Statement by

Scott Charbo

Chief Information Officer

Department of Homeland Security

Before the

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Hearing on

Information Security

June 20, 2007

Thank you, Mr. Chairman, Ranking Member McCaul and Members of the Subcommittee, for allowing me this opportunity to testify before the subcommittee. My remarks will cover the current status of the Department's information security posture.

You have no doubt heard reports of recent information security incidents at various federal agencies, including the Department of Homeland Security. Certainly, we need to increase our vigilance to ensure that such incidents do not happen again, and, in fact, the recent loss of an external hard drive at the Transportation Security Administration has prompted a comprehensive review of how the Department processes and stores privacy information. My office continues to work closely with the Department's Privacy Office and the Chief Human Capital Office to improve the effectiveness of our controls for privacy information.

The Department takes these incidents very seriously, and will work diligently to ensure they do not recur. I'd like to describe for you some of the significant progress we have recently made in improving information security at the Department. The Department is presently working under a decentralized IT governance model. We have named CIOs and attendant IT support staff in each of the major components comprising the Department. To ensure that this model is effective, Secretary Chertoff recently instituted changes in the oversight functions of the Chief Information Officer for the Department. The revised Management Directive 0007.1 *Information Technology Integration and Management* has increased my authority to manage and direct the Department's information technology programs. Specifically:

1. Components must provide their information technology (IT) budgets annually to the DHS Chief Information Officer for review; I will then make recommendations to the Secretary for final budget submissions to the Office of Management and Budget.

2. Any proposed IT acquisition greater than $2.5 million must be reviewed and approved by the DHS Chief Information Officer. These IT acquisitions are defined as services for IT, software, hardware, communications, and infrastructure.
3. Before IT investment proposals greater than $2.5 million are submitted to the DHS Chief Information Officer for approval, the Department's Enterprise Architecture Board must approve the investment and certify its alignment with the Department's enterprise architecture.
4. I approve the hiring of Component Chief Information Officers, as well as set and approve their performance plans, ratings, and annual award compensation in cooperation with component directors.

The result will be a more coherent and effective utilization of IT resources. IT programs and acquisitions are being reviewed at the Department-level to ensure that they are reconciled with the Department's strategic goals and that information security, enterprise architecture and infrastructure considerations are built into them.

The Department's Information Security Program touches virtually every aspect of IT management, to include budget formulation and implementation, system and network design, enterprise and component specific IT operations, information security policy and architecture, and compliance with the Federal Information Security Management Act (FISMA). My authority over all of these areas directly affects our overall security posture. I would like to mention three key IT consolidation initiatives that we have started to not only better align our shared enterprise environment, but to enhance enterprise information security.

First, we are collapsing multiple legacy wide-area networks (WANs) into a single enterprise WAN, called OneNet. OneNet is based on a comprehensive security architecture that uses the latest IT technologies. For example, the new consolidated WAN

fully implements the IPSec protocol, an authentication and encryption protocol that ensures the confidentiality of all data transiting the WAN. And, as a key part of the transition to OneNet, we have also implemented a comprehensive Security Operations Center (SOC) Concept of Operations (CONOP). This CONOP details more efficient processes for the day-to-day management of security functions for OneNet, as well as for reporting incidents both internally to the SOC, and externally to the United States Computer Emergency Readiness Team (US-CERT) and other Law Enforcement and government agencies when required. To aid this effort, we've created the SOCONLINE Incident Reporting web tool for incident reporting, management and closure.

Second, we are standardizing all email and directory services into a single, modern framework that is much more secure than the legacy environments we inherited. The department had 13 different email systems when it was formed. We have standardized the Target Enterprise Architecture for email, deployed a Global Address List and are on track to transition all components to the new email standards by December of 2007. These improvements will eliminate several security vulnerabilities in our email posture and simplify its management.

Third, we are collapsing multiple datacenters into a common shared environment. The first phase of our first datacenter is up and running in Stennis, Mississippi, and we are now in the process of migrating legacy systems into that center. Security has been designed into the Stennis facility from the start and as systems migrate to that facility our security posture will continue to improve.

These initiatives will not only enhance our ability to store, process, and share information, they will also enhance our ability to ensure the confidentiality, integrity, and availability of that information.

In addition to these three major consolidation activities, I have also begun another activity in conjunction with the Chief Financial Officer to enhance the security of our core financial systems. Each component CIO and CFO jointly presented a detailed remediation plan for improving the security of our core financial systems; this was done with the knowledge of both our Inspector General and independent auditors. These plans were personally approved by me, the Department CFO, and the Under Secretary for Management. In addition to ensuring the implementation of these plans, my office partners with the CFO and his team on other issues. One example of our continuing collaboration is a series of workshops that my office has sponsored to assist components in improving the security of these core financial systems. Due to the combined CIO/CFO efforts, we are now making significant progress in resolving prior financial audit findings.

It is my responsibility to ensure that our IT systems comply with all federal and department policies. I now review each component's IT budget and expenditures as outlined in the Exhibit 53s and 300s and ensure their alignment in the following areas:

1. The Secretary's goals and priorities;
2. The Department's enterprise architecture;
3. Needs definition and business case alignment;
4. Privacy rules and regulations;
5. Section 508 (Accessible Systems and Technology) compliance;
6. Information security compliance; and,
7. IT infrastructure compliance.

In 2007, the Department will spend approximately $4.9 billion for information technology, and $332 Million of that is dedicated to IT security. We have requested $5.2

billion for IT in 2008, and we are planning to spend $342 Million on IT security. These numbers represent approximately 6.8 % of the total IT budgets for each of those years. Last week, I completed reviews for all component-level IT budgets for fiscal years 2009 - 2013. These detailed reviews provided me valuable insights into all areas of the Department's information technology programs, and it has given visibility into departmental activities in information technology from strategic mission, portfolio, and technology perspectives. These reviews will allow me to make informed recommendations to the Secretary concerning the Department's IT budget for these future years, while ensuring that all program elements, especially IT security, are adequately addressed.

On the expenditure side, we are working to make sure our acquisitions are in line with our requirements for information security; so far, I have conducted 130 IT Acquisition reviews for security compliance (as well as enterprise architecture, infrastructure compatibility, business case maturity, etc.), and I have favorably adjudicated many issues to ensure that information security requirements are met in all IT acquisitions.

As part of the process of reviewing and making recommendations for component IT budgets, I also take into account components' performance in mitigating their information security vulnerabilities. Included in this improved Management Directive is the authority to recommend budget changes in areas where a component's information security posture is weak. While I have not yet recommended that a component's budget be modified in response to a lack of success in mitigating vulnerabilities, I have provided guidance and direction, both informally and in some cases in writing, to the components that are not satisfactorily progressing in their remediation efforts, and with recommended changes.

To ensure compliance with the Federal Information Security Management Act (FISMA), my Chief Information Security Officer (CISO) maintains a comprehensive systems inventory of all government-owned and contractor-managed systems. The Department's Office of Inspector General has reviewed the inventory methodology and continues to give it high marks for both completeness and accuracy. DHS's Information Security Program has made measurable progress, enough that unlike all previous years the Inspector General's annual FISMA assessment did not rate it as a significant deficiency in 2006.

System owners, government and contractor alike, are held accountable for completing all elements of FISMA compliance for each system. The CISO produces a monthly scorecard, providing each component with an honest assessment of their status. Each component is provided a current assessment on status of certification and accreditation for every system in the inventory, annual controls testing, incident reporting, configuration management, information security training, and information security vulnerability management. The scorecards address the security of internal DHS systems as well as contractor operations. Additionally, the CISO has teams in place that conduct regular training and assist visits, with the current emphasis on vulnerability resolution and configuration management.

I review this scorecard with all component CIOs in regular meetings set aside for this purpose and we discuss the scorecard at Management Council at least monthly. I also present this scorecard to the Secretary and Deputy Secretary periodically, and they in turn emphasize security with agency heads as appropriate. Most of our components have made exceptional progress in improving their overall FISMA posture. Since March 2007, I have written letters to the Directors of three components pointing out program deficiencies and suggesting ways to improve.

While the monthly scorecard is the most visible product of the Department's Information Security Program, there is also a continuing emphasis on the basic tenets of effective information security with the understanding that progress in large federal agencies can only be achieved in increments. The Department's Information Security Program is in the third phase of its 5-year strategic plan.

In the first phase, the Program focused on "establishing a baseline." Basic information security policy and architecture were established and automated tools for enforcing the Department's policy were implemented. A thorough inventory of the Department's IT systems was conducted and system owners were identified to ensure accountability for system security.

In the second phase, the Program focused on completing the accreditation of its IT systems. The significant goal of documenting and accepting system risk was accomplished. The implementation of the *FY 2006 Certification and Accreditation (C&A) Remediation Plan* generated a 68 percent increase in the number of systems accredited. The Department's C&A completion rate went from 26 percent in October 2005 to 95 percent by the end of 2006.

We now have a steady-state baseline from which to build. Our security policies and architecture are continually updated to respond to changing federal guidance, evolving missions, and new threats, and the certification and accreditation process is institutionalized across the Department. The current and future phases of the Information Security Program are aimed at incrementally "raising the bar", and our focus is not only on improving the documentation of controls and processes, but, more importantly on enhancing the operational security of every system.

To this end, we are now evaluating and improving systems security profiles at the system level, and, review teams are providing assistance to Components in improving security plans and contingency plans, as well as providing assistance in other areas including configuration management and vulnerability remediation. We currently have over 4000 IT security related Plans of Action and Milestones (POAM) active, all targeting weaknesses identified through internal systems-level reviews, including certification and accreditation and annual assessments, as well as external audits including those conducted by our Inspector general and the Government Accountability Office. So far in 2007, we have completed remediation efforts for over 7000 weaknesses, and all of the weaknesses identified in the recent GAO Audit of the USVISIT Program now have active POAMs with scheduled completion dates by the end of 2007. We have also completed several tests starting with our most sensitive systems and our Network Perimeters.

Although we still have a ways to go, we've made measurable improvements in the management of information security at the Department. We're not the only ones making this point. The Office of Management and Budget's (OMB) 2006 Report to Congress noted the significant progress we've made in certifying and accrediting the Department's IT systems. I am confident that the DHS Information Security Program is moving in the right direction and I look forward to working with you and your staff in the future.

Thank you and I look forward to your questions.