Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the United States Coast Guard Component of the FY 2009 DHS Integrated Audit

OIG-10-77

April 2010

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

April 9, 2010

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the United States Coast Guard component of the FY 2009 DHS Integrated audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were not required to be reported in the *Independent Auditors' Report,* dated November 13, 2009 and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of Coast Guard's FY 2009 financial statements as part of the DHS Integrated Audit and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated January 21, 2010, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General for
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036

January 21, 2010

Inspector General
U.S. Department of Homeland Security
Chief Information Officer
U.S. Coast Guard
Chief Financial Officer
U.S. Coast Guard

Gentlemen:

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2009, and the related statement of custodial activity for the year then ended (referred to herein as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting (ICOFR) of the balance sheet as of September 30, 2009, and statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources, for the year ended September 30, 2009 (referred to herein as "other fiscal year [FY] 2009 financial statements"), or to examine ICOFR over the other FY 2009 financial statements. Because of matters discussed in our *Independent Auditors' Report*, dated November 13, 2009, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements. In addition, we were unable to perform procedures necessary to form an opinion on DHS' ICOFR of the FY 2009 balance sheet and statement of custodial activity.

In connection with our FY 2009 engagement, we examined the United States Coast Guard's (Coast Guard) internal control over financial reporting by obtaining an understanding of Coast Guard's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls. As noted above, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the effectiveness of ICOFR. Further, other matters involving ICOFR may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheet as of September 30, 2009, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other FY 2009 financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

During our audit engagement, we noted certain matters in the areas of configuration management with respect to Coast Guard's financial systems information technology (IT) general controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. These matters are described in the IT General Control and Financial System Functionality Findings by Audit Area section of this letter.

The material weakness described above is presented in our Independent Auditors' Report dated November 13, 2009. This letter represents the separate restricted distribution report mentioned in that report.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also described in the IT General Control and Financial System Functionality Findings by Audit Area section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR). We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. In addition, we have provided the following: a description of key Coast Guard financial systems and IT infrastructure within the scope of the FY 2009 DHS financial statement audit engagement in Appendix A; a description of each internal control deficiency in Appendix B; the current status of the prior year Notice of Finding and Recommendations (NFR) in Appendix C; and Coast Guard management's written response in Appendix D. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Acting Chief Financial Officer dated December 9, 2009.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General, the Office of Management and Budget, U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

During our engagement to perform an integrated audit of Department of Homeland Security (DHS), we evaluated the effectiveness of the IT General Controls of DHS' financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit as it relates to IT general control assessment at Coast Guard. The scope of the Coast Guard IT general controls assessment is described in Appendix A.

FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial statement audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following six control functions to be essential to the effective operation of the general IT controls environment.

- *Security Management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit, we also performed technical security testing for key network and system devices. The technical security testing was performed from within a select Coast Guard facility, and focused on test, development, and production devices that directly support Coast Guard's financial processing and key general support systems.

Application controls were not tested for the year ending September 30, 2009 due to the nature of prior-year audit findings.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2009, Coast Guard took corrective action to address nearly half of the prior year IT control weaknesses. For example, Coast Guard made improvements by updating the Coast Guard Finance Center (FINCEN) Continuity of Operations (COOP) Plan, strengthening account management controls over the Shore Asset Management (SAM) system, and completed the Certification and Accreditation (C&A) package for their core financial systems. However, during FY 2009, we continued to identify IT general control weaknesses at Coast Guard. The most significant weaknesses from a financial statement audit perspective are related to the controls over authorization, development, implementation, and tracking of IT scripts at FINCEN. These IT control deficiencies limited Coast Guard's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted the internal controls over Coast Guard financial reporting and its operation and we consider them to contribute to a material weakness at the Department level under standards established by the American Institute of Certified Public Accountants (AICPA). In addition, based upon the results of our test work we noted that the Coast Guard did not fully comply with the Departments requirements of Federal Financial Management Improvement Act (FFMIA).

Of the 20 findings identified during our FY 2009 testing, 11 were repeat findings, either partially or in whole from the prior year, and 9 were new IT findings. These findings represent deficiencies in three of the five FISCAM key control areas. The FISCAM areas impacted included Security Management, Access Control, and Configuration Management. We also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems are not compliant with FFMIA 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 (NIST) guidance. Specifically, the findings stem from 1) inadequately designed and operating IT script change control policies and procedures, 2) unverified access controls through the lack of user access privilege re-certifications, 3) entity-wide security program issues involving civilian and contractor background investigation weaknesses, 4) inadequately designed and operating audit log review policies and procedures, 5) physical security and security awareness, and 6) role-based training for individuals with elevated responsibilities. These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and Coast Guard financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS consolidated financial statements.

While the recommendations made by us should be considered by Coast Guard, it is the ultimate responsibility of Coast Guard management to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

IT GENERAL CONTROLS AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS BY AUDIT AREA

Findings Contributing to a Material Weakness in IT at the Department Level

Conditions: In FY 2009, the following IT general control and financial system functionality deficiencies were identified at the Coast Guard and contribute to a DHS-level significant deficiency that is considered a material weakness in IT general and application controls. Our findings are divided into two groupings: 1) financial systems controls and 2) IT system functionality.

Related to IT Financial Systems Controls

Configuration Management – we noted:

Coast Guard's core financial system configuration management process controls are not operating effectively, and continue to present risks to DHS financial data confidentiality, integrity, and availability. Financial data in the general ledger may be compromised by automated and manual changes that are not adequately controlled. For example, the Coast Guard uses an IT scripting process to make updates to its core general ledger software as necessary to process financial data. However, the Coast Guard has not fully developed testing standards to guide staff in the development and functional testing of IT scripts, documented policies and procedures over testing plans that must be performed, and improve processes to ensure that all necessary approvals are obtained prior to implementation. Specifically, we noted the following weaknesses associated with the IT script control process:

- Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests.
- FINCEN analysts may run scripts without seeking approval from the Functional Supervisors for approved recurring scripts.
- Testing requirements are inconsistently followed for the testing of the recurring approval scripts and retaining evidence of testing.
- Reconciliation between the scripts run and the changes made to the database tables is not being performed to monitor the script activities using this report as it is too difficult to accurately and effectively reconcile the scripts to the audit log table changes.
- The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts.
- Variations in the way the PRP Approval Forms are populated and completed exist for fields such as financial impact, test strategy and baseline determinations.
- Proper approval is not consistently obtained and documented prior to the running of each script.

Related to Financial System Functionality:

We noted that financial system functionality limitations are contributing to control deficiencies and inhibiting progress on corrective actions for Coast Guard. These functionality limitations are preventing the Coast Guard from improving the efficiency and reliability of its financial reporting processes. Some of the financial system limitations lead to extensive manual and redundant procedures to process transactions, verify accuracy of data, and to prepare financial statements. Systemic conditions related to financial system functionality include:

1. As noted above, Coast Guard's core financial system configuration management process is not operating effectively due to inadequate controls over IT scripts. The IT script process was instituted as a solution primarily to compensate for system functionality and data quality issues;
2. Annual financial system account recertifications are not being performed due to limitations in the systems;
3. Financial system audit logs are not readily generated and reviewed as some of the financial systems are lacking this capability;
4. Aspects of DHS-required system password requirements are not implemented because some financial systems cannot support the policy;
5. Production versions of operational financial systems are outdated, no longer supported by the vendor, and do not provide the necessary core functional capabilities (e.g., general ledger capabilities);
6. Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls that would improve accuracy, reliability and facilitate efficient processing of certain financial data such as:
    - Tracking of costs to support weighted average pricing for operating materials and supplies;
    - Maintaining data needed to support the calculation of accounting payable and provide detailed listings of accounts payable, which may reduce the resources spent by Coast Guard personnel in manually preparing the accounts payable accrual;
    - Ensuring proper segregation of duties such as automating the procurement process to ensure that only individuals who have proper contract authority can approve transactions;
    - Tracking detail transactions associated with intragovernmental business and eliminating the need for default codes such as Trading Partner Identification Number that cannot be easily researched; and
    - Ensuring that undelivered obligations are properly accounted for upon receipt of goods or services.

Recommendations: Coast Guard should continue to make improvements to implement and better document an integrated script configuration management process that includes enforced responsibilities of all participants in the process, and the continued development of documentation requirements. In addition, Coast Guard should address the IT system aspects associated with the financial system

functionality issues listed in No. 1 through No. 6 above, or develop compensating/mitigating controls in order to eliminate or reduce the associated risk.

Specifically, for the IT script control process, we recommend that the Coast Guard should:

- Continue to design, document, implement, and enforce the effectiveness of internal controls associated with the active (current and future) scripts;

With respect to procedures already in place, Coast Guard should:

- Update / develop procedures and implement technical controls in the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) databases to ensure that the appropriate monitoring and review of script activities is performed and documented;

- Continue to update script policies and procedures to include clear requirements and more detailed guidance over requesting recurring scripts, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. Additionally, ensure that the policies and procedures include detailed guidance over the requirements for the testing of scripts and associated test plans to ensure that the appropriate financial impact of the script is evaluated, reviewed by the appropriate personnel, tested in an appropriate test environment prior to being put into production, and documented prior to execution; and,

- Further develop and implement policies and procedures governing the script change control process to ensure that all script records are accurate and complete.

Other Findings in IT General Controls

Although not contributing to a department-level material weakness, we also noted the following other matters related to financial system IT control deficiencies during the FY09 DHS IT Audit:

1. Access Controls – we noted:
   - Procedures surrounding the use of monitoring reports over contracted personnel data have not been formally documented.
   - Procedures over the process of finalizing and implementing entity-wide processes for account terminations and related notifications are still in draft and have not been implemented or communicated.
   - Audit log reviews for key financial systems are not conducted at a sufficient frequency.
   - Access review procedures for key financial applications do not include the review of all user accounts to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary.
2. Security Management – we noted:

- Background investigations for all civilian employees have not been completed and Coast Guard's civilian position sensitivity designation process is not in compliance with DHS guidance.
- Coast Guard procedures do not include specific guidance for the program managers on how to set the correct and consistent risk levels and position sensitivity designations for contract employees.
- During our after-hours physical security and social engineering testing we identified exceptions in the protection of sensitive user account information. The table below details the exceptions identified at the various locations tested.

After-Hours Physical Security Testing

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a Coast Guard employee's / contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various Coast Guard locations that process and / or maintain financial data.

Security Weaknesses Observed During After Hours Physical Security Testing					
	Coast Guard Locations Tested				
Exceptions Noted	**Coast Guard HQ – Jemal (CG-6)**	**Coast Guard HQ – Jemal (DCMS-8x)**	**Coast Guard HQ – Transpoint (CG-8)**	**Coast Guard Finance Center (FINCEN)**	**Total Exceptions by Type**
Passwords	2	2	1	6	**11**
For Official Use Only (FOUO) Documents					
Keys/Badges					
Personally Identifiable Information (PII)					
Server Names/IP Addresses					
Unsecured Laptops		2			**2**
Unsecured External Drives					
Credit Cards		2			**2**
Common Access Cards (CAC)	1			3	**4**
Common Access Card PIN					
Classified Documents					
Other –US Government official passport					
Total Exceptions by Location	**3**	**6**	**1**	**9**	**19**
Source: Coast Guard management, OIG and KPMG direct observation and inspection of work areas.					

Note that approximately 20-25 desks / offices were examined for each one of the columns in the above table.

Social Engineering Testing

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to deception for the purpose of information gathering, or gaining computer system access, as shown in the following table.

Location	Total Called	Total Answered	Number of people who provided a password
Coast Guard HQ	20	8	0 Passwords
Coast Guard FINCEN*	18	6	1 Password

* Although the password was provided, shortly after the violation, the user became aware of his / her infraction, and changed his / her password. Additionally, the user then notified the FINCEN Information Assurance Support (IAS) group of the social engineering activity. Our full sample of 30 personnel could not be completed due to the intervention from the Coast Guard FINCEN Information Assurance Support (IAS) group.

Recommendations: We recommend that the Coast Guard Chief Information Officer and Chief Financial Officer, in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer**,** make the following improvements to Coast Guard's financial management systems and associated information technology security program.

For access controls:

- Develop procedures for the periodic review of the manual audit logs. In addition, ensure audit log files are configured, retained, and archived in compliance with DHS policy;
- Develop and finalize specific procedures over the review of the CVS reports and reconciliation of contractor accounts to ensure that contractor data within the system remains current and accurate;
- Develop and document an enterprise-wide process that will notify all impacted system owners of terminated, transferred, or retired contractor, military, and civilian personnel;
- Review audit logs containing unusual activity and unexplained access attempts on at least a monthly basis;
- Modify procedures to require an annual review of one hundred percent (100%) of user accounts for the key financial systems and their associated privileges that are greater than read-only to ensure access is still required.

For security management:

- Update the policies and procedures currently in place to include clear guidance for Program Managers and Contracting Officers to assign contractor risk level(s) and position sensitivity designation requirements in order to verify that all contracts issued by the Coast Guard include the appropriate investigation level requirements;

- Perform initial background investigations and re-investigations for civilian employees in accordance with DHS directives;
- Review its policies and procedures regarding Protection of Sensitive Information and update where required in order to address DHS and other Federal requirements, with emphasis being placed on the potential impacts of not consistently and adequately protecting this sensitive information;
- Review, and update as required, its security awareness / training content to address the updated Protection of Sensitive Information policies and procedures; and
- Validate the effectiveness of the updated policies and procedures and associated training through mechanisms such as scheduled and unscheduled desk / floor reviews, awareness training testing, etc. and take appropriate corrective action to address any issues identified during this validation.

Cause/Effect: The IT system development activities did not incorporate adequate security controls during the initial implementation more than six years ago. The current IT configurations of many Coast Guard financial systems cannot be easily reconfigured to meet new DHS security requirements. The existence of these IT weaknesses leads to added dependency on the other mitigating manual controls to be operating effectively at all times. Because mitigating controls often require more human involvement, there is an increased risk that human error could materially affect the financial statements. In addition, the Coast Guard's core financial systems are not FFMIA compliant with the Federal Government's Financial System Integration Office (FSIO) requirements.

Reasonable assurance should be provided that financial system user access levels are limited and monitored for appropriateness and that all user accounts belong to current employees. The weaknesses identified within Coast Guard's access controls increase the risk that employees and contractors may have access to a system that is outside the realm of their job responsibilities or that a separated individual, or another person with knowledge of an active account of a terminated employee, could use the account to alter the data contained within the application or database. This may also increase the risk that the confidentiality, integrity, and availability of system controls and the financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

Furthermore, the lack of documented security configuration management controls may result in security responsibilities communicated to system developers improperly as well as the improper implementation and monitoring of system changes. This also increases the risk of unsubstantiated changes as well as changes that may introduce errors or data integrity issues that are not easily traceable back to the changes. In addition, it increases the risk of undocumented and unauthorized changes to critical or sensitive information and systems. This may reduce the reliability of information produced by these systems.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition, OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial

management systems. The purpose of FFMIA is: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

APPLICATION CONTROLS

Application controls were not tested for the year ending September 30, 2009 due to the nature of the prior-year audit findings.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the Coast Guard CIO. Generally, the Coast Guard agreed with all of our findings and recommendations. The Coast Guard has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments in Appendix D.

OIG Response

We agree with the steps that Coast Guard management is taking to satisfy these recommendations.

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Appendix A

Description of Key Coast Guard Financial Systems and IT Infrastructure within the Scope of the FY 2009 DHS Financial Statement Audit Engagement

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Below is a description of significant Coast Guard financial management systems and supporting Information Technology (IT) infrastructure included in the scope of the engagement to perform the financial statement audit.

Locations of Audit: Coast Guard Headquarters in Washington, DC; the Coast Guard Finance Center (FINCEN) in Chesapeake, Virginia; the Operations Supply Center (OSC) in Martinsburg, West Virginia; and the Pay and Personnel Center (PPC) in Topeka, Kansas.

Key Systems Subject to Audit:

- *Core Accounting System (CAS)*: Core accounting system that is the principal general ledger for recording financial transactions for the Coast Guard. CAS is hosted at FINCEN, the Coast Guard's primary data center. It is a customized version of Oracle Financials.
- *Financial Procurement Desktop (FPD)*: Used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is hosted at FINCEN.
- *Workflow Imaging Network System (WINS):* Document image processing system, which is integrated with an Oracle Developer/2000 relational database. WINS allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. WINS utilizes MarkView software to scan documents and to view the images of scanned documents and to render images of electronic data received. This system is hosted at FINCEN.
- *Checkfree*: A commercial product used to reconcile payment information retrieved from the United States Department of the Treasury. It reconciles transaction items that Treasury has processed to transaction items Coast Guard has sent to Treasury. This system is hosted at FINCEN.
- *Joint Uniformed Military Pay System (JUMPS):* Mainframe application, hosted at PSC, used for paying Coast Guard active and reserve personnel payroll.
- *Shore Asset Management (SAM):* Is hosted at the Coast Guard's Operation System Center (OSC), in Martinsburg, WV. SAM provides core information about the Coast Guard shore facility assets and facility engineering. The application tracks activities and assist in the management of the Civil Engineering (CE) Program and the Facility Engineering (FE) Program.

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Appendix B

FY 2009 Notices of IT Findings and Recommendations at Coast Guard

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Notice of Findings and Recommendations – Definition of Severity Ratings:**

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditors Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist the Coast Guard in the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Department of Homeland Security
United States Coast Guard
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-09-10	The current Coast Guard procedures do not include specific guidance for the Program Managers on how to set the correct and consistent risk levels and position sensitivity designations that correspond to CLINs and labor categories. Therefore, there is insufficient guidance over the level of clearance required which may result in inconsistent risk levels and position sensitivity designations.	Update the policies and procedures currently in place to include clear guidance for Program Managers and Contracting Officers to assign contractor risk level(s) and position sensitivity designation requirements in order to verify that all contracts issued by the Coast Guard include the appropriate investigation level requirements.		X	2
CG-IT-09-14	The Role-Based Industry Standards for Coast Guard Information Assurance (IA) Professionals Commandant Instruction remains in draft form.	• Update the Role-Based Industry Standards for Coast Guard IA Professionals Commandant Instruction to include the procedures by which Direct Access will be used to monitor and verify that training has been completed by all Coast Guard Government personnel with significant information security responsibilities. In addition, the instruction should include the procedures by which Coast Guard contractor compliance will be monitored and verified. • Finalize, communicate, and implement the Role-Based Industry Standards for Coast Guard IA Professionals Commandant Instruction. • Continue with efforts to implement Direct Access as the centralized method for		X	1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		monitoring and verifying Coast Guard personnel compliance with the specialized role-based training requirements.			
CG-IT-09-23	Although the Operation Systems Center (OSC) has begun reviewing Shore Asset Management (SAM) audit logs on a regular basis, detailed policies and procedures have not been created over the process and sufficient evidence is not maintained.	Develop and document comprehensive policies and procedures over the SAM audit log review process. These policies and procedures should establish the independence of the reviewer, the audit logs under review, and the supporting documentation requirements including results and remediation efforts.		X	1
CG-IT-09-25	Procedures do not include an annual review of all Workflow Imaging Network System (WINS) user accounts, as required by the DHS 4300A Sensitive Systems Handbook and required by the DHS Chief Information Officer.	Modify procedures to require an annual review of one hundred percent (100%) of WINS user accounts and their associated privileges that are greater than read-only. The updated procedures should include steps to verify that: a) all terminated individuals no longer have active accounts, b) inactive accounts are locked, and c) privileges associated with each individual/role are still authorized and necessary for that job function.		X	1
CG-IT-09-31	Weaknesses continued to exist over the script configuration management process. Specifically, weaknesses were noted in the areas of approvals, testing, monitoring, maintaining documentation, and audit logging. • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests. • Coast Guard Finance Center (FINCEN) analysts may run scripts without seeking approval from the Functional Supervisors for approved recurring	Continue making improvements to implement and better document an integrated script configuration management process that includes enforced responsibilities of all participants in the process, and the continued development of documentation requirements. We recommend that the Coast Guard should: • Continue to design, document, implement, and enforce the effectiveness of internal controls associated with the active (current and future)		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	scripts. • Testing requirements are inconsistently followed for the testing of the Recurring Approval scripts and retaining evidence of testing. • No reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities using this report as it is too difficult to accurately and effectively reconcile the scripts to the audit log table changes. • The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts. • Variations in the way the Production Review Process (PRP) Approval Forms are populated and completed exist for fields such as financial impact, test strategy and baseline determinations. • Proper approval is not consistently obtained and documented prior to the running of each script.	scripts. With respect to procedures already in place, Coast Guard should: • Update / Develop procedures and implement technical controls in the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) databases to ensure that the appropriate monitoring and review of script activities is performed and documented. • Continue to update script policies and procedures to include clear requirements and more detailed guidance over requesting recurring scripts, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. Additionally, ensure that the policies and procedures include detailed guidance over the requirements for the testing of scripts and associated test plans to ensure that the appropriate financial impact of the script is evaluated, reviewed by the appropriate personnel, tested in an appropriate test environment prior to being put into production, and documented prior to execution. • Further develop and implement policies and			

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		procedures governing the script change control process to ensure that all script records within the Change Management Script System are accurate and complete.			
CG-IT-09-32	Coast Guard has not created specific procedures to address how monthly contractor reports will be analyzed and does not maintain supporting evidence associated with this review.	Develop and finalize specific procedures over the review of the Contractor Verification System reports and reconciliation of contractor accounts to ensure that contractor data within the system remains current and accurate.		X	2
CG-IT-09-33	During our FY 2009 follow-up test work, we determined that Coast Guard is currently finalizing the business process that will be used to remediate the conditions identified in the prior year NFR. Once a business process has been finalized, a technical implementation will occur. Currently, Coast Guard HQ plans to use the Direct Access Human Resources (HR) system to notify system owners of HR status changes for all individuals within the system. This would include terminations. Direct Access is currently undergoing a phased upgrade from PeopleSoft 8.0 to PeopleSoft 9.0. Coast Guard informed us that while the functionality required is not included in the 8.0 version, it should be included in the 9.0 version. At this time, where this functionality fits into that upgrade schedule, has not yet been determined. In addition, Coast Guard has created a service request to track its remediation efforts and has identified the termination process currently conducted at Coast Guard's Personnel and Pay Center (PPC) as a potential solution. At PPC, a report is run within Direct Access whenever an	• Develop and document an enterprise-wide process that will notify all impacted system owners of terminated, transferred, or retired contractor, military, and civilian personnel; and • Develop and finalize entity management policies and procedures for verifying that terminated user accounts have been successfully removed.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	individual separates, retires, or transfers which automatically removes system permissions. However, this process currently excludes contractors and civilians whose information is not currently in Direct Access.				
CG-IT-09-34	Not all WINS change requests were appropriately reviewed and approved by management prior to development and/or prior to implementation. In addition, 1 of the 25 WINS changes selected was identified as having a financial impact consideration to the Coast Guard Financial Statements and, as such, the appropriate Financial Representative approval was not obtained prior to implementation. We further noted that the criterion set forth in the Coast Guard Finance Center Financial Statement Impact Consideration Memo does not provide sufficient detail to assist in making a determination regarding the financial impact of a proposed change.	• Consistently enforce the newly implemented PRP process to ensure that all change requests are properly reviewed and approved prior to development and again prior to implementation. • Periodically verify FINCEN compliance with its PRP and related approval and CM processes. • Formally document detailed decision criteria to be used when determining if a change has a financial impact.		X	1
CG-IT-09-40	During our FY 2009 follow up, we determined that Coast Guard actively monitors all civilians to verify whether they have a valid background investigation on record. We received documentation from Coast Guard that identified 94 individuals with an outstanding investigation. This number has been reduced significantly from the approximately 350 individuals identified in FY 2008. Coast Guard continues vetting individuals based on the Office of Personnel Management (OPM) requirements	• Perform the initial background investigations for civilian employees in accordance with the DHS directives over position sensitivity designations; and • Conduct civilian background re-investigations as required by DHS directives, to ensure that each civilian employee has a favorably adjudicated, valid, and required background investigation.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	which require a National Agency Check and Inquiries (NACI) investigation for those position designations with the lowest risk. A NACI consists of written inquiries and searches of records covering specific areas of a person's background during the past five years including current and past employers, schools attended, references, and local law enforcement authorities. However, all DHS government positions that use, develop, operate, or maintain IT systems are considered at least moderate risk (not low), and per DHS, 4300A requirements, a Minimum Background Investigation (MBI) is the minimum standard of investigation. The MBI consists of the NACI as well as a credit record search, face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. Therefore, Coast Guard is not in compliance with these DHS requirements. In addition, Coast Guard does not complete background re-investigations due to the lack of the requirement under current OPM guidance for low risk positions even though re-investigations must be completed every 10 years for moderate risk positions per DHS Management Directive (MD) 11050.2, *Personnel Security and Suitability Program*.				
CG-IT-09-42	As a result of our audit test work and supported by all the IT NFRs issued during the current year, we determined that Coast Guard is non-compliant with the Federal Financial Management Improvement Act (FFMIA) and we believe that Coast Guard has not fully addressed the	• Continue to implement and improve upon the monitoring of compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of the script configuration management controls.		X	3

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	recommendations in NFR CG-IT-08-42.	• Develop and implement corrective action plans to address and remediate the NFRs issued during the FY 2009 audit. These corrective action plans should be developed from the perspective of the identified root cause of the weakness both within the individual NFR and across related NFRs. The IT NFRs should not be assessed as individual issues to fix, but instead, should be assessed collectively based upon the control area where the weakness was identified. This approach enables corrective action that is more holistic in nature, thereby leading to a more efficient and effective processes of addressing/fixing the controls that are not operating effectively.			
CG-IT-09-43	Coast Guard procedures do not include a review of all UMS user accounts, as required by DHS 4300A Sensitive Systems Handbook and required by the DHS-CIO. A full 100% review of accounts that exceed 'read-only' access would ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with all UMS users are authorized and necessary.	Modify procedures to require an annual review of one hundred percent (100%) of UMS user accounts and their associated privileges that are greater than read-only. The updated procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individuals are still authorized and necessary.	X		2
CG-IT-09-45	Access was not authorized for two of the 15 individuals we tested who possessed badges allowing FINCEN data center access.	Include the badge software database during the data center access review process to ensure that no unauthorized individuals have badges that would allow them access to the FINCEN data center.	X		1

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-09-46	During our testing, we determined that all previous year conditions listed in NFRs CG-IT-08-36 and CG-IT-08-37 were properly remediated by Coast Guard. As part of this year's testing, we identified nine security configuration management weaknesses (i.e., missing security patches and/or incorrect configuration settings) on hosts supporting CAS and FPD.	Implement the corrective actions for the recommendations listed within the NFR.	X		1
CG-IT-09-47	Direct Access passwords do not require a special character, which is a requirement set forth within DHS 4300A Sensitive Systems Policy Directive.	Through our test work, we determined that the control weakness was remediated prior to the fiscal year-end; therefore, no recommendation is required for this NFR.	X		1
CG-IT-09-48	Global Pay accounts are configured to expire after five (5) invalid login attempts, rather than three (3), which is a requirement set forth within DHS 4300A Sensitive Systems Policy.	Through our test work, we determined that the control weaknesses were remediated prior to the fiscal year-end, therefore, no recommendation is required for this NFR.	X		1
CG-IT-09-49	The quarterly JUMPS audit log review addresses unusual activity or unexplained access attempts which DHS 4300A Sensitive Systems Policy Directive requires to be done on a monthly basis.	Review audit logs containing unusual activity and unexplained access attempts on an at least monthly basis to meet the requirements set forth in DHS 4300A, perform the necessary follow up on any incidents identified and maintain sufficient evidence of the audit log reviews, and include copies of audit logs in hard copy or electronic form and evidence that the review of the audit logs was conducted.	X		1
CG-IT-09-50	Not all Direct Access failed logon attempts are logged or reviewed; and account management audit logs for the Direct Access application are not reviewed on a monthly basis, which is a requirement set forth within the DHS	• Identify the Direct Access application security-oriented audit logs that should be reviewed and then have the application system administrators review those Direct Access application security logs on at least a monthly	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	Sensitive Systems Policy Directive.	basis, in accordance with DHS Policy. • Additionally, we recommend that the Coast Guard upgrade to a more current version of PeopleSoft and Oracle so that it uses a vendor supported product with more robust security controls and so that accountability may be established to document changes to security settings and user profiles.			
CG-IT-09-51	Only the last modification to the user account is documented by the COTS PeopleSoft application software, making it difficult to establish accountability for role changes within the Global Pay application. Additionally, role changes for the Global Pay Application are not reviewed on a monthly basis, which is a requirement set forth within DHS Policy.	Review role change logs on at least a monthly basis, in compliance with DHS Policy.	X		1
CG-IT-09-52	100% of Direct Access user accounts with greater than read-only access are not reviewed annually to verify that access remains appropriate, per the DHS 4300A Sensitive Systems Handbook and required by the DHS-CIO.	Modify procedures to require an annual review of one hundred percent (100%) of Direct Access user accounts and their associated privileges that are greater than read-only. The updated procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary.	X		2
CG-IT-09-53	During our after hours physical testing, we identified 11 passwords, 2 unsecured laptops, 2 credit cards, and 4 Common Access Cards (CAC).	• Review its policies and procedures regarding Protection of Sensitive Information and update where required in order to address DHS and other Federal requirements, with emphasis	X		1

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	During our social engineering testing, we were provided with one password.	being placed on the potential impacts of not consistently and adequately protecting this sensitive information. • Review, and update as required, its security awareness/training content to address the updated Protection of Sensitive Information policies and procedures. • Validate the effectiveness of the updated policies and procedures and associated training through mechanisms such as scheduled and unscheduled desk/floor reviews, awareness training testing, etc. and take appropriate corrective action to address any issued identified during this validation.			

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison to

Current Year Notices of Findings and Recommendations at Coast Guard

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

			Disposition	
Coast Guard Component	**NFR #**	**Description**	**Closed**	**Repeat**
FINCEN	08-01	The Coast Guard Finance Center (FINCEN) Continuity of Operations Plan (COOP) has not been updated to reflect the results of testing the COOP, and the Business Continuity Plans for each division have not been finalized.	X	
FINCEN	08-06	During the first half of the fiscal year, the contract with the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) software vendor was still in place, and no corrective action had taken place related to the prior year recommendation. Therefore, the risk exists that the condition was present for the majority of the fiscal year (October 1, 2007 through April 1, 2008). However, due to the Coast Guard decision to terminate the contract with their software vendor and the Coast Guard Headquarters decision to suspend all Software Problem Reports (SPRs) and Software Change Requests (SCRs), the condition did not exist beyond the date of these 2 events.	X	
PPC	08-07	We determined that Coast Guard's Pay and Personnel Center (PPC) has not implemented the following password requirements: • Passwords shall contain special characters • Passwords shall not contain any dictionary word • Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character • Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password • Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123" • Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123 • Passwords shall not be the same as the User ID While compensating controls were implemented to reduce the risk of unauthorized access, they unto themselves do not remove the potential risk from occurring.	X	
CG HQ	08-10	Coast Guard Headquarters has developed but not yet implemented policies and procedures to require that a favorably adjudicated background investigation be completed for all contractor personnel.		09-10
CG HQ	08-14	Coast Guard headquarters has not finalized the Role-Based Training for Coast Guard Information Assurance Professionals Commandant Instruction, which will require all Coast Guard members, employees,		09-14

			Disposition	
Coast Guard Component	**NFR #**	**Description**	**Closed**	**Repeat**
		and contractors with significant IT security responsibilities to receive initial specialized training and annual refresher training thereafter. The online Training Management Tool, which will track compliance, will not be implemented until the Role-Based Training is implemented.		
FINCEN	08-17	Although FINCEN has made significant progress in remediation, we were unable to verify that FINCEN is consistently remediating the vulnerabilities identified by the AppDetective scans in order to make it an effective mitigating control for the Checkfree application.	X	
OSC	08-23	Policies and procedures have not been developed and implemented for the manual periodic review of SAM audit logs. As a result, SAM audit logs are not periodically reviewed.		09-23
FINCEN	08-25	We determined the following weaknesses associated with the Workflow Imaging Network System (WINS) change controls: • Procedures have been created and implemented for the quarterly review of developer and analyst roles. However, the procedures do not include the review of all other WINS user accounts to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary. • 529 users have unlocked WINS database accounts with access to the WINS_USER_R role. Therefore, the number of users with the WINS_USER_R role has increased by 141 users from the 388 users noted during FY 2007. Additionally, a mapping of SQL flow roles within the WINS application to the tables that can be updated within the WINS database has not been created. Therefore, we are unable to perform an analysis of the SQL flow roles and the associated tables that are affected to determine whether access is appropriately restricted. • The password configurations for the PRODUSER and SECURE_LOGON profiles will not be updated to be in compliance with DHS guidance until after the 10G Release 2 (10gR2) Oracle database upgrade. Since no improvements have been made in regards to the WINS password configuration, we determined that the password configurations continue to not meet the following DHS requirement of having a user password contain at least one special character.		09-25
OSC	08-27	We noted that Coast Guard was unable to provide sufficient evidence of the following:	X	

			Disposition	
Coast Guard Component	**NFR #**	**Description**	**Closed**	**Repeat**
		• SAM access request forms are documented and approved; • SAM user accounts are revalidated annually; and • SAM access is revoked in a timely manner for employees or contractors that have left Coast Guard or are reassigned to other duties.		
FINCEN	08-31	Coast Guard's controls over the scripting process remain ineffective. Weaknesses were noted in controls over script implementation, approvals and testing, as well as active script modification. In addition, Coast Guard has not maintained or developed a population of scripts run since the inception of CAS in 2003 nor has it performed a historical analysis of script impact on the cumulative balances in permanent accounts of the financial statements. Specifically: • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests; • The Procedures for Data Scripts do not specifically state the testing and documentation requirements for blanket approval scripts and this policy remains in draft form; • Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through SQL Navigator to run scripts or review what scripts are run; • The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts; and, • Coast Guard has not completed PRP documentation for all scripts executed since their implementation.		09-31
CG HQ	08-32	Although Coast Guard Headquarters has mandated the use of Contractor Verification System (CVS) to maintain and track contracted personnel data, procedures surrounding this process have not been formally documented. As a result, we were unable to determine the effectiveness of the controls in place for contractor tracking.		09-32
CG HQ	08-33	Coast Guard does not consistently notify system owners that individuals are terminating from the Coast Guard so that system accounts can be updated timely.		09-33
FINCEN	08-34	All WINS SCRs are not being appropriately reviewed and approved by management prior to development/deployment. In addition, WINS developers and testers are not updating information in the		09-34

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

			Disposition	
Coast Guard Component	**NFR #**	**Description**	**Closed**	**Repeat**
		PVCS tool in a timely manner.		
FINCEN	08-35	We noted that control weaknesses still exist within the design of FINCEN's Configuration Management policies and procedures for CAS and FPD, as well as the operating effectiveness of those controls. Our test work over the design of the change controls covered both periods of the change control environment; however, our testing of operating effectiveness covered only the period of start of the fiscal year through March 2008, since no changes were made to CAS and FPD from April through the remainder of the fiscal year.	X	
FINCEN	08-36	Configuration management weaknesses continue to exist on hosts supporting the CAS, FPD and WINS applications and the underlying General Support Systems (GSS). Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions.	X	
FINCEN	08-37	Security patch management weaknesses continue to exist on hosts supporting the CAS, FPD and WINS applications and GSS. Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions.	X	
CG HQ	08-40	Although Coast Guard Headquarters is in the process of completing background investigations for all civilian employees, this has not been completed. Additionally, Coast Guard has set its position sensitivity designations to Low for the majority of its employees. However, DHS requires position sensitivity designations no less than Moderate which equates to a Minimum Background Investigation (MBI). Therefore, we determined that the conditions noted in prior year NFR CG-IT-07-40 have not been remediated.		09-40
FINCEN	08-41	FINCEN has not completed the risk assessment for the CAS Suite, and the CAS System Security Plan (SSP) is still in draft form.	X	
CG HQ	08-42	During prior financial statement audits dating back to FY 2003, we noted that implementation and oversight of the Coast Guard's information security policy and procedures was fragmented among the organizations responsible for operating various applications/systems. In FY 2008, significant improvements have been made in some areas; however, improvements are still warranted at the Coast Guard data centers/locations that operate and process key Coast Guard financial information. Improvements are needed		09-42

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

			Disposition	
Coast Guard Component	**NFR #**	**Description**	**Closed**	**Repeat**
		especially in the areas of change control and to a lesser extent, access to data and programs. These two key areas were the subject of significant findings identified and recommendations that were made during the audit. As a result of our audit test work and supported by all the IT NFRs issued during the current year, we determined that Coast Guard is non-compliant with the *Federal Financial Management Improvement Act.*		
FINCEN	08-43	During our testwork over CAS and FPD access accounts, we noted that controls over user account authorizations and controls over user account reviews were not operating effectively.		09-43

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W. STOP 7101
Washington, DC 20593-7101
Staff Symbol: CG-6
Phone: (202) 475-3637
Fax: (202) 475-3930
Email: Michael.W.Massino@uscg.mil

5500
FEB 26 2010

MEMORANDUM

From: M. B. Tytle, CAPT
Acting COMDT (CG-6)

Reply to CG-651
Attn of: Michael Massino
(202) 475-3637

To: Mr. Frank Deffer
Assistant Inspector General, Information Technology Audits
U.S Department of Homeland Security

Thru: K. A. Taylor, RDML
COMDT (CG-8) 2/22/11

Subj: RESPONSE TO INFORMATION TECHNOLOGY MANAGEMENT LETTER FOR THE U. S. COAST GUARD COMPONENT OF THE FISCAL YEAR 2009 DHS INTEGRATED AUDIT

Ref: (a) Mr. Frank Deffer Memo 5500 of 21 Jan 10

1. In response to reference (a), thank you for the DHS, Office of the Inspector General's (OIG) thorough, independent review of the general Information Technology (IT) controls associated with the USGC financial processing environment, IT infrastructure and overall security program. This process, combined with other proactive activities, helps the USCG improve its IT security posture.

2. The OIG identified several conditions and findings that require corrective actions by the USCG. The USCG concurs with the basis for the conditions and findings that were documented in the FY09 IT Notice of Findings and Recommendations (NFRs) and summarized within the IT Management Letter. Specific details of those findings, and their potential impacts, will be discussed early in the FY10 audit during the prior year's review process.

3. The USCG understands the need to continuously improve IT security operations and has demonstrated this commitment by proactively seeking ways to improve controls governing the script process. In seeking those improvements, during FY09, the USCG procured the services of an independent contractor to review internal controls over the USCG script process. The results of that review indicated sufficient compensating controls were in place to justify a low risk weakness versus the high risk rating ultimately assigned during the course of the audit. USCG does agree with the OIG's overall recommendations and is continuing to improve its scripting procedures. A part of this improvement involves the deployment of a more robust script management tool.

4. During the course of the audit, the USCG conducted a series of root cause analyses and determined the most appropriate method(s) for addressing identified weaknesses based upon

Subj: RESPONSE TO INFORMATION TECHNOLOGY MANAGEMENT LETTER FOR THE U. S. COAST GUARD COMPONENT OF THE FISCAL YEAR 2009 DHS INTEGRATED AUDIT

5500

FEB 26 200

system capabilities and resources. This process led the USCG to question several audit recommendations related to low risk impact items. The USCG continues to implement and execute corrective actions to address the underlying conditions and findings to mitigate risk and improve security. These corrective actions [*i.e.*, Plans of action and Milestones (POA&Ms)] are developed, monitored, and reported via the DHS Trusted Agent FISMA (TAF) tool.

5. The majority of the USCG system-oriented IT NFRs were mitigated as they were identified during the audit or early within FY10. The remaining low and moderate risk enterprise-wide / security program IT NFRs require multi-year efforts necessitating coordination between USCG and DHS Headquarters – and will require additional resources (budget and staff) as well.

6. The momentum and collaborative approach of the last two years has improved general Information Technology controls. The USCG looks forward to working with the DHS OIG during the FY10 audit, where we anticipate confirmation of our corrective action approach thorough measurable, tangible results.

a

Copy: CG-6
CG-65
CG-8
CG-84

2

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2009

Report Distribution

Department of Homeland Security

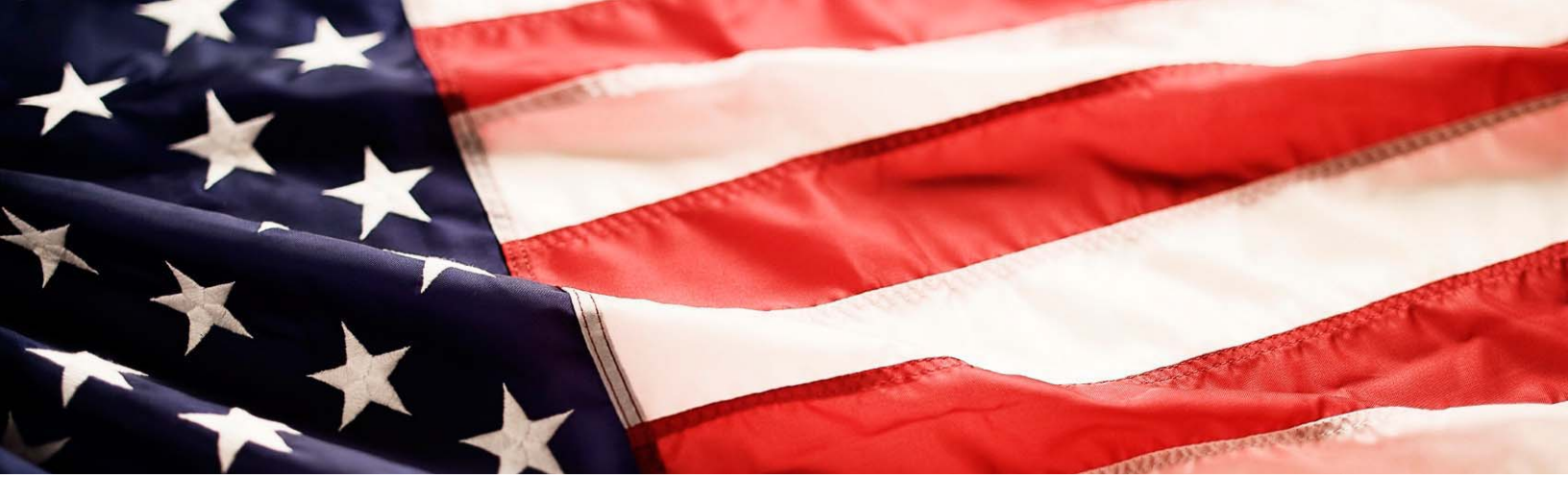
Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Commandant, USCG
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, USCG
Chief Information Officer, USCG
Chief Information Security Officer
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
USCG Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

• Call our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.