STATEMENT OF CLARK KENT ERVIN

INSPECTOR GENERAL

U. S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY

AND FINANCIAL MANAGEMENT

U. S. HOUSE OF REPRESENTATIVES

MARCH 10, 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 to provide an update on how DHS is addressing the inherent challenges involved in realigning its financial operations and addressing its financial systems weaknesses. In that regard, we include financial accounting, contract management, grants management, and information technology.

Overview

Since the department's organization one year ago, it has made notable progress in the integration of legacy agencies and the development of department-wide functions. Through our work in the various bureaus and offices within the department, we have seen the roots of this new organization begin to take hold. This is happening because of the commitment and hard work of many dedicated civil servants. Still, there is much to be done.

When we provided testimony to this subcommittee six months ago on September 10, 2003, we discussed the financial management challenges facing DHS. One of the larger challenges was preparing auditable financial statements for the department. At that time, the FY 2003 financial statement audit was already well under way, but the outcome was hardly clear. Getting an unqualified opinion was the goal, albeit a very optimistic one, but the realities were that the mid-year creation of the department and its dispersed accounting providers proved too much to overcome in such a short period of time. The good news, however, is that the department did receive a qualified opinion on its consolidated balance sheet and statement of custodial activity.

I say "good news" because, with just a few very specific exceptions, we can be reasonably assured that DHS has fairly presented its assets and liabilities as of September 30, 2003, and the custodial revenues it collected over its first seven months of operations. Those are key pieces of information needed for good stewardship, and they provide an essential financial baseline for the new organization going forward. Regarding the other statements – the consolidated statements of net cost and changes in net position, the combined statement of budgetary resources, and the consolidated statement of financing - the auditors were unable to complete their procedures and thus unable to provide an opinion, for reasons I soon will explain.

DHS is to be congratulated on producing its first set of financial statements for audit and for fully accepting this challenge last April 2003 when the department was just establishing itself. Not only do we have a baseline for the department's assets and liabilities, the process itself has been invaluable in providing focus on good financial management practices. We now know where the major financial reporting weaknesses in this new organization lie, and DHS can begin to address them.

Summary of Auditors' Opinion

The Office of Inspector General (OIG) contracted with the independent public accounting firm, KPMG LLP, to audit 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. As noted above, KPMG gave a qualified opinion on the consolidated balance sheet and statement of custodial activity.

The qualification on the balance sheet and statement of custodial activity 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 U.S. Coast Guard (Coast Guard); (2) KPMG's inability to observe sufficient physical counts of operating materials and supplies (OM&S) at Coast Guard or otherwise verify the valuation of OM&S 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 U.S. Secret Service (Secret Service), and post-employment benefits recorded at $201 million at the Coast Guard. However, 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 executive department. It is not uncommon for a large established agency such as the Coast Guard to require additional time to get its processes and systems in place to facilitate a financial statement audit performed at this level of detail. Similarly, even the $3.3 billion in retirement benefits at the Secret Service would not likely have been material at Treasury, where total liabilities reach almost $7 trillion. The Secret Service has obtained an actuarial report on its retirement benefits' liability, and believes it has recorded the correct amount. Coast Guard likewise has 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 – referred to as "activity statements" - 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, prior to the completion of the audit.

Summary of Material Weaknesses and Reportable Conditions

KPMG reported 14 reportable conditions, seven of which were considered to be material weaknesses. "Reportable conditions" are significant deficiencies in internal controls that could adversely affect the department's ability to record, process, summarize, and report financial data. "Material weaknesses" are reportable conditions in which internal controls do

not reduce to a relatively low level the risk of material misstatements in the financial statements.[1]

The following is a brief synopsis of each material weakness. Detailed descriptions of these weaknesses, their causes, and KPMG's recommendations can be found in the *Independent Auditors' Report* that is included as part of DHS' FY 2003 *Performance and Accountability* Report.

Reportable Conditions That Are Considered To Be Material Weaknesses

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

B. 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.

C. 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.

D. Property, Plant, and Equipment (PP&E): The Coast Guard was unable to support the recorded value of $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. The Transportation Security Administration (TSA) lacked a comprehensive property management system and adequate policies and procedures to ensure the accuracy of its PP&E records.

E. Operating Materials and Supplies (OM&S): Internal controls over physical counts of OM&S were not effective at the Coast Guard. As a result, KPMG was unable to verify the recorded value of $497 million in OM&S. The Coast Guard also had not recently reviewed

[1] More specifically, under standards issued by the American Institute of Certified Public Accountants, reportable conditions are "matters coming to the auditors' attention relating to significant deficiencies in the design or operation of internal controls that, in the auditors' judgment, could adversely affect the department's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

its OM&S capitalization policy, leading to a material adjustment to its records when an analysis was performed.

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

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

Other Reportable Conditions

H. 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.

I. 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.

J. 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. Also, 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.

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

L. Intra-governmental Balances: Several large 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.

M. 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.

N. 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.

Other Matters

The material weaknesses and reportable conditions cited above were identified considering their materiality to DHS' financial reporting as a whole. There are other matters significant to individual bureaus that did not rise to the level of material weakness or reportable condition at the DHS consolidated level. KPMG informally communicated these issues to financial management officials during the course of the audit. We plan to summarize these findings in a more formal document; however, with the commencement of the FY 2004 audit upon us, these issues will immediately carry forward into the ongoing audit.

Status of Prior Year Material Weaknesses

DHS inherited 18 material weaknesses from the former Customs Service, the former Immigration and Naturalization Service, the Federal Emergency Management Agency (FEMA), and TSA. KPMG determined that nine of the material weaknesses were corrected or partially corrected. The remaining weaknesses were consolidated into the seven DHS material weaknesses or reclassified to a reportable condition or other matter for management's attention. A reconciliation of the 18 material weaknesses to their current status is found in the *Independent Auditors' Report* that is included as part of DHS' FY 2003 *Performance and Accountability Report*.

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, 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 has not yet 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 many of the 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 on 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, OMB is requiring all agencies to summarize corrective action plans for all material weaknesses, not just FFMIA related non-compliance, in their performance and accountability reports. Given the short time since DHS received our audit report, DHS officials have not had sufficient time to respond to us formally with corrective action plans. 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 Process and Challenges

Now that I have discussed the audit results for DHS, I would like to share some background on how this audit was performed, challenges encountered, and challenges for the upcoming year.

Methodology

We required that KPMG perform the audit according to the General Accounting Office's (GAO) *Auditing Standards* (referred to as the "yellow book") and use *GAO's Financial Audit Manual* (FAM) as the basis for their audit procedures. The FAM requires auditors to identify key internal controls that may materially affect the financial statements and assess whether they are adequate – both in design and in operation. If the auditor finds the internal controls to be reliable, they can reduce the amount of balance and transaction testing. As a result, KPMG looked at processes related to financial reporting, such as revenue collection, disbursement of funds, PP&E, fund balance with Treasury, claims, and payroll, among others. KPMG reviewed these processes at the individual bureaus where they were significant to DHS as a whole. It was this review of key internal controls over financial reporting that led to the identification of material weaknesses and reportable conditions cited earlier.

Audit Challenges For 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 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. 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 department. This brought with it proportionally more scrutiny during our audit, something for which it was not fully prepared. Its financial reporting processes were inefficient and complex. Also, 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 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. Some of the $2.9 billion related to PP&E acquired prior to 1995, 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. KPMG qualified its opinion on the balance sheet for the $2.9 billion, in part, because the Coast Guard could not timely provide sufficient documentation.

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 their 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 prepares DHS consolidated and individual bureau financial statements. Difficulties in using TIER, however, have prevented DHS from preparing timely and accurate periodic consolidated financial statements. Most bureau financial systems are not electronically interfaced with TIER, and bureaus have had to configure their systems and processes to meet TIER submission requirements. As a result, errors continue to occur. TIER is a temporary system solution until a permanent financial reporting system architecture for DHS can be developed and implemented.

The Office of the Chief Financial Officer (OCFO) is responsible for the preparation of consolidated financial statements using TIER. The OCFO operates with relatively few finance personnel, who principally serve to coordinate financial management policy and consolidate financial information submitted by the bureaus. The OCFO has not yet established a hierarchy of financial reporting authority, or an entity-wide financial management organization chart that clearly defines roles and responsibilities and assists with the identification of critical human resources needed to ensure that all financial management responsibilities are assigned. The OCFO has not yet developed SOPs that will 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 will 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 major keys to success, learned from other departments that have already met this date, are the commitment to do so, starting at the top of the organization, and a detailed plan to get there. DHS' Chief Financial Officer (CFO) has assured us that this commitment has been made. In mid-March, the OCFO, bureau financial staff, and the auditors will hold a two-day planning session to map out a strategy.

DHS also will have to deal with problems that it was unable to overcome this year. Coast Guard must still obtain sufficient support for $2.9 billion in PP&E. Weaknesses in inventory procedures at the Coast Guard for OM&S must be corrected to allow for an accurate physical count at year-end. Also, accounts payable and undelivered orders--only a reportable condition this year--and other accrual type accounts will take on paramount importance. Reliable estimation techniques or other procedures will need to be developed at several bureaus to report accruals at a date much earlier than was achieved in 2003. The OCFO must address gaps in its staffing, create SOPs that will guide the bureaus and support timely and accurate reporting, and establish clear organizational roles and responsibilities.

Also, H.R. 2886, if passed, would require DHS to include in its FY 2004 performance and accountability report an assertion on internal controls over financial reporting. Management's assertion as to the adequacy of internal controls, supported by adequate documentation, testing, and reporting, is essential to a successful audit on internal controls over financial reporting. H.R. 2886 would require the auditors to provide an opinion on internal controls over financial reporting at DHS starting with the FY 2005 reporting period.

Contracts Management

A major challenge for DHS is 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 are 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 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. 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 begin integrating the procurement functions of its component organizations to ensure that good management controls are consistently applied. Several of the incoming procurement organizations have lacked important management controls. For example, during its first year of operation, the Transportation Security Administration (TSA) relied extensively on contractors to accomplish its mission, while providing little contract oversight. Contracts were written without clearly defined deliverables, and on occasion, contractors themselves were permitted to determine need and to define deliverables. As a result, the cost of those initial contracts ballooned. TSA is in the process of devising policies and procedures that require adequate procurement planning, contract structure, and contract oversight. Also, the Federal Emergency Management Agency (FEMA) has just recently discovered that it has not been reporting or tracking procurements let by its disaster field offices.

Some 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, in early 2004, the department will award a contract for the development of the 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. It is anticipated that US-VISIT will be a multi-billion dollar program implemented over the next ten years. DHS OIG will be reviewing these major procurements on an ongoing basis.

Grants Management

DHS inherited a variety of grant programs that provide money for disaster preparedness and 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 inter-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.

Consolidation of Preparedness Grants

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

The department is also in the process of creating a Grants Management Council (Council). It is intended to be a group of senior DHS managers who provide advice on issues regarding the department's grants. The Council will identify innovative approaches to promote effective business practices that ensure the timely delivery and proper stewardship of federal assistance funds. The first meeting was held in February 2004. OIG supports this effort and will participate in an advisory role.

DHS Grants Management System

DHS is faced with developing an effective, integrated grants management and accounting system. The Department is still a long way from accomplishing that objective. Grants managed by the Science and Technology Directorate (S&T), Office of Domestic Preparedness (ODP) (fire only), ICE, and the Information Assurance and Infrastructure Protection Directorate (IAIP) are processed under MOUs with FEMA. ODP (except for fire) grants are processed by the Department of Justice; TSA aviation grants are processed by the Federal Aviation Administration, port security grants by the Department of Transportation;

and S&T grants and contracts with Oak Ridge National Laboratories are processed by the Department of Energy.

The DHS Grants Policy and Oversight Office has been inventorying DHS grants, collecting the regulations and relevant laws for each, and identifying awarding offices, servicing offices, grants management systems, and administrative staff. This office was also spearheading the e-grants initiative until the DHS Resource Management Transformation Office took over that responsibility in September 2003.

OIG believes that progress has been slow because DHS may have underestimated the problem of consolidating the grant management systems. About 63 FY 2002 grants and more than 83 FY 2003 grants were integrated into DHS, yet the Grants Policy and Oversight Office was staffed by only one full-time person for much of the past year. The problem is receiving additional attention and funding in FY04. OIG will continue to monitor DHS' progress.

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. To address these issues, DHS has established the eMerge^2 program (electronically managing enterprise resources for government effectiveness and efficiency), scheduled for implementation by September 2006. Program goals include implementing DHS-wide enterprise solutions to increase efficiency and effectiveness significantly while optimizing investments. Based upon recent OIG discussions with management officials, the program 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 between 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 very general transition strategy, but it must be detailed further for the architecture to be implemented. Work is currently under way on version 2 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 is 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 to collectively represent a material weakness, as mentioned earlier.

The challenge of merging numerous entities into DHS is 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 primarily consist 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 made on 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 programs.

Conclusion

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