INTERNAL CONTROL WEAKNESSES AT THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND FINANCIAL MANAGEMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

OCTOBER 27, 2011

Serial No. 112–109

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
73–167 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. McHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DesJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
EDOLPHUS TOWNS, New York
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

Lawrence J. Brady, *Staff Director*
John D. Cuaderes, *Deputy Staff Director*
Robert Borden, *General Counsel*
Linda A. Good, *Chief Clerk*
David Rapallo, *Minority Staff Director*

Subcommittee on Government Organization, Efficiency and Financial Management

TODD RUSSELL PLATTS, Pennsylvania, *Chairman*

CONNIE MACK, Florida, *Vice Chairman*
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas

EDOLPHUS TOWNS, New York, *Ranking Minority Member*
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
ELEANOR HOLMES NORTON, District of Columbia

CONTENTS

INTERNAL CONTROL WEAKNESSES AT THE DEPARTMENT OF HOMELAND SECURITY

THURSDAY, OCTOBER 27, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION,
EFFICIENCY AND FINANCIAL MANAGEMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2247, Rayburn House Office Building, Hon. Todd Russell Platts (chairman of the subcommittee) presiding.

Present: Representatives Platts, Lankford, Amash, and Towns.

Staff present: Linda Good, chief clerk; Hudson T. Hollister, counsel; Mark D. Marin, director of oversight; Tegan Millspaw, research analyst; Nadia A. Zahran, staff assistant; Jaron Bourke, minority director of administration; Beverly Britton Fraser, minority counsel; Jennifer Hoffman, minority press secretary; and Adam Koshkin, minority staff assistant.

Mr. PLATTS. Good morning. The subcommittee will come to order.

A quick housekeeping, our understanding is votes on the floor may happen, we thought 11, 11:30, now they are saying maybe as early as the next 20 to 30 minutes. So we're going to try to get through your testimony and hopefully a round of questions. My worry is that when the votes go up, it may be a long series. We are going to try not to have you sitting here waiting. We will hope for votes being a little later than expected.

The purpose of today's hearing, I am going to shorten my opening remarks for the purpose of getting to your testimony as quickly as we can. But the purpose of today's hearing is to evaluate the effectiveness and security of financial systems at the Department of Homeland Security. DHS is one of the largest Federal departments and spent $56.4 billion on its operations in 2010. Because of the size and importance of DHS, it is crucial that we have strong financial management systems and that data is properly protected.

However, in 2010, independent auditors found numerous weaknesses in DHS' financial management and information technology security systems. And this hearing will examine the results of that audit and DHS' progress in resolving the problems in its financial management systems.

The audit was conducted by the independent auditing firm KPMG and identified 161 weaknesses in DHS' internal controls over crucial financial systems. Almost two-thirds of the weaknesses were repeats from KPMG's 2009 audit of the Department. The findings contributed to five significant weaknesses as well as one material weakness in information technology and financial system functionality.

DHS has been working continuously to improve its financial Management and its efforts should be acknowledged. However, as this audit shows, there are still significant problems and the Department must address these problems. Many of these deficiencies are long-term that have never been resolved. This hearing is intended to review the findings of the audit and evaluate how we can better address these identified deficiencies.

The subcommittee appreciates DHS' ongoing work to improve its financial management and its cooperation and assistance with the auditors. I certainly want to thank our witnesses for being here today and to share your expertise and insights with us to allow our committee in our oversight role to be more effective in partnering with you and the full committee in trying to achieve what we are all after, which is an efficient, well-run, accountable Department, and how we handle the public's funds and fulfill your mission, which is so important to our Nation's security.

With that, I am going to submit my entire statement for the record and yield to the ranking member, Mr. Towns from New York, for the purposes of an opening statement.

Mr. TOWNS. Thank you very much, Mr. Chairman, for holding this hearing on such an important issue.

I thank our witnesses for their appearance before the committee and for their testimony today. Ms. Sherry, it is good to see you again.

Federal Government information systems are constantly under threat of cyberattack. And the incidence of cyberattacks has escalated in recent years. It is critical that we maintain strong defenses to those attacks.

The Department of Homeland Security is responsible for the cybersecurity of most of the executive branch agencies. It is also responsible for protecting its own information systems from attack.

Our success at keeping our information systems safe depends on how well the Department executes internal controls over its components. Today we examine the weaknesses in the Department's internal controls and how we can eliminate them to improve defenses against present and future threats.

In fiscal year 2010, the auditors from KPMG listed more than 161 findings, as the chairman mentioned. The audit concluded that old legacy computer systems are impairing the functionality of DHS' financial management system as a whole. The audit also found many weaknesses in controlling access to sensitive data facilities and financial information in the Department.

These weaknesses go straight to the heart of protecting against outside threats and to equality of data that feeds the DHS financial system. I would like to get answers to at least two issues from this hearing today. First, what progress has the Department made in the months since the audit report was issued in addressing material weaknesses and IT control deficiencies that were identified? Second, what is the status of updating and integrating your old legacy computer system that is impairing financial accountability in the Department?

As the Department successfully works through these issues, we should begin to see a decrease in internal control weaknesses over financial reporting and increased protection over information system from threats within and outside of the United States. This committee is here to assist you. This is not one of those “I gotcha” committees, even though they do exist here in this House. But this is not one. We are here to see how we can work together and to see how we can help you. And I know it, because at one time I was chairman, and the chairman was ranking. And now you can see he is chairman and I am ranking. So we have been working on this for quite some time and we are willing to continue to work with you.

On that note, I yield back and I recognize the schedule, Mr. Chairman, and I am willing to cooperate with you in every way I can to make certain that we follow it.

[The prepared statement of Hon. Edolphus Towns follows:]

Opening Statement
Rep. Edolphus Towns, Ranking Member
Hearing on "Internal Control Weaknesses at the Department of Homeland Security"
Subcommittee on Government Organization, Efficiency and Financial Management
October 27, 2011

Mr. Chairman, I thank you once again for holding this hearing on such an important issue. I thank our witnesses for their appearance before this committee and for their testimony. Ms. Sherry, it's good to see you again.

Federal government information systems are constantly under threat of cyber-attack, and the incidence of cyber attacks has escalated in recent years. It is critical that we maintain strong defenses to those attacks. The Department of Homeland Security is responsible for the cybersecurity of most of the executive branch agencies. It is also responsible for protecting its own information systems from attack.

Our success at keeping our information systems safe depends on how well the Department executes internal controls over its components, and its oversight over internal controls throughout the executive branch. Today we examine the weaknesses in the Department's internal controls and how we can eliminate them to improve defenses against present and future threats.

In fiscal year 2010, the auditors from KPMG listed more than 161 findings of concern. The audit concluded that old, legacy computer systems are impairing the functionality of the DHS financial management system as a whole. The audit also found many weaknesses in controlling access to sensitive data facilities and financial information in the department. These weaknesses go straight to the heart of protecting against outside threats and to the quality of data that feeds the DHS financial statement.

I want to get answers to at least two issues from this hearing: First, what progress has the department made in the months since the audit report was issued in addressing material weaknesses and IT control deficiencies that were identified. Secondly, what is the status of updating and integrating your old legacy computer systems that is impairing financial accountability in the Department?

As the Department successfully works through these issues we should begin to see a decrease in internal control weaknesses over financial reporting and an increase protection of our information systems from threats within and outside of the United States. This committee is here to assist the department in getting through these issues for the protection of our federal government. Let us know how we can help.

Mr. PLATTS. I thank the gentleman, and I appreciate your very appropriate remarks, that our effort is about partnering, partnering between us in a non-partisan way, as chairman and ranking member, chairman and ranking member reversed in the past, and with you, and that we are all after that same goal.

We are delighted to have several very distinguished witnesses before us who bring great insights into the issues that we are addressing here today. We are going to first start with Ms. Peggy Sherry, Deputy Chief Financial Officer, as well as Acting Chief Financial Officer at the Department of Homeland Security; Mr. Robert West, Chief Information Security Officer at the Department; Mr. John McCoy, Deputy Assistant Inspector General for Audits at the Office of Inspector General for the Department of Homeland Security.

If I could, it is the practice of the committee that we swear in all of our witnesses. So if I could ask the three of you to stand and raise your right hands.

[Witnesses sworn.]

Mr. PLATTS. Thank you. You may be seated. The Clerk will reflect that the witnesses answered in the affirmative. And again, I apologize for the abbreviated introductions. But to try and accommodate everyone's schedules, we will go to your testimony. If you can try to limit it to about 5 minutes, your full testimonies are submitted for the record. Then we will get into questions.

Ms. Sherry, if you could begin?

STATEMENTS OF PEGGY SHERRY, DEPUTY CHIEF FINANCIAL OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY, ACCOMPANIED BY ROBERT WEST, CHIEF INFORMATION SECURITY OFFICER; AND JOHN E. McCOY II, DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF PEGGY SHERRY

Ms. SHERRY. Thank you very much. Thank you, Chairman Platts, Ranking Member Towns and members of the committee, for the opportunity to provide information on the fiscal year 2010 audit findings and the processes that have been put in place to correct our internal control weaknesses.

When DHS was formed, our initial audits identified pervasive material weakness conditions in the financial systems security controls across all DHS components. There was strong partnership between my office and the Chief Information Security Officer. We have been successful in correcting many IT control risks. And by fostering a positive working relationship with the Office of the Inspector General and our external auditors, we have been able to move the Department forward in addressing IT and financial management control weaknesses.

Over the past few years, we have significantly reduced IT material weakness conditions and largely contained them to three components. We expect this year's audit to reflect significant progress at the U.S. Coast Guard, FEMA and at ICE.

In addition to our strong partnership with the Chief Information Security Officer, we have also developed a focused approach to systematically evaluating the areas of greatest risk. Components developed action plans to target these high risk areas, and my office reviewed and provided input to ensure these plans are comprehensive, reasonable and address the root cause of our IT weaknesses.

Over the past 5 years, the Department has made significant progress improving our internal control environment, including the IT environment. During 2007 and 2008, the CFO and CISO worked together to build an internal control program to assess controls over our CFO-designated systems. We provided comprehensive guidance to the entire Department on how to secure financially significant systems.

In 2009, we used that guidance to perform a baseline IT internal control assessment at many of our components. This assessment included testing the design and effectiveness of IT controls. Due to the repeating nature of some IT findings, in fiscal year 2010, we focused on ensuring that the Department's IT plans of action were addressing and designed to address the root causes of the most material IT findings. And we used independent verification and validation techniques to ensure corrective actions were being implemented across the IT control environment.

This targeted approach allowed us to address many of the causes of repeat IT NFRs with the goal of permanent correction. I would like to highlight some of the work undertaken this year to address specific component findings. The U.S. Coast Guard has created an oversight process to identify and evaluate systems scripts or computer processing code that have an impact on financial statements. The Coast Guard also updated their policies and procedures, developed a desk guide to provide training and created a segregation of duties policy.

Along with my office and Mr. West's office, the FEMA CFO and CIO worked very closely this year, and as a result, significant progress in closing system audit findings occurred. They instituted a recertification process for users of the National Emergency Management Information System and remediated many control deficiencies surrounding the National Flood Insurance program.

ICE also made progress this year, and in the coming months, they will be updating their data base server. This improvement will make needed corrections in ICE's financial system, and along with increased training and user awareness provide greater controls against duplicate payments in the future.

This is just some of the work our components continue to do to remediate control deficiencies and demonstrate progress to adhere to the tenets of the Financial Accountability Act. Even though the Department has shown significant improvement over the past few years in financial Management and in improving systems security, financial management remains challenging as a result of IT functionality limitations in certain financial systems.

Some legacy systems limit our ability to develop application controls to support financial reporting and operations, limit our ability to provide timely and accurate data, and contribute to inefficient labor-intensive processes and the need for extensive workarounds and compensating manual controls. Limitations include lack of integration in some of our systems, IT system configuration limitations, systems lacking key application controls, which are more efficient and effective and reliable than manual controls. These conditions hinder our ability to provide sustainable internal controls to support the audit as well as to ensure our control systems are designed to achieve our missions, which is another key objective of the Financial Accountability Act.

These weaknesses highlight the need to modernize certain legacy systems, and this remains a priority for the Department. While we work with components to develop a path forward, we continue to help them to improve and standardize their business processes and internal controls. We are implementing a common line of accounting and we are developing common data standards, all very critical.

Using the objectives outlined in the Accountability Act, we continue to make significant progress in improving financial Management. I am fortunate to work with the dedicated staff at DHS, as well as have the support of Department leadership and the Chief Information Security Officer and our auditors, as we continue these efforts.

I thank you for and appreciate the efforts we have received from this committee and Congress, and I look forward to working with you in the future. I am happy to take questions later, sir.

[The prepared statement of Ms. Sherry follows:]

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.

Mr. PLATTS. Thank you, Ms. Sherry.

Mr. West.

STATEMENT OF ROBERT WEST

Mr. WEST. Chairman Platts, Ranking Member Towns and members of the committee, thank you and good morning. I am Robert West, Chief Information Security Officer for the Department of Homeland Security, and I would like to provide you an update on the Department's progress in addressing the Department's IT financial management control weaknesses. Department leadership takes all audit findings seriously and we are fully committed to resolving these issues as quickly as possible.

First, I would like to acknowledge the progress that we have made in improving the Department's overall IT security posture since the standup of the Department in 2003. Over the last 8 years, we have reduced both IT security risks and costs by successfully transitioning from a highly decentralized IT environment to a modern enterprise ecosystem, with a robust set of shared services and common security controls.

DHS inherited a complex legacy environment that included approximately 1,100 separate and unique IT systems and one where each system owner was individually accountable for all security controls. Today, our IT systems are more secure than ever before, due in large part to the fact that we have instituted an enterprise security architecture. We call it mission assurance through defense in depth.

We have consolidated six legacy wide area networks into a single, secure, modern, fully encrypted backbone infrastructure, and we have also made significant progress in consolidating multiple data centers into two modern enterprise data centers. These new data centers have been designed also with a robust set of security controls that support all systems, including financial systems that operate in these environments. We have also consolidated our internet access behind redundant trusted internet connections.

Within this enterprise environment, the Department today operates 783 systems in support of the various missions of the Department, and 32 of these systems support the Department's financial management and reporting and are considered material to the financial statements. Most of these financial systems have been in operation for many years, and they predate the Department's creation in 2003.

While these systems are certainly more secure due to the fact that they operate within the enterprise environment that I explained, some of these systems are still missing a number of important systems-specific controls, and cannot fully support business processes that ensure accurate financial reporting. Heavily manual processes are still required to compensate for a lack of fully automated technical controls, highlighting the need to modernize these legacy systems.

Second, I would like to briefly discuss the nature of audits themselves. Auditors necessarily report what they observe. And often those reported observations are only symptoms of larger issues. For this reason, the Department not only systematically reviews all notice of findings and recommendations with component leadership, we also require at least one action plan for each finding issued. Additionally, we also have institutionalized a three-phased approach to identify and better understand systemic issues. This approach includes a current state assessment, root cause analyses and independent validation and verification of component action plans by the Department.

We have also provided root cause analysis training to components, so they can better develop realistic corrective action plans that address root causes.

Finally, significant weaknesses identified in the 2010 IT management letter center around five key areas: access controls, configuration management, security management, contingency planning and segregation of duties. I have outlined specific actions taken to address each of these areas in written testimony. I would be happy to discuss each of those in more detail if you desire.

In closing, I would like to reiterate that the Office of the CIO, including my office, along with the Office of the Chief Procurement Officer, Program Accountability and Risk Management Office and all appropriate component offices are working closely together to ensure financial modernization projects are planned and executed to meet reporting requirements and minimize costs for financial operations. DHS remains fully committed to improving our financial systems security in order to provide timely, accurate and complete financial information to our key stakeholders, including you, the Congress, and the American taxpayers.

Thank you.

Mr. PLATTS. Thank you, Mr. West.

Mr. McCoy.

STATEMENT OF JOHN E. McCOY II

Mr. MCCOY. Good morning, Mr. Chairman, Ranking Member Towns and members of the committee. I am John McCoy, II, Deputy Assistant Inspector General for Audits with the Department of Homeland Security.

Thank you for inviting me today to discuss financial management weaknesses at DHS. My testimony today will focus on information technology [IT] issues, identified during the fiscal year 2010 financial statement audit conducted by the independent accounting firm, KPMG.

In fiscal year 2010, KPMG identified 161 IT deficiencies, of which approximately 65 percent are repeated from fiscal year 2009. KPMG also noted that DHS's financial systems had many functional limitations that affect the Department's ability to implement and maintain internal controls.

From a financial statement perspective, DHS's five most significant weaknesses are access controls, configuration Management, security management, contingency planning and segregation of duties. KPMG noted access control weaknesses at several of the DHS components that allowed excessive potential for unauthorized access to key financial systems. Also at several of the components, KPMG observed configuration management controls that were not fully defined, followed or effective.

Security management weaknesses were identified at several DHS components where financial systems as well as general support systems were not properly certified and accredited. KPMG also found scenarios where roles and responsibilities were not clearly defined, a lack of policies and procedures and non-compliance with existing policies.

KPMG noted weaknesses in continency planning. There were instances of incomplete or outdated business continuity plans, systems with incomplete or outdated disaster recovery plans. Some plans were not adequately tested and did not contain current system information, emergency processing priorities or procedures for backup and storage.

At several of the DHS components, KPMG noted a lack of proper segregation of duties for roles and responsibilities within financial systems. Collectively, these IT control deficiencies limited the Department's ability to ensure the confidentiality, integrity and availability of critical financial and operational data. KPMG considers these control deficiencies to collectively represent a material weaknesses for DHS under established professional auditing standards.

The fiscal year 2010 audit also looked at the functionality of DHS's financial systems. Many of the Department's financial systems have not been substantially updated since the creation of DHS. Some components cannot modify IT system core software or install controls to prevent duplicate payments. This contributed to duplicate payments made by Immigration and Customs Enforcement in fiscal years 2009, 2010 and 2011. These and other IT system limitations also lead to extensive manual and redundant procedures to process transactions, verify the accuracy of data and prepare financial statements.

DHS has made several attempts to modernize its financial systems. Its most recent initiative was the Transformation and Systems Consolidation [TASC]. TASC was canceled in March 2011 after the Government Accountability Office sustained one of the bid projects. GAO recommended that DHS reevaluate the requirements with regard to the estimated scope and pace of work, as well as the integrated solution requirement.

In September, the Under Secretary of Management announced the Department would now pursue a decentralized approach instead of an enterprise-wide solution. Implementation of a new financial systems solution combined with improving IT security controls should allow the Department to achieve greater effectiveness in its financial management.

We will continue our positive working relationship with the Department by taking a proactive approach to overseeing DHS's financial management and IT security improvement efforts. We look forward to continuing our audit efforts and providing the results and solutions to the Secretary and to the Congress.

Mr. Chairman, this concludes my prepared statement. Thank you for this opportunity. I welcome any questions from you or the Members.

[The prepared statement of Mr. McCoy follows:]

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you on behalf of the Department of Homeland Security (DHS) Office of Inspector General (OIG). My testimony today will focus on information technology (IT) issues discovered during the fiscal year (FY) 2010 financial statement audit. The information provided in this testimony is based on the report: *Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit (OIG-11-103).*

We engaged the independent accounting firm of KPMG, LLC to perform an integrated financial audit of the DHS, which included an evaluation of the following IT controls and issues:

- General controls of DHS' financial processing environment as defined by the Federal Information System Controls Audit Manual (FISCAM).
- Technical security for development and production devices that directly support key general support systems.
- Application controls on a limited number of DHS' financial systems and applications. Application controls are the structure, policies, and procedures that apply to supporting systems, such as inventory and payroll.
- Financial system functionality.
- Physical security, e.g. physical access to media and equipment that could be used to gain unauthorized access to financial systems.

DHS Financial Systems Progress and Challenges

DHS made some progress in remediating the IT findings reported in FY 2009, which resulted in the closure of approximately 30 percent of the prior year IT findings. In FY 2010, KPMG identified 161 findings, of which approximately 65 percent are repeated from FY 2009. In addition, DHS' financial systems have many functional limitations that affect the Department's ability to implement and maintain internal controls.

IT General Control Issues

From a financial statement perspective, DHS' five most significant weaknesses are: (1) Access Controls, (2) Configuration Management, (3) Security Management, (4) Contingency Planning, and (5) Segregation of Duties.

Access Controls protect information from unauthorized modification, loss, and disclosure by limiting access to data, programs, and facilities. At several DHS components KPMG noted excessive potential for unauthorized access to key financial applications. For example, system administrator access to financial applications was not properly restricted and strong password requirements were not enforced. KPMG observed ineffective safeguards over physical access to sensitive facilities and resources such as government credit cards, passwords, and laptops. KPMG also used social engineering to attempt to manipulate individuals into divulging sensitive information or allowing computer system access. During the audit, some DHS employees provided their system user names and passwords to an auditor posing as a help desk employee.

Configuration Management controls help ensure that systems are operating securely. At several components, KPMG observed configuration management controls that were not fully defined, followed, or effective. For example, KPMG found a lack of documented policies and procedures to prevent users from having concurrent access to the development, test, and production environments of financial systems. In addition, configuration, vulnerability, and patch management plans were not implemented, or did not comply with DHS policy.

Security Management controls provide a framework for managing risk, developing security policies, and monitoring the adequacy of computer-related security controls. At several DHS components KPMG noted that financial systems as well as general support systems were not properly certified and accredited. KPMG also found scenarios where roles and responsibilities were not clearly defined, and a lack of policies and procedures and compliance with existing policies. For example, procedures for exit processing of contractors had not been established, and procedures for IT-based specialized security training were not in place.

Contingency Planning controls involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur. KPMG noted instances of incomplete or outdated business continuity plans and systems with incomplete or outdated disaster recovery plans. Some plans were not adequately tested and did not contain current system information, emergency processing priorities, or procedures for backup and storage.

Segregation of Duties controls constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations. At several DHS components, KPMG noted a lack of proper segregation of duties for roles and responsibilities within financial systems. For example, financial system users had conflicting access rights as the Originator, Funds Certification Official, and the Approving Official. In addition, policy and procedures to define and implement segregation of duties were not implemented.

Collectively, these IT control deficiencies limited DHS' ability to ensure the confidentiality, integrity, and availability of critical financial and operational data. KPMG considers them to collectively represent a material weakness for DHS under standards established by the American Institute of Certified Public Accountants and the Government Accountability Office.

Financial System Functionality Issues

Many of the Department's financial systems have not been substantially updated since the creation of DHS. In some cases, financial system functional limitations are negatively affecting DHS' ability to implement and maintain strong internal controls, especially in the areas of financial data processing and reporting. For example, some components cannot modify IT system core software or install controls to prevent duplicate payments. This contributed to duplicate payments made by Immigration and Customs Enforcement (ICE) in FYs 2009, 2010, and 2011. These and other IT System limitations also lead to extensive manual and redundant procedures to process transactions, verify the accuracy of data, and prepare financial statements.

Component IT Financial Systems

For FY 2010, we issued separate IT management letter reports for the United States Citizenship and Immigration Services (USCIS), the United States Coast Guard (Coast Guard), Customs and Border Protection (CBP), the Federal Emergency Management Agency (FEMA), the Federal Law Enforcement Training Center (FLETC), ICE, and the Transportation Security Administration (TSA). We also issued an overall consolidated IT management letter report that summarized the IT issues for all seven components. Each management letter addressed component-level IT security issues and provided individual findings and recommendations. KPMG recommended that the components' chief information officers and chief financial officers work with the DHS chief information and chief financial officers to address the issues noted in the reports.

USCIS

During FY 2010, USCIS took corrective action to address prior year IT control deficiencies such as physical controls at the Manassas Data Center, and access controls over security software. However, during FY 2010, KPMG continued to identify IT general control deficiencies that could potentially impact USCIS' financial data. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System configuration and patch management, and deficiencies within the Computer Linked Application Information Management System (CLAIMS) 3 LAN and CLAIMS 4 user account management. Collectively, the IT control deficiencies limited USCIS's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability.

Of the 14 findings identified during our FY 2010 testing, 3 were new IT findings. These findings represent control deficiencies in four of the five FISCAM key control areas: configuration management, access controls, segregation of duties, and security management. Specifically, these control deficiencies include: (1) a lack of strong password management and audit logging within the financial applications, (2) security management issues involving staff security training and exit processing procedure weaknesses, (3) inadequately designed and operating configuration management, and (4) the lack of effective segregation of duties controls within financial applications.

Coast Guard

During FY 2010, KPMG determined that the Coast Guard remediated eight IT findings identified in previous years. Specifically, the Coast Guard took actions to improve aspects of its user recertification process, data center physical security, and scanning for system vulnerabilities. The Coast Guard's remediation efforts have enabled KPMG to expand test work into areas that were not practical to test previously, considering management's acknowledgment of the existence of control deficiencies.

During FY 2010, KPMG identified 28 IT findings, 10 of which were repeat findings from the prior year and 18 were new findings. Most of the new findings relate to IT systems that were added to the examination scope this year. Collectively, these findings represent deficiencies in four of the five key control areas, including security management, access control, segregation of duties, and configuration management.

KPMG also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems are not compliant with the *Federal Financial Management Improvement Act* and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control weaknesses and strengthening the control environment at the Coast Guard. The majority of the findings indicate a lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS Sensitive System Policy Directive 4300A requirements and National Institute of Standards and Technology guidance. Since key Coast Guard financial systems house TSA financial data, deficiencies identified in the Coast Guard's IT environment also impact TSA.

CBP

During FY 2010, CBP remediated 13 IT findings identified in previous years and took corrective action to address prior year IT control weaknesses. For example, CBP made improvements over various system logical access processes and system security settings, and system administrator access processes and procedures. CBP also performed more consistent tracking of contractors and system user rules of behavior agreements. However, during FY 2010, KPMG identified 23 IT findings, of which 16 were repeat findings from the prior year and 7 were new findings. Collectively, these findings represent deficiencies in security management, access control, and segregation of duties, as well as deficiencies related to financial system functionality. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and CBP financial data could be exploited, thereby compromising the integrity of financial data used by management and reported in CBP's financial statements.

FEMA

During FY 2010, FEMA took corrective action to address certain prior year IT control weaknesses. For example, FEMA made improvements over implementing certain logical and physical access controls over National Flood Insurance Program information systems, as well as development and maintenance of the inventory of FEMA Chief Financial Officer-designed financial management systems. However, during FY 2010, KPMG continued to identify weaknesses that could potentially impact FEMA's financial data. Some of the most significant weaknesses from a financial statement audit perspective related to controls over security management, access control, configuration management, and contingency planning, as well as weaknesses over physical security and security awareness. Collectively, these weaknesses limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. Of the 63 findings identified during our FY 2010 testing, 50 were repeat findings, either partially or in whole from the prior year, and 13 were new IT findings. In FY 2010, disagreements with management's self assessment on the status of repeat findings occurred almost entirely at FEMA. As reported by KPMG during audit status briefings to the OIG and management, this condition did not repeat in FY 2011.

FLETC

During FY 2010, FLETC took corrective action to address prior year IT control weaknesses, such as improvements over configuration management in Momentum and the Glynco Area Network and management review over Momentum auditing logs. However, during FY 2010, KPMG continued to identify IT general control weaknesses that could potentially impact FLETC's financial data. The most significant weaknesses were related to the Glynco Area Network logical access controls and weaknesses over physical security and security awareness. Collectively, the IT control weaknesses limited FLETC's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. Of the six findings identified during our FY 2010 testing, one was a new IT finding. These findings represent control deficiencies in configuration management, security management, and access controls.

ICE

During FY 2010, ICE took corrective action to address some prior year IT control weaknesses. For example, ICE made improvements over physical controls at facility entrances, and Active Directory Exchange user account lockout settings and recertifications. However, during FY 2010, KPMG continued to identify IT general control weaknesses that could potentially impact ICE's financial data. The most significant findings from a financial statement audit perspective were related to the Federal Financial Management System configuration, patch management and user account management and weaknesses over physical security and security awareness. Collectively, the IT control deficiencies limited ICE's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability.

Of the 16 findings identified during our FY 2010 testing, 9 were new IT findings. These findings represent control deficiencies in 4 of the 5 key control areas: configuration management, access controls, security management, and segregation of duties.

TSA

During FY 2010, TSA took corrective action to address prior year IT control deficiencies. For example, TSA made improvements in its policies and procedures over its configuration management monitoring controls related to the development, implementation, and tracking of scripts at Coast Guard's Financial Center. However, during FY 2010, KPMG continued to identify IT general control deficiencies that impact TSA's financial data. Of the four findings issued during FY 2010 testing, three were repeat findings and one was a new IT finding. These findings represent deficiencies in three of the five FISCAM key control areas. Specifically, the deficiencies were: (1) unverified access controls through the lack of comprehensive user access privilege re-certifications, (2) security management issues involving the terminated employee process, and (3) physical security and security awareness issues.

KPMG also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems that house TSA financial data are not compliant with the *Federal Financial Management Improvement Act* and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control deficiencies.

DHS Financial Systems Modernization

DHS has made several attempts to modernize its financial systems. It's most recent initiative was the Transformation and Systems Consolidation, or TASC. This initiative was intended as an enterprise-wide solution that would consolidate financial, asset and acquisition management systems for all of DHS. In March 2011, the TASC project was cancelled after the Government Accountability Office sustained one of the protests and recommended that DHS reevaluate its requirements with regard to the scope of work covered by the solicitation, and if appropriate, issue a revised request for proposals to appropriately reflect the Department's actual requirements. In September, the Under Secretary of Management announced that the Department would pursue a decentralized approach instead of an enterprise-wide solution like TASC. The new approach will prioritize system modernization for components with the most critical need. The implementation of a new financial systems solution combined with improving IT security controls should allow the Department to achieve greater effectiveness in its financial management.

We will continue our positive working relationship with the Department by taking a proactive approach to overseeing DHS' financial management improvement efforts. We look forward to continuing our audit efforts and providing the results and solutions to the Secretary and the Congress.

Mr. Chairman, this concludes my prepared statement. Thank you for this opportunity and I welcome any questions from you or Members of the Subcommittee.

Mr. PLATTS. Thank you, Mr. McCoy. Again, thanks to all three of you for your testimony here today, as well as your written testimony. Having that in advance certainly allowed me to be better prepared for today's hearing.

I guess I want to start, one of the things that jumps out, and Mr. McCoy just referenced it in his testimony, the 65 percent repeat deficiencies. This is the 2010 fiscal year that we are still looking at, 2011 has just ended. If each of you would want to comment based on the best of your ability at this point, what are we likely to see on the 2011 audit regarding repeat deficiencies, and what progress are we making?

In the ones that are identified, we are doing a better job of closing them and shrinking that number, because we did start, as you referenced, Mr. West, in the legacy systems, some dramatic challenges. I think 18 material weaknesses when the Department was first formed. But that was 8 years ago. And we are now 8 years later. So if each of you could comment on the issue of the repeat weaknesses and what to expect in the coming audit.

Ms. SHERRY. Thank you, Chairman. Yes, that is something that clearly, Mr. West and I, when we had seen the number of the repeat findings, was something that we really realized that we did have to address. I think that the process that we have used over the last 5 years has really gotten us to the point where we will see some success this year, we will see more remediation.

In particular, you will notice that the IG and the KPMG had pointed out that FEMA in particular had had issues in this area. As far as part of the process they identified at the beginning of the year, do they think they have actually corrected a particular finding? FEMA in particular had identified things that they thought were corrected, which in fact were not corrected.

One of the approaches that we used this year for the last few years was really to identify, work very closely with the components to see if they were identifying the root causes of the NFRs. As Mr. West pointed out, sometimes it is just a symptom, it doesn't really point to exactly the reasons why you are having particular weaknesses.

So his office and my office worked very closely with the CIO over at FEMA, as well as the CFO, which was a new paradigm for us. We had been working very closely together. Clearly it has worked well for the Department, encouraging the components to do that as well. So they worked very closely. And I think that what you will see this year is FEMA really was able to better assess which of those NFRs they would be able to correct. The reason they were able to do that is because they were, to be able to address the root causes, they were also able to work with their business partners within FEMA to really identify what those root causes are. So I think that what you will see this year is improvement in that particular area.

Mr. PLATTS. I appreciate the focus on FEMA. I think over a third of the deficiencies are FEMA, and I think 80 percent of FEMA's are repeat deficiencies.

Ms. SHERRY. That is exactly right.

Mr. PLATTS. So that focus, I think, in the big picture helps, and hopefully that carries across all the component agencies.

Ms. SHERRY. Yes, sir.

Mr. PLATTS. Mr. West or Mr. McCoy.

Mr. WEST. Yes, sir, I would like to make two comments. One, I don't want to minimize the importance of the findings, and we take all findings seriously. Our goal is to close all audit findings. We use the fact that some are associated with a material weakness as a way to prioritize our efforts.

Mr. PLATTS. Right.

Mr. WEST. But any finding is something that needs to be closed. And I want to acknowledge that up front.

I haven't said that, when you look at the way the process works, unlike the FISMA audit, which is my other world, the FISMA audit is generally a snapshot in time, and it is just, this is the state of the program at a given date. With the financial systems audits, we have to show the auditors, we have to convince the auditors that controls have been effective for the entire audit cycle, generally a year, before we can close them.

So the way the process works is that there will be a notice of findings and recommendations, sometimes with maybe as many as seven or eight specific findings within that one NFR. We remediate. At some point we believe that we fix the problem and we assert the next audit cycle back to the auditors that we think this is closed. The auditors then review that, and they can either agree and close the audit, they can—six of eight are closed, but you still have work to do. Or they in some cases even will get, a number of cases, frankly, will get audit, NFRs issued, whereas it is findings with no recommendations, meaning okay, we think the controls you have put in place are good, you have solved the problem, but we can't rely on it for the entire audit cycle, the whole year.

So when we get repeat findings, I would temper that just a bit. I don't want to downplay it. Like I say, we take them all seriously. But there is an audit pace that goes with these. And it is generally 1 or 2 years before you actually get to the point where something is fully closed with the auditors.

The second thing I want to mention real quick is with FEMA. The thing that I think, the issue in 2010 with FEMA being the large majority is that the way that they were looking at NFRs at that time, they were really kind of looking at them more from a FISMA perspective, as I talked about. So with the CFO and my office together, we went into FEMA, we did some training and the CFO and the CIO at FEMA really, they instituted a whole program around how to review NFRs before they make assertions back to the auditors that the findings have been closed.

They put that process in place and the auditors can verify this, but in my view what FEMA is doing today in that regard is the best practice for the government. And as a result, I can't speak for the 2011 audit, we are still in the middle of it. I really don't know how we are going to end up. I hope we will end up, I am confident we will end up in a better place. But I think with FEMA, you will see significant progress for that very reason.

Mr. PLATTS. Good. Mr. McCoy.

Mr. MCCOY. Yes, sir. We are identifying this year that the Department is making progress. As Mr. West said, the audit is ongoing. It will be over in approximately 2 weeks. At that point in time we will be issuing the report. We have identified improvement at FEMA. Last year, as noted in the report, FEMA said they had closed 80 percent plus of their NFRs at the beginning of the audit of those they identified, and KPMG disagreed with that. This year, all the ones that KPMG has completed looking at, KPMG concurs with management that the findings have in fact been closed. There is definite improvement this year.

Mr. PLATTS. Thank you. I yield to the ranking member.

And my intent is, the votes just went up. There is going to be one vote and then debate, motion to recommit debate, and then another series of votes. What my intent is is to go to about a quarter of, just get what we can in. I am going to go over, cast one vote, come back and it may just be me coming back, depending on the schedule. Because we will have maybe another 25 minute window, so you are not here waiting very long, come back, have another 20, 25 minutes, and then we will wrap up when we get back for the final series.

With that, I yield to the ranking member.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Ms. Sherry, I guess I will start with you. Given the absence of an integrated, streamlined financial management program at FEMA, will FEMA continue to produce a reliable financial data using its current information technology system, which is still antiquated?

Ms. SHERRY. Yes, sir, you make a very good point. FEMA's system is old, it is outdated, it is proprietary. I believe it is not even supported at this particular point.

FEMA, like many of the components where they have a legacy system that is not completely modernized, either with the right patches in it, in the right configuration management, they have to have various compensating controls or manual controls, things that are outside of those application controls within a well-performing system in order to be able to compensate for some of those weaknesses. So FEMA is able to attest and represent to their balances at this particular point.

As you know, sir, we are still just doing a balance sheet audit, as well as the custodial statement. But at this point, they are able to do it. But with a modern system, it would clearly be a more efficient process and one that would not have to, you would have to develop audit trails outside of the system. Instead, the auditors should be able to rely on those audit trails within the system, if you have strong application controls. So again, it is just not as efficient a process, and there are manual controls that are required, which is, as you know, are subject to, they are prone to errors, maybe not as accurate and certainly not as timely.

Mr. TOWNS. Right. Let me ask this. If there is a situation where the auditor comes in and they make these recommendations and you feel that it is really not necessary, that your information is accurate and that there is no need to make any changes, what happens in a situation like that? Right down the line.

Ms. SHERRY. I will start real quickly. We have been very, very fortunate. Since I have been at the Department, for a little over 4½ years, we have had an incredible relationship with the IG, as well as with our external auditors. They have made every effort to get to know the component very well, and we have made every effort in my office to be able to make sure that we had a real good understanding of exactly what those recommendations are.

So I am happy to report that there are, there really are not times where we just absolutely disagree with the auditors. As Mr. West had pointed out, many times your notice of finding of recommendations really highlights certain conditions. Sometimes they don't necessary go to the root cause.

One of the best practices that the auditors implemented this year, actually maybe even last year, was to have the Department really take a look at what those root causes are. So what they do is when they give us a particular finding, they don't necessarily come right out and give you the road map on how to fix this. This has been really important in really developing competencies within the Department, really training people and really, how do you understand what is in that hot notice of finding of recommendation and how do you go about fixing it.

So I am pleased to report that we really don't have disagreements with the auditors. They may not prescribe necessarily how we go about fixing something, leave it up to the Department to figure that out. And really the way we have been working since I have been with the Department, really building those competencies, so that we are able to address it, with recommendations that are actually going to fix the problems.

Mr. TOWNS. Mr. West, do you want to comment on that?

Mr. WEST. Yes, sir. I would make two comments. I would agree with Ms. Sherry completely about the auditors. I think we have really been fortunate in that we had a lot of continuity in the IG office for a number of years, pretty much since the beginning, as well as with the financial auditors, KPMG. It is the same audit team, with a few exceptions, or few changes, I guess, the same audit team has been our financial auditors for a number of years. As a result of that, we have gotten to know them and we have a very close working relationship as a result of that.

The other thing I would say is that, I would agree with Ms. Sherry, there are very few times when there is just disagreement. And we generally sit down and work through what the issue is. And we generally come to an agreement.

The one area where, in the past, maybe there has been, and this is going back to FEMA again, has been an issue that we have resolved in policy actually now, is around FISMA and the audit standards for FISMA and with the NIST standards, National Institute of Standards and Technology standard. And then the FISCAM, or the Financial Information Security Controls Audit Manual, published by GAO. And they really are coming at it from different perspectives. So we think something is good in the FISMA world, but there are additional things we need to do to be able to show controls were effective for the entire year, for example.

So as a result of that, we have actually modified policy. We have systems that we believe are material to the financial statement, we call them in policy CFO-designated financial systems. And we put additional requirements in policy specific to those systems, so there really is no confusion. I won't say no, but we have really minimized the confusion. Generally when the auditors say this is an issue, they are referring back to our policy, and it is something that we would agree with.

Mr. TOWNS. Do you want to add?

Mr. MCCOY. Yes, sir. As Ms. Sherry indicated, 2 years ago we started the policy of having the Department evaluate the NFR and come up with the best recommendation or the best way that the Department could remediate it. Management knows their core businesses better than the auditors. We identify the condition, but we may not always identify the root cause. So that definitely improved the remediations in 2009 and 2010, as well as 2011.

Also I think this year, with the Department's involvement at FEMA, it has produced more of a culture change related to the financial statement audit and improvements with the financial statement NFRs and remediation . So there has definitely been improvement this year at FEMA.

Mr. TOWNS. I am happy to hear that, because looking at it from the outside, you would think that even if recommendations are made that there would come a dispute and it would take years and years to work it through. So I am happy to know that is not the case.

On that note, Mr. Chairman, I yield back.

Mr. PLATTS. I thank the gentleman.

Picking up on that issue, not so much disagreements between the Department and auditors, but the relationship between the Department and the components. One of the things I think that has helped get us heading in a strong direction is the relationship between Mr. West, Ms. Sherry, the two of you partnering and working hand in hand at the Department level. I think that has paid great dividends and will continue to. I thank you for that approach and that leadership you are providing.

One of the challenges you have is you are called to testify here about the audits of the Department, and the challenge is in the audits of some of the specific components, FEMA in particular, ICE, Coast Guard. The relationship that you have with your counterparts, or I would say subordinates, they might not see it that way, but for the CFO at FEMA, CIO at FEMA or ICE, can you share, I guess, is there a chain of command that has been strengthened within the Department that, if you as acting CFO for the Department contact FEMA CFO about remediation requirements or whatever it may be in this area, that it is seen as that individual being given in essence an order or marching orders from a superior?

Ms. SHERRY. Yes, Chairman. I am happy to say that in the time that I have been at DHS, what I have really seen is a great evolution in that relationship. I do believe that the CFOs, the components, the CIOs as well as the security officers and the chief financial officers within each of the components do look to the Department really to set the tone on overall financial management and are not out there basically trying to circumvent the policies of the Department.

We do this in many ways. We meet at the beginning of the year and then we meet periodically throughout the year to really jointly set what our strategic plan is for the Department. What we do is we set out what our objectives are. At the beginning of last year, we set out the very aggressive goal of obtaining a qualified opinion this year on our balance sheet. The primary reason we needed to do that is because we want to be able to have a full scope audit. Recognizing I was never going to be able to bring the Department to that, to be able to have that additional scrutiny over all of our statements until such time as we got a balance sheet, we jointly set out, all the CFOs jointly set out in our strategic plan was to be able to obtain a qualified opinion this year, which meant that, in particular the Coast Guard had a lot of work to do. But many of the other components had their objectives as well that they really needed to achieve.

And then what we do is, we have statements that they sign off on to be able to agree to these particular goals. And the we meet with them periodically on them. I am happy to report that we have very little difficulty being able to work together on our overall objective as a community in DHS.

Mr. PLATTS. That is good to hear. I guess a specific follow-up is, if in laying out that game plan, how to go forward, if you have, whether it is Coast Guard or FEMA, ICE, any of the component entities, that is not meeting what they need to do to have the overall departments succeed in this effort, how do you rectify that? Because you don't have any say in the hiring or firing of those component CFOs, is that correct?

Ms. SHERRY. Actually, the Department does have a role in being able to hire certain people within the components. That would include both the chief financial officer, the deputy chief financial officer and other key positions, such as the budget director.

Mr. PLATTS. So would you go to the Under Secretary?

Ms. SHERRY. Absolutely. And if I had any issues at this particular point, I have direct lines to the Secretary as well as the Deputy Secretary and the Under Secretary. In fact, I meet with the Deputy Secretary on a very regular basis. Every Thursday morning, we get together. There is a group of her key leaders that get together with her and meet with her on a myriad of financial management issues. Clearly over the last couple of months, one of those key issues has been the audit.

Mr. PLATTS. With the Deputy Secretary?

Ms. SHERRY. Yes, that is correct.

Mr. PLATTS. Each Thursday?

Ms. SHERRY. Absolutely. And then we meet on a less regular basis with the Secretary, but we get that information up to her as well. The Under Secretary for Management, we meet with him on a bi-weekly basis. We meet with him very regularly, but we meet with him on a bi-weekly basis on specific audit issues. And the Deputy Secretary has made, in fact, a statement that she made to me 45 days ago or so was that if there is any time that you need me to be able to "bang a head" she said you call me at any time. She said it doesn't matter when it is, if you need me to get behind you in order to be able to make sure that we achieve the objectives that we set out this year, you reach out to me.

Mr. PLATTS. I am glad to hear that, because that is one of the concerns, and we have seen it in the past with, Ranking Member Towns, I know you remember, NASA, a similar type challenge, where the administration at the senior level, but then you had all the separate NASA centers that weren't necessarily directly responding to the CFO. So I am glad to hear, that, and it also goes to the issue that we don't have, we are grateful for the great work you are doing, but a Senate-confirmed compliance with the statute as written, Senate-confirmed CFO, which I believe would give you even greater weight within the Department when you are out there with those component agencies. But I am glad to hear that the effort is to make sure that is what is happening from the top down.

I am going to try to squeeze one more in question in here. As I said, I am going to then run over, cast one vote, come back, have about 20 minute or so for a couple more questions, and then we will not hold you again, because it will be a little while after that before the vote series ends.

On the most significant weaknesses identified, access controls, and three in particular, access controls, segregation of duties, contingency planning, and I will maybe get into them in a little more detail when I come back. But I want to, I guess contingency planning, that one, this Department came out of the attack of 9/11. And the fact that we're a Nation under attack, and there was obviously an unprecedented emergency.

Yet we have this Department not setting an example for the rest of the Federal Government as we like it to to better prepare for those types of emergencies in how you manage your data, your information technology systems. So where are we and what do we need to do to address that, that DHS, out of all the departments and agencies, is a role model for contingency planning when it comes to information security?

Mr. WEST. Sir, I will speak to that. Specifically the financial systems in the 2010 audit, you are right, what can I say. But all systems, all financial systems and all NFRs associated with contingency planning in the 2010 audit, we went back directly to the components and said, you need to update your contingency plan, if you don't have one, you need to produce one. And every one of those systems now has a contingency plan that has been tested. We are still waiting on the results from the auditors as to how we close it out, with some exceptions. And those exceptions, we now have required a plan of action from each component for each system.

Mr. PLATTS. Which components or systems?

Mr. WEST. I would have to get back to you on the details, if you would like.

Mr. PLATTS. Okay.

Mr. WEST. But those, we do have plans of action for those. And we have given them 6 months. In some cases, big systems, there is a bit of a lift to get them, so we have given them 6 months. But within 6 months, those will all be remediated.

Mr. PLATTS. Okay, great. Good. I am glad to hear it. I think that is important, because again, setting that example, given how your department came to be formed in response to an emergency.

On the issue of, I will try to squeeze this in here quickly, segregation of duties. Again, it seems to me, I look at it as a more basic internal control, that you can't be the one approving the check and writing the check and then checking if the check, I mean, why are we failing in that regard? A fairly straightforward internal control.

Ms. SHERRY. I agree, Chairman, it is absolutely one of the most important internal controls that you should have. And I think there are two pieces of it. One is from a functional standpoint, what are those particular roles and responsibilities that someone should have that potentially could be in conflict, to cause an internal control weakness.

So kind of the best practice is, you shouldn't be able to certify a payment as well as initiate a p.o. or something, a purchase order or something. So the ability to be able to articulate what those conflicting roles are is very critical. The Department has been able to do that. We have done that for some time as part of our A123 process.

The difficulty gets into is when you are actually in the system. If you have a particular system that allows you to do those types of things. So in other words, you know you shouldn't enter a purchase order and then turn around and approve a payment. But if the system either does not have those preventive application controls in them, or they are not configured appropriately, there is the possibility that you could go in there and do that as well.

Mr. PLATTS. I assume we are trying to well identify those system weaknesses to then correct.

Ms. SHERRY. That is exactly right. And those are clearly what, those are the high risk ones. And one of the processes that we did, or our approach this year, over the last couple of years, in particular this year, was to really look at those high risk ones, such as segregation of duties. If you have a particular system that is not configured in a way that prevents you from doing that, where are those detective controls that you have out there.

So developing those policies and procedures, training people so that they know that those are incompatible responsibilities, and then to the extent possible, going in behind and making sure that something hasn't happened.

Mr. PLATTS. Get to that root cause.

Ms. SHERRY. Absolutely, yes, sir. That is right.

Mr. PLATTS. With that, we are going to stand in recess for about 10 minutes. And I will be right back.

[Recess.]

Mr. PLATTS. I didn't realize I could be that quick. [Laughter.]

I do appreciate your patience. On the floor, we have 10 minutes of debate and another series of votes, which means we probably have about 15 to 20 minutes before running back across.

The other issue, in addition to contingency planning, segregation of duties, is specifically the access control deficiency area. And maybe where we are on that, and I know with the new identification card and how that will play into trying to ensure that we are not allowing, and maybe especially the issue of former contractors or former employees who haven't been shut off after leaving the Department, if we could address that. Please, Mr. West?

Mr. WEST. Yes, sir. You are exactly right about the issue. The biggest issue with access controls as identified in the audit center around the inability in some cases to quickly remove or deactivate accounts when people either move on for whatever reason, either they are an employee and they have left the Department, moved to another department, or component within the Department, and especially contractors who, frankly, come and go with the contract.

So we have done some remediation work around that. The components have put processes in place to where they will review the account list, the approved account list on some periodicity. Generally it is like 90 days. I think in one case it may be 6 months. Don't quote me on that. But they have manual processes in place to review periodically the removal of accounts and determine which ones are still valid.

That is kind of a band-aid on a bigger issue. And as you mentioned, the Department is aggressively deploying HSPD 12 common access cards. And the goal is to get to the point where we can use those for mandatory logical access at some point. We are working on a plan to get to that as quickly as possible. The Deputy Secretary is very interested in that herself. The CIO and I also meet with her regularly and this is a key issue not just for financial systems but for the Department more generally.

And then once we have HSPD 12 cards, then we will be able to upgrade the individual applications to take advantage of that, so that we will be able to remove people in more real time. But I think until we have that identity capability on sort of a core infrastructure, until we have that, we are going to still have to rely on these manual processes, reviewing access lists periodically like we are doing today.

Mr. PLATTS. And the periodic 90-day review, double checking that no one is still on that list, ideally you get to where it is more automated, with the access card. But is there a more real basic internal control of a process when an employee leaves the Department, whoever their superior is, that I would think has a checklist of what you go through, you turn in your key, you turn in your badge. And I make sure that your access from a technology standpoint is cut off. I would assume that there is that type of more basic human-oriented internal control that is apparently not being followed. The fact that you have former employees or contractors staying on for some period of time.

Mr. WEST. Yes, sir. With respect to employees, the components all have programs for that that are different. The Coast Guard is the fifth service, and they have a very DOD-centric approach to that.

I believe that the biggest issue centers around contractors. And as I said, contractors come and go with the contract, and in fact, some time the same contract, different people are swapped out for various, all kinds of reasons, business reasons. And it is keeping track of contractors, because they have access in some cases to our systems as well. That is probably the biggest challenge. And frankly, the best I can say, that is a challenge. Like I said, we need to get to the point where we have strong token-based authentication so that the system can do, in an automated way, can do the removal as opposed to having to rely on a contracting officer to tell the system administrator that this person has left. That has just been a challenge.

And as I said, what we have put in place to mitigate that are these periodic reviews. And at the Department level, we have asked that we do that in as short a cycle as possible. It is labor-intensive. There is a drain for that. Generally it is 90 days. That is kind of where we are with that. HSPD 12 gives us a lot of promise, and we are, like I said, we are really going after that.

Mr. PLATTS. And just given the information that you, as a Department, hold within your data bases, a lot of very sensitive information, all the more important that access be a priority, and of those five major areas of weaknesses, that that continue to be focused on. Technology ultimately could be a wonderful solution. But in the meantime, whatever we need to do to make sure from a manual standpoint. Because we don't want to have it where it is always more of that Herculean effort to comply. We want to get to it. But in the meantime, because of the sensitivity of the information, whatever it takes is what needs to be done.

Mr. WEST. Yes, sir.

Mr. PLATTS. The financial system functionality issues, Mr. McCoy, you identify in your testimony about the example with ICE and the issue of duplicate payments. As a subcommittee, we focused on improper payments in a significant way. And the numbers are staggering, the official number, $125 billion in the most recent year available of improper payments. All sorts, including duplicate payments. And you reference in your testimony duplicate payments by ICE in fiscal years 2009, 2010, and 2011.

Is there a ball park of what type, from a financial dollar standpoint that we are talking about there, the significance of those types of duplicate payments?

Mr. MCCOY. Yes, sir, I have the number for 2011, but I do not have the numbers, I can get those, for 2009 and 2010. For 2011, the duplicate payments occurred on January 28th, and it was approximately $1.5 million.

Mr. PLATTS. And what type of contract, or do you have those details with you?

Mr. MCCOY. I believe it was a vendor payment and it was scheduled multiple times. So multiple payments went to that vendor.

Mr. PLATTS. All for $1.5 million?

Mr. MCCOY. All for $1.5 million went to one vendor. ICE is in the process, if they have not already recouped it all, will recoup it either through offsets or the money has been returned.

Mr. PLATTS. So $1.5 million was the amount of the payment and it was made multiple times?

Mr. MCCOY. The $1.5 million was the total amount. It was multiple payments.

Mr. PLATTS. Okay. So it might have been a $500,000 that was actually owed, paid three times, something of that nature?

Mr. MCCOY. I believe it is more along the lines of $80,000 paid multiple times or something different. It is a smaller number, it was paid multiple times.

Mr. PLATTS. The dollar amount being smaller may actually make me even more concerned. Because if it was $750,000 and we duplicate paid it once, that would be troubling and a risk to taxpayers. But if it was $100,000 and we did it 15 times, then that tells we have a real breakdown in the internal controls.

Mr. MCCOY. It is part of the functionality with that system. They have put a patch in to prevent that from happening again. It also has something to do with training, with certified officials.

Mr. PLATTS. Ms. Sherry, is that one that you are familiar with, that case?

Ms. SHERRY. Yes, absolutely. In fact, since 2009, I believe ICE has had three separate duplicate payments that have been both a mixture of manual errors, as Mr. McCoy had indicated, as well as system issues. I think that the number is about $15 million in total over the last 3 years. And that is in context of about $26 billion that they would have paid during that time. So relatively small percentage-wise, clearly something that is very concerning to us.

As we identify these issues, again, the goal in any of this, any payment management controls, is to prevent that type of stuff. So clearly, relying on detective controls is not a best practice. That is not something that we want to do. But when ICE had identified these duplicate payments, and typically what would happen is on a particular schedule, when they go to make the payment, it has a myriad of individuals on that particular schedule. So what happens is when you pay it once, and then if you are allowed to pay it again, I believe either through a systems bug or a patch that didn't quite work, or the system allows certifiers to maybe, schedulers to certify the same schedule twice. Things of that nature, what ends up happening is you end up paying all those individuals again, and that is what is indicated then.

We worked very closely with ICE, clearly, for the last 3 years, to really identify the reason for the duplicate payment. Because what we really wanted to find out, number one, we wanted to prevent it from happening again. They detected it, how do we prevent if from happening again. They have successfully put in fixes for each of those. I believe in November they will be putting in a fix to the Oracle data server in order to be able to address any of the interface issues which I think contributed to this last duplicate payment. So we aggressively go after the fix of these.

ICE also is very much making sure that they are forward looking. So in other words, if there is a particular schedule that is paid that is out of the ordinary, maybe it is expedited or it is not paid on their normal schedule, they are hypersensitive in really reviewing those, just to make sure that nothing abnormal actually happened.

Mr. PLATTS. That focus, I appreciate the point that $15 million out of $26 billion percentage, but $15 million of American taxpayers' hard-earned dollars is still $15 million.

Ms. SHERRY. I completely agree, sir, and we did recoup all the payments. So we aggressively go after them to make sure that we recoup them. And the Department has other programs in place, such as the improper payments. And doing recovery auditing, really using those forensics to go out there to determine whether or not there are duplicate payments out there, what we find happily through those forensic type looks is that duplicate payments is not really rampant throughout the Department. So it is not just at ICE.

But what we want to do is again, we have to prevent them as opposed to just detecting them after the fact. Again, protecting the American taxpayer dollar is what we need to do. So one of the things that we will be doing this year, through the A123 process, is really that end to end review of our payment processes throughout the Department. And really training, we need to be able to make sure that if an improper payment is occurring because of a particular condition, we make sure that we don't just fix it at that one component, but instead, that all the components are addressing those particular issues.

Mr. PLATTS. And I commend that approach. I think that has been a hallmark of your leadership at the Department. It really isn't just a one-time short fix, but a permanent solution. And getting to root causes that we are putting in place and what we have learned at ICE, let's make sure at FEMA or Coast Guard or wherever that we are not having to repeat the error to reinvent the wheel. Let's be comprehensive. I think that ultimately gets to where I know where you are trying to get, ultimately, to that clean audit in the long term.

I am going to put in one more question and then we are going to have to wrap it up. That goes to the issue of the financial systems modernization. And back in March, with the cancellation of the transformation and systems consolidation approach, more of an enterprise-wide and then just last month, the announcement by the Under Secretary of the decentralized approach. I guess if I could have kind of a summary of where we stand on that change and that new approach, decentralized.

And Mr. McCoy referenced in his testimony that in making the change to a decentralized approach that there would be prioritized system modernization for components with the most critical need. What is going to be the approach of that prioritization? Is it going to be from a sensitivity of the information? Dollar amounts that maybe are at risk? The history of that entity, ICE versus FEMA versus, if you look at FEMA with the number of repeat deficiencies, how are you going to prioritize in making this new approach decentralized?

Ms. SHERRY. Yes, sir. As you correctly point out, in March we had the sustainment of the protest. What we have done, what GAO had asked us to do was to really take a look at whether or not our requirements had changed. So what we did is we took that to heart and we took a look. We realized because of the changes that have really occurred since we originally went out with the solicitation, in particular in information technology, that in fact we were able to do this differently.

So rather than bringing one system, one instance of a system within our data warehouse, within our data centers, that there was just a change in the security posture in general and change in IT as it relates to cloud computing. In addition to the fiscal pressures and the realization that you can't have 10-year implementation, where it takes you 10 years, $10 billion later, to be able to get to initial operating capability.

So it has been something that our leadership has been very much focusing on, not just for financial systems, but for all of our IT projects, to be able to say, you need to be able to get to operating capability quicker. What they are really looking for, challenging us to be able to develop projects in smaller ways such that we can develop that capability quicker. So that is really what the intention is.

So all of that together, really, the Department looked back and said, yes, there is a different way for us to be able to do this. We haven't exactly said that FEMA will go here, Coast Guard will go here, ICE will go here. Instead, what we are doing, we are working with each of those components and having them do an analysis of alternatives. They are doing their market research, they are looking what is out there, they are defining what their requirements are with the Department. What we are doing is we are setting forward kind of the standards. In the event that you were to be able to go out to a shared service provider or a commercial provider out in the cloud some place, here are the basic minimum internal controls you absolutely must have, the things that you must do.

So we are working with the components in setting those particular standards. Also working with them on common data structures, such that we won't be overly proscriptive to be able to limit their ability to be able to go out there and find the right provider. But really the basics, such that in one of our components, in their accounting line, they don't have a budget year. So they don't have a budget year, which again, that causes so many problems, so many audit problems as well as workarounds and reconciliations. For my purposes, it causes me great concern from a funds control standpoint.

So the basic chocolate and vanilla type standards that you must have out there, you have to have a budget year in your accounting line. So we worked very closely with them on that.

We want to focus on those systems that are most critical, and they are critical for many fronts. What we are not doing is waiting until we modernize the systems to address those security issues. So the access controls, those key controls for security, we are working with them on that. Instead what we will do is look at those components that have, that basically are almost in extremis with their systems. FEMA in particular will be one that we had focused on initially for TASC that we were going to move forward with. We are moving forward very aggressively with FEMA right now as well to be able to replace their system.

Working with the Coast Guard, I believe we will not be able to get a full scope audit done very effectively and efficiently without the Coast Guard doing something to their accounting system. And as we have talked about this morning, ICE, with their system issues as well as lack of integration, really is something that we need to address.

Mr. PLATTS. The approach, and with the Department setting minimum standards, is there a relationship as you are working to do that between you and the CIO but also the IG in a prospective, proactive way, versus after the fact that you go this route and then IG and then internal and outside audits says, no, that is not going to work? How does that relationship proceed?

Ms. SHERRY. That is a great question, because it is something, one of the lessons learned as we have done TASC, which really is that we need to involve all of the key stakeholders, including the components, very early. But in particular, we need to involve the OIG as well as the GAO in really taking a look at them.

So as part of, with the Department being on the high risk as it relates to many of these issues, financial management being one of them, we work very closely with the GAO. In fact, we briefed them just a few weeks ago on what this approach was. We took some recommendations from them. We also met with the IG just recently and gave them actually our data standards, here is the standardization that we are trying to do and we have invited both the GAO as well as the IG to provide comments to us on that.

We will continue to share our documentation with them as we develop it. We are working on a concept of operations currently at the Department level, and then we work very closely with the components. So right now, we are working closely with FEMA as they develop their documentation and invite the IG in as well as the GAO to be able to help us with best practices, so that we can again look at that, not looking back and reading it in an audit report, but really trying to prevent these types of problems.

Mr. PLATTS. And again, that approach I think is very commendable and ultimately what is going to help you succeed. As Mr. Towns well stated earlier, our role is trying to partner with you as you make that progress and go forward. And as the Deputy Secretary said, if you need help in banging some heads, we are glad to bring in any component entity before us to talk about what they are doing, if they are not in line with what you are trying to do as a Department. And again, not to play gotcha, but just to make sure they understand the importance that we all need to work together to get this done.

And your reference to the approach I think is very important that, I think for the American people, it is hard for them to understand that when the Federal Government says, we have identified this problem and it is going to be 2 or 3 or 4 or 5 or 10 years before we think we will fix is, in the private sector, the business would be closed and out of business. Because of the role Government plays, it will still be one and still just kind of doing its best while it is trying to fix the problem. The American people, I think understand, they approach it, what can we do and get it done, the sooner the better. And especially here, protecting tax dollars and sensitive information, so all the more important.

With that, we are going to need to wrap up. I want to thank each of you again for your testimony, your knowledge that you share as we try to fulfill our responsibility as an oversight subcommittee and look forward to continuing to work with you. The 2011 audit will be coming out and hopefully set a stage here seeing some good news in just a few weeks.

We will keep the record open for 7 days, if there is any additional information. I think I am good n the 2009 and 2010 with the numbers you shared. For 2011, I don't need that additional information.

Also I do want to thank Mr. West and Mr. McCoy, in addition to your work in your current positions, your prior service in uniform. I am very grateful. I love what I do, but what I do pales in comparison to you as a former Navy aviator and U.S. Marine. I should say former, not former, you are always a Marine, just no longer actively serving as a Marine. I am grateful for both of your service and collectively all three in your civilian positions, what you are doing on behalf of our country and our citizens.

So with that, this hearing stands adjourned.

[Whereupon, at 11:22 a.m., the subcommittee was adjourned.]

[The prepared statement of Hon. Gerald E. Connolly follows:]

Statement of Congressman Gerald E. Connolly
Subcommittee on Government Organization and Efficiency
October 27th, 2011

Thank you, Chairman Platts for the latest in a long line of substantive hearings. We are fortunate to have the opportunity to discuss cybersecurity with three DHS witnesses, including one who came before this Subcommittee during the last Congressional session.

As we consider cybersecurity reforms such as the Administration's cybersecurity proposal and the Liebermann/Carper/Collins Senate bill, I believe we first must understand whether we are asking the right questions and using the right metrics to assess progress. As we learned during the last session, in the past agencies would comply with FISMA requirements, by sending their employees to security trainings, for example, but had no way of assessing the functionality of their information security systems. For example, the GAO reports a "tripling" of cyber activity targeting the U.S. since 2009, but does not help us understand what percentage of those attacks were successful or what the consequences were. Fortunately, under the leadership of this Administration and DHS it appears that we are making significant progress moving toward performance rather than compliance-based assessments of information security, including but not limited to FISMA requirements. For example, DHS has been working with its own components as well as other agencies to implement continuous monitoring of system functionality and monitoring of intrusions through the use of the "Einstein" system. Some agencies, such as the Department of Justice, have retrofitted nearly all of their entire information technology systems to use continuous monitoring. This represents real progress, and I hope we can learn from today's hearing how we can help DHS continue to implement continuous monitoring within its components and at other agencies.

While continuous monitoring is a superior metric to the old, largely meaningless check-the-box compliance activity, such as training attendance, it is still a proxy for performance rather than a performance metric. To understand if agencies' systems are more or less secure today than in the past, we must know the following information: 1) Number of attempted cyber attacks; 2) Number and percentage of successful cyber attacks; 3) Of the successful cyber attacks, the number and percentage that exposed sensitive federal information or information of American citizens. We know that the number of cyber attacks will continue to grow; this fact alone does not mean we are less secure. Even the fact that the number of successful cyberattacks is growing does not necessarily mean that we are less secure if the number of attacks that exposed sensitive information actually went down. One of the flaws of our monitoring of cyber attacks is that we fail to disaggregate between the isolated incident which exposes one federal employee's private email password and the cyber attack which steals all individuals' personal information as housed in the Social Security or Veterans Affairs Administration. DHS is developing its third iteration of the Einstein program, which finally will begin to provide details about the severity of cyber attacks. Without this level of granularity we will remain unable to assess which threats are most pressing. At this hearing I hope to learn more about how DHS can assess agencies' efficacy at interrupting cyber attacks and about other steps it will taking to analyze the nature of successful cyber attacks that have occurred.

In November the National Protection and Programs Directorate will be receiving agency information about the number and nature of cyber attacks. When DHS has compiled and analyzed this information I would appreciate the opportunity to learn more about it, either through another hearing of this Subcommittee or a staff briefing. This information from the National Protection and Programs Directorate will complement the information we have today on continuous monitoring and provide a far more accurate picture of our cyber security and which agencies and DHS components are most at risk. With critical information from Social Security numbers to national security databases at risk, this clearly is an important subject for our Subcommittee to address. Thank you again, Chairman Platts, for organizing this important hearing.