Deputy Chief Financial Officer Peggy Sherry

And

Chief Information Security Officer Robert West

U.S. Department of Homeland Security

Testimony

Before the Subcommittee on Government Organization, Efficiency and Financial Management; of the House Oversight and Government Reform Committee

Thank you Chairman Platts, Ranking Member Towns, and members of the Committee for the opportunity to provide an update on the Department of Homeland Security's (DHS) progress in addressing recommendations found in the Office of the Inspector General Audit report titled "Information Technology Management Letter for the FY 2010 Financial Statement Audit." Department leadership takes all audit findings seriously, and we are fully committed to resolving these issues as quickly as possible.

The Department has made significant progress in reducing IT security control risks and costs by transitioning from a highly decentralized IT landscape to enterprise data centers and services. DHS inherited approximately 1,100 separate and unique IT systems, with each system individually accountable for all security controls. IT systems are more secure today than ever before because the Department's enterprise security architecture—called "Mission Assurance through Defense-in-Depth"—now includes a comprehensive set of layered security controls.

DHS has consolidated six wide-area networks into a secure, modern, fully-encrypted backbone infrastructure and has made significant progress in consolidating multiple data centers into two enterprise data centers. These data centers have been designed with a robust set of security controls to support systems that operate in those environments.

In addition to the enhanced security controls for the transport infrastructure and the two enterprise datacenters, the Department has also increased security by consolidating all Internet traffic behind two redundant Trusted Internet Connections (TIC). Currently over 95 percent of all of the Department's traffic accesses the Internet via the TICs, and the Office of the Chief Information Officer (OCIO) has placed TIC-like functionality in front of each major Component to ensure that Components can maintain flexible security policies appropriate for their individual missions, while at the same time maintaining a baseline security foundation from which to operate. These "Policy Enforcement Points" include both monitoring capabilities as well as next generation, application-aware firewalls designed specifically to address Advanced Persistent Threats (APT), which are malicious actors who regularly target the Department's information and information systems. The Department also has a dedicated, enterprise Security Operations Center, with trained analysts who leverage new monitoring tools to proactively look for and respond to APT-type activity.

The Department currently operates 783 IT systems that support multiple, complex and highly diverse missions. Of those systems the auditors identify IT systems material to the financial audit. Most of these financial systems have been in operation for many years and predate the Department's creation in 2003. While these legacy systems are now more secure due to the fact that they operate within the enterprise framework described above, some of these systems are missing system-specific controls and cannot fully support business processes that ensure accurate financial reporting. Heavily manual processes that are needed to compensate for a lack of automated controls highlight the fact that the significant progress we have made in financial management, reporting and accountability could be furthered with improvements to some of these financial systems.

When the Department was formed in 2003, we inherited 30 significant deficiencies, including 18 material weaknesses. DHS has shown great progress implementing corrective actions and improving the quality and reliability of our financial reporting in the past five years and now only has six material weaknesses.

As recommended in the OIG IT Management Letter, the Department has reviewed all IT Notices of Findings and Recommendations (NFRs) and Component leadership has created Plans of Actions and Milestones (POA&Ms) detailing planned remediation. In FY 2011, DHS focused on strengthening financial system security and controls using a three-phase assessment approach including a current state assessment, root cause analysis, and independent verification and validation of Component POA&Ms. IT personnel responsible for preparing POA&Ms are now trained on creating realistic corrective action plans that address root causes.

Additionally, the DHS Information Security Office (ISO) performed Critical Control Reviews (CCRs) in FY 2010 and FY 2011 to independently validate the implementation of key security controls information reported in a system's accreditation and certification documentation. Following each review, system owners are provided with detailed results and recommendations to improve security controls documentation and implementation. System owners are required to develop POA&Ms for weaknesses identified. The CCRs have increased Component awareness of security control issues and Component POA&Ms have greatly improved the documentation of IT security issues at the Department.

During the FY 2010 assessment, the auditors noted that DHS made progress in remediating IT findings from FY 2009, closing approximately 30 percent of the findings. The Department has taken numerous actions to address the five remaining significant weaknesses related to IT controls on financial systems as described below.

1) Full implementation of Homeland Security Presidential Directive - 12 (HSPD-12) Personal Identity Verification (PIV) smart card will make significant progress towards addressing the challenge of restricting unauthorized access to key DHS financial applications. For example, mandating use of PIV credentials provides the

2) Configuration management control weaknesses are being addressed through a continuous monitoring program initiated in FY 2011. This program is a risk management approach to IT that maintains an accurate picture of an organization's security risk posture, provides visibility into assets, and leverages use of automated security management tools to quantify risks, ensure effectiveness of security controls, and implement prioritized risk mitigation.[1] As a part of the "Defense-in-Depth" security framework, the Department is implementing a comprehensive continuous monitoring capability for maintaining configuration for all IT assets at DHS including financial systems. Efforts are currently underway at all Components, and will be completed by the end of FY 2012.

3) Corrective actions have been taken or are ongoing to remediate security management deficiencies in the certification and accreditation process. The financial systems that had not completed the required certification and accreditation process have either been accredited or were retired from use in FY 2011. As for deficiencies in adhering to and developing of policies and procedures, Component management is required to submit POA&Ms detailing the implementation of missing policies and procedures, as well as verifying and validating that the corrective action is complete. The POA&M process has also been improved to require additional monitoring of remediation progress and alert management when progress is delayed or appears inadequate.

[1] NIST Special Publication 800-37, Revision 1, *Applying the Risk Management Framework to Federal Information Systems)*.

4) Contingency plans that lacked current and tested continuity plans developed to protect DHS resources and financial applications, have been updated. During FY 2011, Component personnel either conducted continuity plan tests or submitted a POA&M committing to complete the required testing within six months. For those tested, the continuity plans were updated with lessons learned as appropriate and, in some instances, an independent verification and validation was performed to confirm the completion and adequacy of the updated, tested plan.

5) The lack of proper segregation of duties for roles and responsibilities within financial systems, are being addressed on a system-specific basis by each Component. Components are identifying and documenting the duties that should not be performed by one employee because doing so provides an opportunity to engage in erroneous activity. For example, personnel who submit check requests should not be jointly assigned responsibility for approving check requests. This information will ensure that Components properly divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one employee would have the necessary authority or system access to be able to engage in erroneous, fraudulent or criminal activity. The Department has made significant progress in resolving this issue, and full remediation at all DHS Components will continue over the next two to three years.

Many improvements made in financial management at DHS over the past few years are a direct result of the processes and structures that have been put in place to ensure consistent operations for each of our financial accounting centers and financial management offices within DHS Components. The Department has made key changes to improve the overall internal controls process to enhance systems' security. The DHS DCFO and CIO have worked to improve the overall controls process by aligning the FISMA[2] framework with the DHS internal

[2] Federal Information Security Management Act (FISMA) requires that all federal IT systems comply with the National Institute of Standards and Technology Risk Management Framework FISMA framework.

control assessment process to improve financial systems security at the Department. DHS's major activities under this integrated approach include:

- Published the Department's 5th Annual Internal Controls Playbook on March 31, 2011 which builds upon previous successes, defines current internal control initiatives, and establishes Mission Action Plans, milestones, and focus areas for the Department's most significant internal control challenges. The Playbook includes DHS's approach to documenting and testing the design effectiveness of financial system Information Technology General Controls (ITGCs).
- Updated the OCFO Designated Systems List for FY 2010 as a result of the IT general control assessments performed in FY 2009. The list specifies the financial systems that require additional management accountability to ensure effective controls exist over financial reporting.
- Perform ongoing verification and validation procedures to ensure POA&Ms address root causes of financial system security control deficiencies identified from the financial statement audits and FISMA annual assessments. Issuance of the FY 2010 DHS Information Security Performance Plan includes the requirements to ensure key financial system security controls are tested annually and quality POA&Ms are developed and completed in a timely manner.
- Continue tracking remediation status of the issues identified during the OMB Circular A-123 ITGC annual assessments as a metric on the Department's monthly FISMA Scorecard. The Scorecard measures Components compliance with OMB FISMA reporting requirements and DHS senior management priorities such as the status and quality of system certifications and accreditations and weakness remediation.
- Continue annual revisions of the DHS 4300A, Sensitive Systems Handbook, Attachment H: Plan Of Action & Milestones (POA&M) Process Guide which includes the guidance and procedures for developing, maintaining, reporting, and maturing DHS Components' remediation plans to reduce vulnerabilities.
- Provide ongoing POA&M training, including root cause analysis, to DHS Components.

While the Department has shown major improvements over the past few years in financial management and improving financial system security, updated financial systems are necessary in order for DHS to fully remediate financial management issues. We are working closely with Components to standardize business processes and internal controls, implement a common line of accounting, maintain data quality standards, and provide oversight and approval for any proposed efforts for financial system upgrade or replacement projects.

The DCFO and CIO along with the Office of the Chief Procurement Officer, Program Accountability and Risk Management Office, and Component offices will work together to ensure financial modernization projects are planned and executed to meet reporting requirements and minimize costs for financial operations. Currently, the Department is analyzing the best way forward for financial system modernizations. DHS remains fully committed to improving our financial system security in order to provide timely, accurate, and complete financial information to our key stakeholders including Congress and the American taxpayers.

Thank you.

Homeland Security

Biography

Peggy Sherry

Deputy Chief Financial Officer

Peggy Sherry is the Department of Homeland Security's Deputy Chief Financial Officer. She joined the Department in 2007 as the Director of Financial Management responsible for developing Department-wide financial management policy, preparing Department-wide financial reports and leading the Department's financial audits.

Prior to joining the Department, Ms. Sherry was the Deputy Chief Financial Officer for the United States Holocaust Memorial Museum. Before then, she was an auditor with GAO for more than nine years. During her time at GAO, Ms. Sherry oversaw numerous financial audits, to include leading segments of the financial statement audit of the U.S. Government. Prior to her service in the public sector, she worked as a financial manager in the banking and construction industries.

Ms. Sherry has her Bachelor's degree in Accounting from George Mason University and a Masters in Accounting and Finance from University of Maryland University College. Ms. Sherry is a Certified Public Accountant and a Certified Government Financial Manager.

Current as of 7/19/2011

Homeland Security

Biography

Robert C. West
Chief Information Security Officer

Mr. West is a native of Chattanooga, Tennessee. After graduating from Vanderbilt University in 1974 with a Bachelor of Engineering degree in Electrical Engineering, he was assigned to Navy Flight Training and was designated a Naval Aviator in 1975. He served with distinction as a career Naval Officer, including Command of an aviation squadron, before retiring with the rank of Captain in 2001. In his final assignment prior to retiring, he served as the first Deputy Commander for the Defense Department's newly established Joint Task Force for Computer Network Defense, created in 1998 as a direct response to both real world and exercise computer incidents. The Task Force is responsible for defending all of the Defense Department's 3.5 million operational computers and networks worldwide.

After retirement, Mr. West was employed with the Critical Infrastructure Assurance Office (CIAO) at the United States Department of Commerce. In that capacity, he served as Senior Policy Analyst where he was a major contributor in the development of the National Strategy to Secure Cyberspace, a White House initiative. As principle liaison with private sector companies specializing in information security, he assessed new and emerging technologies and made recommendations for their use in the Strategy.

In late 2002, the CIAO was identified as one of 22 agencies to be transferred to the newly established Department of Homeland Security. At that time, and based on his unique background, Mr. West was assigned to the Office of the CIO, Homeland Security Transition Planning Office, White House, where he was responsible for developing a strategic plan for implementing an Information Security Program for the Department. He was subsequently selected as the first Chief Information Security Officer for the Department and currently serves in that position.

Mr. West holds a Master of Science degree in Computer Science (emphasis in Information Security) from James Madison University, a Master of Science degree in Political Science from Auburn University, a Juris Doctor degree from the Columbus School of Law, Catholic University in Washington, DC, and is currently a member of the District of Columbia Bar. He also teaches computer science as an adjunct professor at both George Washington University in Washington, DC, and James Madison University in Harrisonburg, Virginia.