challenge, DHS, among other things, established an Operational Integration Staff to assist departmental leadership with the integration of certain DHS missions, operational

activities, and programs at the headquarters level and throughout the DHS regional structure

In any event, much remains to be done in integrating DHS programs and functions, and we have reported that structural and resource problems continue to inhibit progress in certain support functions. For example, while the department is trying to create integrated and streamlined support service functions, most of the critical support personnel are distributed throughout the components and are not directly accountable to the functional Line of Business (LOB) Chiefs, i.e., the Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO), Chief of Administrative Services (CAS), and Chief Procurement Officer (CPO).

In August 2004, the Secretary and Deputy Secretary directed the DHS LOB Chiefs to design and implement systems that will optimize their functions across the entire department. The LOB chiefs were also instructed to develop Management Directives to guide the department's management of those business functions. The Directives were to be built on a concept of "dual accountability," where both the operational leadership and the LOB chiefs are responsible for the successful preparation of the Directives and their ensuing implementation. This concept has been described as a "robust dotted line" relationship of agency or component functional heads to the LOB chiefs for both daily work and annual evaluation. Final Management Directives were signed by the Secretary in October 2004 to institutionalize the arrangements before FY 2005. In addition, the department's Management Council signed charters for each LOB that establish a formal governance and advisory board structure to ensure that the objectives and intent of the Directives are executed.

While the concept underlying the Management Directives may be workable in some environments, we have concerns that the DHS LOB chiefs may not have sufficient resources or authority to ensure that department-wide goals and challenges in their respective LOBs are addressed effectively, efficiently, or economically, or that available resources can be marshaled to address emerging problems. These concerns were heightened by the department's experience this past fiscal year in reorganizing the former Immigration and Naturalization Service (INS) and the U.S. Customs Service into three new bureaus – Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS), referred to as the "tri-bureaus" – and the consolidation of accounting services for many small programs from outside of DHS into ICE. However, the department and ICE did not prepare a thorough, well-designed plan to guide the transition of accounting responsibilities within ICE. ICE fell seriously behind in the performance of basic accounting functions, such as account reconciliations and analysis of abnormal balances. The pervasiveness of errors in ICE's accounts prevented the auditors from completing their work at ICE for the FY 2004 DHS financial statement audit.

The department also faces a structural problem in its financial management organization. The bureaus control most of DHS' accounting resources, but the DHS Chief Financial Officer (CFO) has responsibility for DHS' consolidated financial reporting, which is

dependent on those resources. Although coordination mechanisms are in place, monitoring controls at the DHS CFO's level are insufficient to ensure the accuracy of consolidated financial information. The seriousness of the material weaknesses and reportable conditions at DHS demands strong DHS CFO oversight and controls.

Similarly, creating a single infrastructure for effective communications and information exchange remains a major management challenge for DHS. We reported in July 2004, that the DHS CIO is not well positioned to meet the department's IT objectives. The CIO is not a member of the senior management team with authority to strategically manage department-wide technology assets and programs. No formal reporting relationship is in place between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for his central IT direction. Further, the CIO has limited staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-making and a reliance instead on cooperation and coordination within DHS' CIO Council[1] to accomplish department-wide IT integration and consolidation objectives. The department would benefit from following the successful examples of other federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on department-wide IT investments and strategies.

We will be monitoring and evaluating the progress made in each LOB area very closely, not only during FY 2005, but also for years to come.

INTELLIGENCE

Under the Homeland Security Act of 2002,[2] the department is responsible for receiving, integrating, and coordinating the sharing of federal information to help ensure border security and protect the U.S. from terrorist threats. Specifically, the Homeland Security Act of 2002 gave DHS significant responsibility to coordinate the sharing of information to protect the U.S. from terrorist threats. The law requires the DHS Under Secretary for Information Analysis and Infrastructure Protection (IAIP) to consult with the Director of Central Intelligence and other appropriate intelligence, law enforcement, or other elements of the federal government to establish collection priorities and strategies for information relating to threats of terrorism against the U.S.[3] The law also directs the IAIP Under Secretary to review, analyze, and make recommendations to improve the policies and procedures governing the sharing of law enforcement, intelligence, intelligence-related, and other information relating to homeland security.[4]

---

[1] The DHS CIO Council is comprised of the CIOs from each DHS component, ex officio representatives from General Counsel, the Chief Financial Officer's Council, the Office of the CIO, and the Executive Procurement Executive Council. The CIO Council was chartered to develop, promulgate, implement, and manage a vision and direction for information resources and telecommunications management within DHS.
[2] Public Law 107-296 (Nov. 25, 2002), codified at 6 USC 101 *et seq.*
[3] 6 USC 121 (d)(10).
[4] 6 USC 121 (d)(8).

However, with the creation of the Terrorist Threat Integration Center under the Director of Central Intelligence and the Terrorist Screening Center under the Director of the FBI, the role and responsibilities of IAIP for intelligence collection, analysis, and dissemination has been abated. Creation of the new Director of National Intelligence position makes the DHS intelligence coordination role even more uncertain, calling for prompt clarification of federal lines of authority in this area.

In a recent memorandum, the IAIP Under Secretary provided us an update on several actions being taken, which he believes will largely clarify some of these issues. Specifically, the IAIP Under Secretary said that the department has been fully supportive and involved in the development of a *Terrorist-Related Screening Procedures Strategy Report*, and a *Terrorist-Related Screening Procedures Investment and Implementation Plan* pursuant to Homeland Security Presidential Directive – 11.

The recommendations from the strategy report were forwarded to the President in November 2004. The end result of such actions, the IAIP Under Secretary concluded, would be intra-agency watch list coordination and consolidation, a high-level review of terrorist information sharing activities, and a cohesive and coordinated federal screening program. We will continue to monitor progress in carrying out these activities to determine the extent to which they provide for a cohesive and coordinated federal screening and information sharing program.

PREPAREDNESS

Our office focused, so far, on examining the programs and mechanisms that enhance preparedness at the federal, state, and local levels of government, including the utility of IAIP data on port security grant award decisions. In its December 2004 report, the Heritage Foundation recommended consolidating DHS critical infrastructure protection, preparedness, and state/local/private coordination efforts under an Undersecretary for Protection and Preparedness. According to the Foundation, consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state/local/private sector entities on securing those vulnerabilities and preparing for attacks, and make grants to help get the job done and to induce cooperation. Again, on the surface, this proposal appears to have merit. However, insofar as we have not studied the implications of this proposal, we are not in a position to address the pros and cons of such a consolidation. Nevertheless, we do have reservations about segregating FEMA's preparedness functions from its response and recovery responsibilities. Disaster preparedness, response, and recovery are intricately related, each relying on the other for success. This proposal should be carefully studied before it is put into practice.

Infrastructure Protection

One of the significant challenges facing the new Secretary is the need to base the department's business decisions, such as its grant awards, on information relating to nationally critical infrastructure and key assets. We learned from two surveys completed in 2004 and a more recent review of DHS' Port Security Grant Program, which we will issue shortly, that the department lags in integrating critical asset data and its "preparedness" initiatives into its business decisions. Also in 2004, we concluded that if IAIP did not produce a condensed list of most sensitive critical assets, other elements within DHS would be at risk of failing to direct their grant resources toward national critical infrastructure protection and preparedness. This concern materialized in port security grant awards: administrators designed and operated the program as a sector-specific grant program and conducted at least three rounds of grants, totaling $560 million, without definitive national priorities for securing the seaport infrastructure of the nation. Poor integration of critical asset information meant that port security grant award decisions were made without sufficient information about our national priorities. DHS components need to strengthen their working relationships with IAIP, which has primary responsibility within DHS for critical asset identification, prioritization, and protection. The department's investments in new technologies, systems, and grant-making programs must reflect national priorities as determined by IAIP's risk management activities.

Also, a lack of coordination between the Science and Technology Directorate (S&T) and other DHS components slowed S&T's long term plan to invest in threat vulnerability and risk assessment tools. S&T is required to coordinate with other executive agencies, particularly those within DHS, to (1) develop an integrated national policy and strategic plan for identifying and procuring new technologies, (2) reduce duplication and identify unmet needs, and (3) support IAIP in assessing and testing homeland security vulnerabilities and possible threats. TSA, the Coast Guard, and IAIP have developed risk assessment tools and performed analyses of critical infrastructure. It is critical for the S&T to have a clear understanding of the terrorist threat picture facing the nation and the current technical capabilities and ongoing research and development initiatives of other DHS elements. To be effective, it must be able to prioritize its investment decisions, and avoid duplicating technology initiatives by other DHS components, especially in the area of risk assessment. To that end, the extent that the new Secretary oversees these efforts and makes intra-agency coordination a reality, will determine his effectiveness in ensuring that DHS' investments are adequately matched to risk.

We are seeing signs that IAIP is becoming more involved in risk assessment activity and grant decision-making across the department and agencies are increasingly seeking assistance from IAIP. S&T has intensified efforts to obtain terrorist threat information from IAIP and incorporate it into S&T's selection of new technologies. The Coast Guard is working closer with IAIP on maritime risk assessments and programs. Grant officials signaled their intention to consult IAIP and make better use of critical infrastructure information in future rounds of port security grants.

The new Secretary needs to ensure that this progress continues and becomes a regularized part of DHS's business decision-making. DHS components must share information, assimilate data to better coordinate risk management activities, and subscribe to a single concept of national priorities and interests. These actions are the foundation of solid business judgments now and in the future. Without this leadership, DHS risks having multiple, confusing, and possibly conflicting sources of priority for its investments.

State and Local Grant Programs

In March 2004, we reported on the distribution and expenditure of grant funds targeted for "first responders" in state and local jurisdictions. We reported that a slow rate of expenditure was due primarily to delays at the state and local level. In some cases, grantees delayed spending funds until they completed risk and strategy assessments that would enable them to spend the money more effectively.

We are currently reviewing preparedness issues through a series of ongoing audits. We are reviewing the effectiveness of state homeland security risk assessment and preparedness strategy processes. We are also reviewing the National Response Plan, to determine whether DHS has fully coordinated the National Response Plan with its state and local government and private sector partners; the plan meets the expectations of an all-hazards all-disciplines plan; and training and exercises are sufficient to fully implement the plan. Further, since July 2004, an OIG team has worked with DHS on a review of TOPOFF-3, the third and much expanded preparedness and response exercise involving top federal, state, and local officials and first responders.

We are also reviewing the Urban Search and Rescue Response System Preparedness Program. The objectives of this audit are to determine whether: the system's defined goals that relate to preparedness are being achieved; preparedness funding is having the intended effect on the system's capacity to respond to major disasters or emergencies; and there are opportunities for improvements in the program.

Finally, we are auditing state and local spending of First Responder Grant Funds. Our audit will determine whether: state and local jurisdictions are spending their first responder grant funds according to regulations and grant requirements; controls are adequate to ensure proper spending of grant funds; and program goals are being achieved.

Madam Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the members may have.

# # #