STATEMENT OF CLARK KENT ERVIN

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS

SUBCOMMITTEE ON FINANCIAL MANAGEMENT, THE BUDGET, AND INTERNATIONAL SECURITY

UNITED STATES SENATE

JULY 8, 2004

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to be here today to discuss the FY 2003 financial statement audit at the Department of Homeland Security (DHS) and ways to improve the financial management and accountability of DHS. My remarks will focus on financial accounting and reporting, revenue collection, contract management, grants management, and information technology.

On March 1, 2003, almost 180,000 employees and 22 disparate agencies combined to form DHS in one of the largest government reorganizations ever. The reorganization had elements of a merger, divestiture, acquisition, and startup. Notably, the General Accounting Office (GAO) designated the implementation and transformation of DHS as a "high risk" because of the size and complexity of the effort, the existing challenges already faced by the incoming components, and the importance of DHS' mission. GAO also noted that successful transformations of large organizations under even less complicated situations could take from 5 to 7 years.

Since the department's formation it has made noteworthy progress in the integration of legacy agencies and the development of department-wide functions. Still, there is much to be done, including needed improvements in DHS financial operations.

Financial Accounting and Reporting

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. Further, DHS was presented with the challenge of preparing its first set of financial statements for audit, and met that challenge under difficult circumstances.

The Office of Inspector General (OIG) engaged KPMG LLP (KPMG), to complete an audit of DHS' financial statements as of September 30, 2003, and for the seven months then ended, as required by the Accountability of Tax Dollars Act of 2002. Despite limited staff with many other responsibilities, DHS officials ultimately agreed to accept the challenge of a financial statement audit even though it added strain to 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:

(1) 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;

(2) KPMG's inability to observe a sufficient number of the 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

(3) 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 Coast Guard became a larger bureau relative to its parent 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 since obtained an 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 Immigration and Naturalization Service (INS), the Federal Emergency Management Agency (FEMA), and the Transportation Security Administration (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) needed 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 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 $3.3 billion in 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 Bureau of Customs and Border Protection's (CBP) accounting system lacked automated controls to detect and prevent excessive drawback claims and payments.

- Import Entry In-bond: CBP did not have a reliable process of monitoring the movement of "in-bond" shipments -- i.e., merchandise traveling through the U.S. that is not subject to duties, taxes, and fees until it reaches a port of destination. 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 Bureau of Citizenship and Immigration Services' (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 standard operating procedures 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 and the Bureau of Immigration and Customs Enforcement (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 department's 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*.

Compliance with Laws and Regulations

For agencies subject to the Chief Financial Officers' Act (CFO Act), the Federal Financial Management Improvement Act (FFMIA) requires financial statement auditors to report on compliance with it. DHS is not subject to the CFO Act, and, consequently, FFMIA; therefore, KPMG did not directly report on DHS' compliance with FFMIA. However, KPMG did report significant deficiencies in the three key areas of FFMIA: financial management systems, the application of federal accounting standards, and the recording of financial transactions at the U.S. standard general ledger level. Based on these deficiencies, if DHS were subject to FFMIA, the Office of Inspector General (OIG) would have concluded that DHS was not in substantial compliance with FFMIA. Specific areas of non-compliance are described within the material weaknesses and reportable conditions already cited.

DHS had not implemented procedures to ensure accuracy and completeness in its reporting process for the Federal Managers' Financial Integrity Act (FMFIA). FMFIA, as implemented by OMB Circular A-123, *Management Accountability and Control*, requires agencies to report on an annual basis material weaknesses in their controls and plans to correct those weaknesses. KPMG noted that DHS did not report some material weaknesses identified in the *Independent Auditors' Report*, nor corrective actions plans for all material weaknesses. KPMG also noted some timeliness and consistency issues between the bureaus and DHS headquarters.

KPMG found weaknesses across DHS in its entity-wide information security program management and in controls over system access, application software development, system software, segregation of duties, and service continuity. These weaknesses represent instances of non-compliance with the Federal Information Security Management Act, which requires agencies to provide information security for their systems. Because of the importance of system security, I am providing more details of these findings later in this testimony.

KPMG also noted that certain cost-share analyses and follow-up were not performed when the percentage of cost share funds paid/unpaid was greater than 20 percent. This is required under OMB Circular A-133, subpart D – *Federal Agencies and Pass-Through Entities* and Appendix B, *Compliance Supplement*.

Corrective Action Plans

Because DHS is not subject to FFMIA, it is not required to submit an FFMIA mandated remediation plan to OMB. However, DHS has a corrective action plan covering all of the bureaus that, we are told, is near completion. Many of these weaknesses will not be fully addressed until the department and its bureaus implement information technology (IT) system solutions. OIG will be working closely with DHS officials to ensure that remedial actions are timely and complete.

Audit Challenges Faced in 2003

The challenges of this audit were several. First, the mid-year and mid-quarter creation of DHS made it difficult to get good cut-off balances as of March 1, 2003; that is, beginning balances for DHS. Beginning balances are needed to audit successfully activity over a period of time. Many of DHS' bureaus had to reconstruct their balance sheets as of March 1, 2003, which was outside of their normal reporting periods. The bureaus mostly succeeded in this task; however, in the case of the Coast Guard, difficulties in conducting the audit, as described in the next paragraphs, caused KPMG to run out of time to complete its audit procedures in this area. This was a contributing factor to KPMG's inability to opine on the DHS' consolidated statement of net cost and changes in net position, combined statement of budgetary resources, and consolidated statement of financing, which I will refer to as "activity statements" for the purpose of this testimony. One of the results of this beginning balance work, though, is that it helped the bureaus and programs ensure a more complete and accurate documentation of the transfer of assets, liabilities, and budgetary authorities into DHS, which were then compared for consistency with transfers out by the legacy agencies.

Second, the Coast Guard is proportionally a larger bureau within DHS compared to the Department of Transportation, its legacy parent department. This brought with it proportionally more scrutiny during our audit, something for which the Coast Guard was not fully prepared. Its financial reporting processes were inefficient and complex. Because the Coast Guard had never received an audit opinion on its own financial statements (although its financial information received audit coverage specific to its legacy department's financial statement audit), auditing standards required KPMG to test certain Coast Guard balances related to prior years. The Coast Guard had not maintained certain documentation needed to support the valuation and existence of PP&E in the net amount of $2.9 billion out of total net balance of $9.1 billion at the DHS consolidated level. Much of the $2.9 billion related to PP&E acquired prior to 1996, just when departments were starting to implement reform legislation requiring audited financial statements. Nevertheless, auditing standards required us to seek objective evidence, including estimates using documented and acceptable methodologies, to support this

balance. Because the Coast Guard could not provide sufficient documentation, KPMG qualified its opinion on the balance sheet for the $2.9 billion.

The Coast Guard also had significant weaknesses related to OM&S. The Coast Guard maintains OM&S primarily as inventory to support its fleet of ships and aircraft. Because of poor controls at field sites over physical counts (procedures that verify the existence and completeness of inventory), KPMG could not validate the valuation of $497 million out of $1.2 billion net OM&S, inventory, and stockpile balance at the DHS consolidated level. Auditing standards require auditors to observe physical counts of inventories as part of its validation procedures. KPMG attempts to observe inventory procedures were made difficult in some cases because of ships being out to sea, or the Coast Guard being unable to resolve differences between the physical counts and the accounting records.

Third, financial reporting at the consolidated level in particular was a challenge. Although the large bureaus came into DHS with financial reporting mechanisms in place, those processes had to be created at the consolidated level. DHS was fortunate to be able to use the Department of the Treasury's *Treasury Information Executive Repository* (TIER), a data warehouse that collects DHS bureaus' financial information, interfaces with other software, and supports preparation of DHS consolidated and individual bureau financial statements. Difficulties in using TIER, however, prevented DHS from preparing timely and accurate periodic consolidated financial statements. Most bureau financial systems were not electronically interfaced with TIER, and bureaus had to configure their systems and processes to meet TIER submission requirements. As a result, errors occurred. TIER is a temporary system solution until a permanent financial reporting system architecture for DHS can be developed and implemented.

The OCFO is responsible for the preparation of consolidated financial statements using TIER. The OCFO operated with relatively few finance personnel, who principally served to coordinate financial management policy and consolidate financial information submitted by the bureaus. The OCFO had not established a hierarchy of financial reporting authority, or an entity-wide financial management organization chart that clearly defined roles and responsibilities and assisted with the identification of critical human resources needed to ensure that all financial management responsibilities were assigned. The OCFO had not developed SOPs that would result in consolidated financial reports that are consistent, timely, accurate, and in compliance with federal accounting standards. These conditions were not unexpected for a newly created organization, especially one as large and complex as DHS. Nevertheless, the problems associated with TIER, the lack of clear DHS-wide organizational roles and responsibilities and SOPs, and the insufficient number of qualified personnel or contractors at the OCFO would continue to make complying with financial reporting requirements difficult.

Audit Challenges for 2004

For FY 2004 OMB has accelerated the reporting deadline for audited financial statements and the *Performance and Accountability Report* to November 15, two and a half months

earlier than last year's deadline. Meeting this date will be a considerable challenge for DHS.

Many of the financial reporting challenges that DHS faces stem from its still recent creation from 22 disparate agencies. Although DHS has reduced the number of accounting service providers from 19 to 10, reporting processes remain complicated, and financial managers continue to spend considerable time on transitional issues.

One of the greatest transitional challenges DHS has faced this year is the realignment of back office functions at ICE, CBP, and CIS that took place at the start of FY 2004. Nine months into the fiscal year, many agreements regarding intra-bureau services that are being provided between the bureaus are not in place, leaving many accounting issues open. The CFO recently reported progress in this area, but time is short to clear up the accounting issues in this fiscal year. Also, as part of this realignment, ICE took over accounting responsibilities for several other DHS components, several of which were previously serviced by legacy agencies. This has taxed ICE's accounting resources, which already had been taxed by significant staff attrition in the last year.

As noted in last year's audit report, weaknesses in financial systems complicate the financial reporting process. There is not an integrated system to consolidate financial information from the bureaus, so in many instances a manual interface is necessary, and changes, corrections, and reconciliations are more difficult. Financial managers' time also has been taken up closing temporary accounts used in FY 2003 to help get DHS off the ground. Transitioning these accounts into permanent account structures is another task unique to DHS that has claimed a portion of its limited resources.

Because the *Performance and Accountability Report* was issued in February, DHS had little time to take corrective action on the material weaknesses and reportable conditions reported last year before it entered the FY 2004 audit cycle. To the extent that these weaknesses remain, they will continue to make preparation of the financial statements and the auditing of them more difficult. The accelerated reporting date requires a new audit approach that relies more heavily on internal controls and systems and earlier audit testing.

Another challenge for DHS is its cost accounting processes. The financial systems that DHS components brought with them from their legacy agencies were designed to summarize financial information for the purposes of those legacy agencies. Summarizing cost information by DHS' new priorities – its strategic goals – is very difficult, and makes compilation of DHS' Statement of Net Cost a challenge.

Finally, key milestones for this audit are approaching fast. July will be a crucial month because this is when balance testing must begin. It will be difficult for DHS and the auditors to overcome any significant problems that remain beyond July. The lack of sufficient staff, particularly in the OCFO and ICE, to deal with these problems and others that may arise is another of the major challenges DHS financial management faces.

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, the second largest revenue source after income taxes. 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. CBP estimated the revenue gap to be $170 million for FY 2003. However, the reliability of the compliance measurement data is questionable. OIG 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 inaccurate.

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 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:

(1) 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.;

(2) Revising its International Mail Operations and Enforcement Handbook to standardize operations at all IMBs, and;

(3) 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 U.S. Postal Service, CBP must work cooperatively with the Postal Service to ensure that all mail is delivered to CBP for inspection, and outstanding duties are collected from the Postal Service.

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. 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. A drawback is a remittance of duties, taxes, or fees previously paid by an importer, and 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. Also, 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. Also, drawback review policies do not require drawback specialists to review all related drawback claims against the associated entries to determine whether, in 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 risk of fraudulent claims or claims made in error is increased.

Also, CBP is responsible for collecting user fees from air passengers and commercial vessels arriving in the U.S. 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 for not collecting the fee.

To comply with the reporting requirements of the Aviation and Transportation Security Act (ATSA), CBP mandated the use of the 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/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 Fiscal Year 1998 and 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.

Contracts Management

A major challenge for DHS has been the identification and management of its procurements (the "procurement universe"). Although the department inherited procurement responsibility for 22 incoming organizations, only 7 procurement shops came into DHS. The remaining 15 components were receiving procurement services from organizations outside of the department, limiting the department's ability to apply effective and consistent oversight to its procurements. In addition, the Chief Procurement Officer has not been granted the authority to realign existing procurement resources to meet the procurement service needs of all 22 components better. Under these circumstances, the department has struggled even to prepare a detailed and accurate listing of its procurement universe. The data the department has received to date has come from 22 different sources and has not been independently validated. For example, FEMA discovered that it had not been reporting or tracking procurements let by its disaster field offices. Although efforts are under way to bring all department procurements under the umbrella of one comprehensive reporting system, data for fiscal years 2003 and 2004 have not been reported in detail sufficient to manage the procurement universe. DHS needs to integrate the procurement functions of its component organizations to ensure that good management controls are consistently applied.

Several of the incoming procurement organizations lacked important management controls. For example, during its first year of operation, TSA relied extensively on contractors to accomplish its mission, while providing little contract oversight. Contracts were written without clearly defined deliverables, were not modified to reflect changed circumstances, and, in some circumstances, TSA failed to provide a basis for assessing contractors' performance. As a result, the cost of some contracts ballooned. For example, TSA made major changes to its screener recruitment contract without performing trade-off studies or cost benefit analysis. The ceiling for that contract rose from $104 million

to $741 million. TSA also did not follow sound practices in awarding and administering a contract for the installation and maintenance of Explosives Detection Systems and Explosives Trace Detection Systems. As a result, TSA paid contract fees based on a percentage of total invoiced costs, which had the effect of creating a cost-plus-a-percentage-of-cost type contract. This type of contract is prohibited in the federal government. TSA also paid more than $44 million in award fees without adequate evaluation of the contractor's performance, and paid the contractor a profit that was disproportionately high when compared to the contractor's cost and risk and compared to what other agencies allow as profit under such contracts.

TSA has since devised policies and procedures that require adequate procurement planning, contract structure, and contract oversight. For example, TSA has established a contract management team that closely monitors the work of its current personnel recruitment contractors. This team is responsible for all activities related to inspection of contractor's performance and documenting compliance with contract provisions, including tracking cost and schedule performance. Their oversight activities include a formal monthly program review to gauge programmatic success and identify issues. TSA intends to establish similar contract management teams for each of its major programs.

Other bureaus have large, complex, and high-cost procurement programs under way that need to be closely managed. For example, CBP's Automated Commercial Environment (ACE) system 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, the department recently awarded a contract for the development of United States Visitor and Immigrant Status Indication Technology System (US-VISIT). US-VISIT is an automated system for tracking and controlling the entry and exit of all aliens by air, land, and sea ports of entry. US-VISIT will be up to a $10 billion dollar program implemented over the next ten years. DHS OIG will be reviewing these major procurements on an ongoing basis.

Grants Management

DHS inherited a variety of grant programs that provide money for disaster preparedness, response, 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, DHS OIG's report on the Assistance to Firefighters Grant Program (OIG-ISP-01-03, September 2003) pointed out that many items authorized for purchase under the program are also authorized for purchase under the State Homeland Security Grant Program. In addition, preparedness grant programs were located in different DHS directorates, creating challenges related to intra-departmental coordination, performance accountability, and fiscal accountability. Furthermore, DHS program managers need 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. OIG's March 2004 report (OIG-04-15) on distributing and spending first responder grant funds identified a number of reasons for delays in getting equipment and training into the hands of first responders. ODP has begun taking actions recommended in the report.

OIG continues to audit individual disaster assistance grants awarded by FEMA to states and sub-awarded to local governments. We have reported on 121 such audits since March 1, 2003, and questioned $68 million in claimed grant costs. An important byproduct of those audits is that we identify recurring problems, such as repeated instances of FEMA's not enforcing regulations designed to ensure managerial control over grant funding. For example, state and local subgrantees often ignore the requirement that they get written approval from FEMA before continuing with public assistance projects that are going to cost more or take more time to complete than estimated at the time FEMA initially approved the project. Often, when FEMA closes the grant and discovers this rule violation, it retroactively approves the increases with no consequence to the grantee or subgrantee. Ignoring such regulations increases the risk of waste, fraud, and abuse.

Consolidation of Preparedness Grants

DHS consolidated two offices, the Office of Domestic Preparedness and the Office of State and Local Government Coordination, into the Office of State and Local Government Coordination and Preparedness. The new office addresses the need to locate all DHS terrorism grant programs in a single office and eliminate the inefficiency resulting from similar grant programs located in separate organizational units. When the reorganization is completed, the office will include 25 DHS grant programs and will provide a "one-stop shop" for DHS terrorism preparedness grants. OIG applauds this effort.

In addition, DHS established a Grant Council that provides a forum for senior DHS financial assistance officials to work together. The Council is intended to address issues affecting DHS financial assistance mechanisms (grants, cooperative agreements, reimbursable agreements and other types of assistance) to meet the common needs of organizational elements, and to develop and implement short term and long term goals for the DHS grants management system. The Council is intended to address innovative approaches to promote effective business practices and ensure the timely delivery and proper stewardship of DHS grants. OIG supports this effort and participates in an advisory role.

DHS Grants Management System

DHS is making progress in developing an integrated grants and financial management system. Grants are still being processed outside the department under memoranda of understanding with other federal agencies. However, the department is developing an

integrated grant and financial management system, known as "eMerge2" (electronically managing enterprise resources for government effectiveness and efficiency), which is scheduled for implementation by September 2006. The Office of Grant Policy and Oversight, which reports to the Chief Procurement Officer, and several DHS major grant-awarding offices, have been involved in the development of this system, but the primary responsibility for its development and implementation resides with the DHS Resource Management Transformation Office.

The department has updated the Catalog of Federal Domestic Assistance to reflect the assistance programs that were either transferred from the 22 federal agencies or developed as a result of congressional direction and new funding. Also, the department has created internal and external websites to provide updated information on grant activities. OIG will continue to monitor DHS' progress.

Information Technology

Systems Integration

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. Because of the lack of standardization and systems interoperability in the current environment, many of these activities are tedious, manual, and burdensome. The eMerge2 program is intended to address these issues by implementing DHS-wide enterprise solutions to increase efficiency and effectiveness significantly while optimizing investments. Based upon recent OIG discussions with management officials, the program is on schedule in the design and acquisition phase, requirements have been identified, and a request for proposals has been issued 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 set up an Enterprise Infrastructure Board that meets periodically to discuss strategies for connecting DHS 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 the DHS networks. DHS is enhancing ICE's backbone to create the department-wide network that establishes data communications among all of its organizational elements.

With release of the first version of an enterprise architecture in September 2003, the CIO has also made progress toward the goal of one DHS infrastructure. In December 2003, enterprise architecture officials in the CIO's office told OIG that the department had not yet issued a request for proposal to implement the enterprise architecture. Version 1 of the document outlines a general transition strategy, but it must be detailed further for the

architecture to be implemented. Work is currently under way on version two of the enterprise architecture. One of the objectives of the DHS enterprise architecture team is to make the transition strategy in version 2 more detailed and easier to implement.

Information Technology Controls

A key aspect of the financial statement audit was the assessment of DHS IT general controls, as IT systems significantly facilitate DHS' financial processing activities and maintain important financial data. Controls over IT and related financial systems are essential elements of financial reporting integrity. Effective general controls in an IT and financial systems environment are typically defined in seven key control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, service continuity, and system functionality. In addition to reliable controls, federal financial management system functionality is important to program monitoring, increasing accountability of financial and program managers, providing better information for decision making, and increasing the efficiency and effectiveness of services provided by the federal government.

KPMG found weaknesses at each bureau across all IT general control areas. Collectively, these weaknesses limited DHS' ability to ensure that critical financial and operational data was maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively affected the internal controls over DHS financial reporting and its operation, and KPMG considered them collectively to represent a material weakness, as mentioned earlier.

The challenge of merging numerous entities into DHS has been a key contributing factor to these weaknesses. These various entities have had their own IT functions, controls, and processes. DHS has taken some steps to begin addressing these issues, such as implementing the *Information Technology Security Program Publication*, which contains many requirements for maintaining a DHS-wide information security program. In addition, DHS is currently designing a department-wide IT architecture, as mentioned above. Until the architecture is complete and the related IT infrastructure, controls, and processes are implemented, DHS' IT control environment will continue to consist primarily of the IT processes and controls in place at the entities that were consolidated into DHS.

We believe that to address these weaknesses DHS needs to design and implement DHS-wide policies and procedures related to IT controls, and to ensure that the policies and procedures are enforced through the performance of periodic control assessments and audits. Focus should be aimed at implementing and enforcing a DHS-wide security certification and accreditation (C&A) program, and IT training for administrators and users. Many of the technical issues identified during this review, such as weak technical security controls and the lack of contingency planning strategies, can be addressed through an effective C&A and training program.

Conclusion

Mr. Chairman, this concludes my prepared statement. Please be assured that our office will continue to place a high priority on financial management issues. Again, I appreciate your time and attention and welcome any questions you or members of the subcommittee might have.