

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2005 Customs and Border Protection Balance Sheet Audit (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552 (b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-06-41

June 2006



**Homeland
Security**

JUN 29 2006

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 published by our office as part of our DHS oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report presents the information technology (IT) management letter for CBP's balance sheet audit as of September 30, 2005. It contains observations and recommendations related to information technology internal control that were not required to be reported in the balance sheet audit report (OIG-06-12, December 2005) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of CBP's balance sheet as of September 30, 2005, and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 2, 2005, and the conclusions expressed in it. We do not express opinions on CBP's financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been discussed in draft with those responsible for implementation. It is our hope that 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.


Richard L Skinner
Inspector General



KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 2, 2005

Inspector General
U.S. Department of Homeland Security

Commissioner
Bureau of Customs and Border Protection

Chief Information Officer
Bureau of Customs and Border Protection

We have audited the consolidated balance sheet of the U.S. Department of Homeland Security's Bureau of Customs and Border Protection (CBP) as of September 30, 2005. In planning and performing our audit of CBP's consolidated balance sheet, we considered CBP's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the consolidated balance sheet. Audit procedures may not include examining the effectiveness of internal controls and an audit does not provide assurance on internal control. We have not considered internal control since the date of our report.

During our audit, we noted certain matters involving internal control and other operational matters with respect to information technology that are summarized in the Information Technology Management Letter starting on page 1. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies. These comments are in addition to the reportable conditions presented in our *Independent Auditors' Report*, dated November 2, 2005, and represent the separate restricted distribution report mentioned in that report. A description of each Notice of Findings and Recommendations is provided in Appendix B. We have also included the current status of each prior year Notice of Findings and Recommendations in Appendix C. Our comments related to financial management that are in addition to the reportable conditions presented in our *Independent Auditors' Report* will be reported in the DHS consolidated management letter.

Our audit procedures were designed primarily to enable us to form an opinion on the consolidated balance sheet and therefore may not bring to light all weaknesses in policies and procedures that may exist. We aim, however, to use our knowledge of CBP's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

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

Very truly yours,

**Information Technology Management Letter for the FY 2005 Customs and Border Protection
Financial Statement Audit**

Department of Homeland Security - Customs and Border Protection

Information Technology Management Letter

September 30, 2005

A handwritten signature in black ink that reads "Robert Todero". The signature is written in a cursive style with a large, looped initial "R".

Robert Todero
Partner

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
September 30, 2005

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

	Page
Information Technology Objective, Scope and Approach	1
Summary of Findings and Recommendations	2
Findings by Audit Area	2
Entity-Wide Security Program Planning and Management	2
Access Controls	3
Segregation of Duties	5
Service Continuity	6
Application Software Development and Change Controls	6
Management Comments and OIG Evaluation	7

Appendix	Subject	Page
A	Description of Financial Systems and IT Infrastructure within the Scope of the FY 2005 CBP Balance Sheet Audit	8
B	FY 2005 CBP Notices of Findings and Recommendations – IT Detail	10
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notice of Findings and Recommendations	18
D	Management Response to Draft CBP IT Management Letter	21

INFORMATION TECHNOLOGY OBJECTIVE, SCOPE AND APPROACH

KPMG performed a review of CBP's IT general controls in support of the FY 2005 CBP consolidated balance sheet audit. The overall objective of our review was to evaluate the effectiveness of IT general controls of CBP's financial processing environment and related IT infrastructure as necessary to support the audit. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our review and was supplemented by the National Institute of Standards and Technology (NIST) Special Publication 800-53 and applicable CBP and DHS policies. The scope of the IT general controls assessment included testing at CBP's Office of Finance and Office of Information Technology.

FISCAM is 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 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.

- *Entity-wide security program planning and management (EWS)* – 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.
- *System software (SS)* – Controls that limit and monitor access to powerful programs that operate computer hardware.
- *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.
- *Service continuity (SC)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.

To complement our general IT controls review, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls. The technical security testing was performed from within CBP, and was focused on test, development, and production devices that directly support CBP financial processing and key general support systems. We also tested application controls, which are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. The application control testing was performed to assess the controls that support the financial system's internal controls over the input, processing, and output of financial data and transactions.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2005, CBP took corrective action to address prior year IT control weaknesses. However, during FY 2005, we continued to find IT general control weaknesses at CBP. The most significant weaknesses from a balance sheet audit perspective related to entity-wide security and access controls. Collectively, the IT control weaknesses limited CBP's ability to ensure that critical financial and operational data was maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over CBP financial reporting and its operation, and we consider them to collectively represent a material weakness under standards established by the AICPA. The information technology findings were consolidated into one material weakness regarding *Financial Systems Functionality and Technology* for the FY 2005 audit of the CBP consolidated balance sheet.

Although we noted improvement, many of the conditions identified at CBP in FY 2004 during our engagement to audit DHS' consolidated financial statements have not been corrected because CBP still faces challenges related to the merging of numerous IT functions, controls, processes, and overall organizational shortages. During FY 2005, CBP took steps to help address these conditions, such as implementing increased controls over access to sensitive applications functions, improving its IT security program by implementing CBP-wide security training and implementing a new financial management system replacing the legacy mainframe system.

Despite these improvements, CBP needs further emphasis on the monitoring and enforcement of the policies and procedures through the performance of periodic security control assessments and audits. Further improvements are needed in implementing and enforcing the CBP-wide security certification and accreditation (C&A) program, and technical security control training for system administrators and security officers. Many of the technical issues identified during our review, which were also identified during FY 2004, such as weak system access controls and inconsistent contingency planning, can be addressed through a more effective security C&A program and security training program.

FINDINGS BY AUDIT AREA

Entity-Wide Security Program Planning and Management

During FY 2005, CBP improved its level of entity-wide security program planning and management. However, continued efforts are needed, especially in the areas of program management related to the detection and monitoring of technical information security weaknesses. Collectively, the identified entity-wide security planning and management issues, coupled with the access control issues described later in this management letter, reduce the overall effectiveness of the entity-wide security programs for CBP.

Conditions noted regarding entity-wide security program planning and management at CBP were:

- Security risk assessments were not performed regularly and consistently;
- CBP has not made efforts to evaluate the need for a separate C&A for the applications remaining in the seven business process areas defined in the Administrative Applications C&A;

Department of Homeland Security - Customs and Border Protection

Information Technology Management Letter

September 30, 2005

- Initial security awareness training for CBP employees and contractors was not completed; and
- Improvements are still needed in CBP's Incident Handling and Response Capability. Specifically, issues still exist related to incident prevention, response, recovery, and reporting.

There is a process in place for tracking incidents. However, process is not consistent and/or complete. Incidents were not included on requested weekly reports and incident documentation was missing.

Recommendations:

Entity-wide security program planning and management controls should be in place to establish a framework and continuing cycle of activity to manage security risk, develop security policies, assign responsibilities, and monitor the adequacy of computer security related controls. We recommend that the CBP Chief Information Officer (CIO), in coordination with the Chief Financial Officer (CFO), other CBP functional leaders, and the DHS CIO continue efforts to fully implement a security program to ensure that:

- Security risk assessments are regularly completed in a consistent manner per Office of Management and Budget (OMB) and NIST guidance;
- Information security planning efforts more consistently follow Federal guidance (OMB and NIST) specifically regarding the implementation and enforcement of the C&A program and with respect to the applications remaining in the seven business process areas defined in the Administrative Application C&A;
- Management consistently applies the requirements for initial security awareness training for all employees and contractors upon initially establishing LAN/mainframe accounts to CBP information systems; and
- Continue to test and implement a standard real-time automated reporting process whereby information can be generated on all incidents, response, and recovery activities on a regular basis for servers and workstations. Additionally, management should develop a consistent process to respond to system flaw notifications and track reported security incidents.

Access Controls

During FY 2005 we noted significant access control vulnerabilities with [redacted]. These are significant issues because personnel inside the organization who best understand the organization's systems, applications, and business processes were able to make unauthorized access to some systems and applications. Some of the identified vulnerable devices were used for test and development purposes. In some cases, users were able to access [redacted] with group passwords, system default passwords, or the same passwords with which they logged into [redacted]. As a result, hackers could target [redacted].

Department of Homeland Security - Customs and Border Protection

Information Technology Management Letter

September 30, 2005

[REDACTED] to obtain information (e.g., [REDACTED]) to attempt further access into CBP's IT environment.

Conditions noted regarding access controls at CBP were:

- Instances where non-supervisory users had excessive access to sensitive and high-risk [REDACTED];
- Instances within [REDACTED] where certain controls could be overridden without supervisory approval;
- Instances where policies and procedures for restricting and monitoring access to CBP's [REDACTED] were not implemented or were inadequate, the ability to monitor security logs did not exist, and separated employees had active accounts in [REDACTED];
- Instances of missing user passwords [REDACTED] - weak user passwords, and weaknesses in user account management. We also noted several cases where user accounts were not periodically reviewed for appropriateness, including authorizations to use group user accounts and excessive account privileges;
- Instances where legacy point-to-point frame relay connections existed without formal interconnection service agreements (ISA);
- No formal process existed to confirm or enforce compliance with the [REDACTED] re-certification process at the field sites;
- Physical access to the [REDACTED] was not adequately implemented or enforced; and
- Inconsistent authorization and recertification process for virtual private network (VPN) users.

Recommendations:

In close concert with an organization's entity-wide information security program, access controls for general support systems and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, loss, or impairment. Access controls are facilitated by an organization's entity-wide security program. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of information.

We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders:

- Ensure that the assignment of sensitive functions and high-risk combinations of functions to non-supervisory users is based on a documented business need and approved by a supervisory

Department of Homeland Security - Customs and Border Protection

Information Technology Management Letter

September 30, 2005

official. Exceptions from the guidance provided in the memorandum should be formally approved and documented.

- Develop a process to mitigate the systemic [redacted] weakness where certain controls can be overridden without supervisory approval.
- Implement and enforce a password account management process to ensure the periodic review of user accounts. Develop a formal centralized process for tracking the termination of employee and contract personnel and coordinate the deactivation of all systems access of terminated employees and contractors immediately upon separation from CBP. Design and implement an entity-wide security configuration process to enforce the guideline of least privilege system access and the monitoring of security logs [redacted].
- Implement a formal vulnerability assessment process whereby systems are periodically reviewed for security weaknesses and ensure that password controls meet DHS and CBP password requirements on all systems;
- Complete efforts to identify all connections with the [redacted] and formally establish ISAs with these entities;
- Formalize the process to confirm or enforce compliance with the [redacted] and formally document the verification of [redacted].
- Perform a formal review of all personnel that have access to [redacted], determine those that do not have a formal user access form in place. Confirm that current personnel with [redacted] actually need this access to perform their job functions and remove those who do not. Additionally, establish a formal authorized user access form for each person identified; and
- Continue to use the official authorization form for new VPN users, formally re-certify all VPN employee accounts on a periodic basis and document results.

Segregation of Duties

During FY 2005, we continued to note instances where an individual controlled more than one critical function within a process, increasing the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed, without detection. Additionally, we noted a lack of segregation of duties among major operating and programming activities, including duties performed by users, application programmers, and data center staff.

Conditions noted regarding segregation of duties at CBP were:

- Instances where individuals were able to perform incompatible functions, such as the changing, testing, and implementation of software, without sufficient compensating controls in place; and

Department of Homeland Security - Customs and Border Protection

Information Technology Management Letter

September 30, 2005

- Instances where key security positions were not defined or assigned, and descriptions of positions were not documented or updated.

Recommendations:

We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders, ensure that:

- Responsibilities are documented so that incompatible duties are consistently separated. If this is not feasible given the smaller size of certain functions, then sufficient compensating controls, such as periodic peer reviews, should be implemented; and
- Policies and procedures are developed and documented to assign key security positions and maintain current position descriptions.

Service Continuity

During FY 2005 we noted that CBP took some corrective actions to address IT control issues related to the back-up and protection of critical system data. Despite these improvements, a weakness related to disaster recovery plans and business continuity plans continued to exist. Service continuity is important because losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission.

The condition noted regarding service continuity at CBP was:

- An incomplete and outdated alternate processing site agreement regarding specifics related to the identified equipment and priority service requirements.

Recommendation:

We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders:

- Formally update the alternate processing site agreement to accurately reflect the current hardware and support that will be required of the alternate processing site vendor in the event of an emergency.

Application Software Development and Change Control

During FY 2005 we noted that CBP took corrective actions to address IT control issues related to application software changes. However, we noted that in some cases the application software change control documentation was still not consistent with CBP guidance.

Conditions noted regarding configuration management and change control at CBP were:

- Instances where  application developers were found with access to the production environment;

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
September 30, 2005

- Instances where [redacted] codes were not configured to the “Productive” setting, allowing users with "mass deletion/change" access to transactional data; and
- Instances where changes to [redacted] were not always documented.

Recommendations:

We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders:

- Develop and employ a formally documented process for granting [redacted] normal and emergency access to the production environment;
- Perform a formal analysis of the new [redacted] system’s configurations to determine the appropriate settings to prevent users from accidentally or purposely deleting or altering transactional data. Based on this analysis, the system should be configured accordingly; and
- Formally document test plans, test cases, and test results for all [redacted] changes and formally document business and customer impact analyses for [redacted] change requests.

MANAGEMENT COMMENTS AND OIG EVALUATION

We obtained written comments on a draft of this report from the CBP CIO. Generally, the CBP CIO agreed with all of the report’s findings and recommendations. We have incorporated the comments where appropriate and included a copy of the comments in their entirety at Appendix D.

In his response, the CBP CIO stated that CBP is:

- Taking steps to ensure that entity-wide security program planning and management controls are in place to establish a framework and continuing cycle of activity to manage security risk;
- Working to ensure that the assignment of sensitive functions is legitimate, that the weaknesses that can lead to a control override in certain systems is mitigated, and that physical and electronic access to sensitive CBP systems is secured and carefully monitored;
- Continuing to develop applicable policies and procedures to ensure that certain duties are separated, as necessary and to monitor user roles and new user or access requests to prevent future segregation of duty conflicts;
- Working to ensure that the [redacted] Continuity of Operations Plan (COOP) is as current as possible, and that the alternate processing site has the hardware and support necessary to continue operations in the event of an emergency; and
- Ensuring that proper separation of roles between the development and production environments are established.

OIG Response

We agree with the steps that CBP is taking to satisfy these recommendations.

United States Bureau of Customs and Border Protection
Information Technology Management Letter
September 30, 2005

Appendix A

**Description of Financial Systems and IT Infrastructure within the
Scope of the FY 2005 CBP Balance Sheet Audit**

United States Bureau of Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

Below is a description of significant CBP financial management systems and supporting IT infrastructure included in the scope of the September 30, 2005 CBP consolidated balance sheet audit.

Locations of Review:

[REDACTED]

Systems Subject to Review:

[REDACTED] was decommissioned in FY 2005 and replaced by [REDACTED]. It was CBP's IBM [REDACTED] based financial management system that supported primary financial accounting and reporting processes, and a number of additional subsystems for specific operational and administrative management functions. The core system consisted of general ledger, accounts receivable, disbursements/payables, purchasing, and budget execution modules. [REDACTED] was hosted on a customized version of [REDACTED].

- [REDACTED] – [REDACTED] is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the [REDACTED] using a phased approach. The [REDACTED] was implemented and utilized in FY 2004. Other [REDACTED] were implemented in FY 2005.
- [REDACTED] is a collection of mainframe-based applications used to track, control, and process all commercial goods, conveyances and private aircraft entering the United States territory, for the purpose of collecting import duties, fees, and taxes owed the Federal government.
- [REDACTED] – Used for tracking seized assets, Customs Forfeiture Fund, and fines & penalties.

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
September 30, 2005

Appendix B

FY 2005 CBP

Notices of Findings and Recommendations – IT Detail

Department of Homeland Security - Customs and Border Protection
 Information Technology Management Letter
 September 30, 2005

FY 2005 CBP Notices of Findings and Recommendations – IT Detail

NFR #	Condition	Recommendation
CBP-IT-05-01	A number of [redacted] IDs had a segregation of duties conflict.	Coordinate with each field office that has a segregation of duties conflict to either (1) correct the problem by removing the conflicting roles, or (2) sign a waiver to accept responsibility for issues arising from the segregation of duties conflict. Continue to prevent new IDs with a segregation of duties conflict from being created.
CBP-IT-05-02	<p>Three [redacted] [redacted] to specify security modes for individual users without a justified business need.</p> <p>Two [redacted] with [redacted] had full security administration privileges, which violated separation of duties principles.</p> <p>One [redacted] account had not been utilized since August 6, 2004.</p>	<p>Remove unnecessary privileges and/or accounts given the exceptions we noted related to the authorities/functions granted to certain [redacted]. Accesses granted should be based on the least privilege concept to the minimum number of personnel with a defined and documented need.</p> <p>As an alternate means of providing availability to functions not used on a regular basis, continue implementation of a [redacted] for use by authorized individuals during pre-determined circumstances. Establishment of a [redacted] would enable the removal of privileges from individuals who do not regularly require such access [redacted] are controlled through the use of a hardcopy log, secure storage of passwords, auditing of all [redacted] activities and suspension after each use.</p>
CBP-IT-05-03	After the re-organization of the Office of Information Technology (OIT), security administration functions at the [redacted] including mainframe security, network security, and incident response, were not independent of the operations function. Rather, the Security Operations Center reported to Technology Operations, which was not an independent security function.	Ensure that security administration functions remain independent of operations. In order to maintain independence, the security administration function should not report to operations management.
CBP-IT-05-04	Due to the design of [redacted] certain controls could be overridden without supervisory approval. Management plans to implement functionality in the [redacted] to prevent the override capability. KPMG noted that although [redacted] will eventually replace [redacted] will not be implemented in FY 2005.	Develop a process to mitigate the systemic [redacted] weakness that certain controls can be overridden without supervisory approval. Considering the number of years necessary to fully replace [redacted] functionality with [redacted] this process should be designed in a manner to ensure supervisory review of [redacted] overrides while maintaining a minimal burden on management. CBP should ensure that the new [redacted] system has the appropriate requirements for such controls and that these controls are applied prior to implementation.
CBP-IT-05-05	Formal procedures for granting access to	Formally establish a process for granting [redacted]

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

NFR #	Condition	Recommendation
	sensitive [redacted] technical team member roles have not been developed.	access to sensitive technical team roles (e.g. basis and security team members) and consistently apply these processes. The procedures should include requirements for documenting the authorization request and include the exact roles that should be granted. Additionally, the procedures should require a periodic documented recertification of the user roles within [redacted].
CBP-IT-05-06	The [redacted] contingency plan has not been updated with the results of the FY 2004 continuity of operations plan (COOP) tests. Additionally, the COOP has not undergone the annual re-evaluation as required. Also, implementation of the new financial management system changed the mainframe environment to a client-server based [redacted] environment. However, the plan has not been updated and, therefore, might contain outdated and improper contingency procedures for information systems and data.	Update the [redacted] COOP with the most recent test results. Additionally, re-evaluate the COOP for overall contingency planning procedures on an annual basis, especially in the event of a major system change or upgrade, such as [redacted].
CBP-IT-05-08	The requirement for initial security awareness training for employees and contractors was not consistently applied.	Consistently apply the requirements for initial security awareness training for all employees and contractors upon initially establishing LAN/mainframe accounts to information systems.
CBP-IT-05-09	Improvements were still needed in security controls affecting [redacted] management and staff's system access to applications and data.	<p>Coordinate with DHS in developing enterprise-wide solutions for improving network and host-based system configuration design(s) to reduce the risks of compromise.</p> <p>Consider use of system administrator level security management monitoring tools to detect and correct security deficiencies in preventing possible intrusions. Use of such tools should include a planned "prioritized" schedule for checking all servers.</p> <p>Proceed with the implementation of [redacted]</p> <p>Provide and approve more robust standards for [redacted] for a standard and sustainable baseline set of system management security controls.</p> <p>Consider development of a compliance-level policy that provides for adherence to agency password management policies. This policy should be developed at [redacted] where</p>

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

NFR #	Condition	Recommendation
		<p>local system administrators and help desk staff may apply such policies (e.g., changing password age, account lockout, password uniqueness, password length, etc.).</p> <p>For [redacted] review, justify, and ensure that the level of access is based on strict adherence to least privilege principles where the absolute minimum level necessary is applied. As CBP moves with DHS toward more technology efficient enterprise-wide solutions (e.g., centralized means of managing network assets), the ability to reduce current levels will be enhanced.</p>
<p>CBP-IT-05-10</p>	<p>[redacted] security audit log reviews were not evidenced for the majority of FY 2005.</p>	<p>Continue to review the audit logs daily and maintain documented evidence.</p> <p>Train backup personnel to perform this task in the event that the primary personnel performing this task are not available.</p>
<p>CBP-IT-05-11</p>	<p>[redacted] administrator staff have not documented ISAs for all entities that connect with the [redacted]. Although there was [redacted] of all partners that have an ISA with CBP, this database failed to capture all connections with [redacted]. The majority of financial institutions connected to [redacted] have not formally established ISAs.</p>	<p>Complete efforts to identify [redacted] connections that are considered “legacy” connections and formally establish ISAs with these entities.</p> <p>Complete efforts to identify all connections with the [redacted] and formally establish ISAs with these entities.</p>
<p>CBP-IT-05-12</p>	<p>The “equipment” and “priority of service” requirements have not been annually updated. As a result, the agreement was outdated and did not reflect the current operating environment at [redacted].</p>	<p>Formally update the alternate processing site agreement to accurately reflect the current hardware and support that will be required of the alternate processing site vendor in the event of an emergency.</p>
<p>CBP-IT-05-13</p>	<p>No formal process existed to confirm or enforce compliance with the [redacted]. Although field site administrators were trained to perform the re-certifications every six months, there was no management oversight to ensure that the field site administrators were performing the re-certifications.</p>	<p>Formalize the process to confirm or enforce compliance with the [redacted] at the field sites and formally document the verification of field site [redacted].</p>
<p>CBP-IT-05-14</p>	<p>Procedures have not been adequately implemented for restricting access to the data center located in [redacted]. Specifically, nineteen out of thirty-two individuals selected did not have proper authorizations documented for access to the data center.</p>	<p>Perform a formal review of all personnel who have access to the [redacted] to determine those who do not have a formal user access form in place. Establish a formally authorized user access form for each person identified.</p> <p>Confirm that current personnel with data center access actually need this access to perform their job</p>

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

NFR #	Condition	Recommendation
		<p>functions.</p> <p>Promptly remove physical access rights to the [redacted] facility when an employee is terminated, thus, restricting access to the data center.</p>
<p>CBP-IT-05-15</p>	<p>[redacted] had access to the production environment.</p>	<p>Develop a formally documented process for granting normal and emergency access for [redacted] to the [redacted] production environment. The access request and authorization should include specific justification for their access and be documented and retained.</p>
<p>CBP-IT-05-16</p>	<p>Improvements were still needed in CBP's Incident Handling and Response Capability. Specifically, issues still exist related to incident prevention, response, recovery, and reporting.</p> <p>[redacted]</p> <p>A formal automated reporting capability does not exist to report, in a timely manner, on the servers and workstations with identified vulnerabilities, the number that have been patched, and the number of servers that remain vulnerable.</p> <p>There is a process in place for tracking incidents. However, the weekly incident report process is not consistent and/or complete. Incidents were not included on requested weekly reports and incident documentation was missing. Sample information or evidence was not available for system flaw notifications.</p>	<p>Develop a process to identify the workstations that have yet to install the [redacted].</p> <p>Continue to test and implement a standard real-time automated reporting process whereby information can be generated on all incidents, response, and recovery activities on a regular basis for servers and workstations.</p> <p>Develop a consistent process to respond to system flaw notifications and track reported security incidents.</p>
<p>CBP-IT-05-17</p>	<p>[redacted] was not configured to indicate a company code setting of "productive."</p>	<p>Perform a formal analysis of the company code setting to determine if it should be set to "productive." This will prevent users with "mass deletion/change" access the ability to accidentally or purposely delete transactional data.</p>
<p>CBP-IT-05-18</p>	<p>An excessive number of users had access to sensitive [redacted] unctions and high-risk combinations of functions.</p>	<p>Ensure that the assignment of sensitive functions and high-risk combinations of functions to non-supervisory users is based on a documented business need and approved by a supervisory official. Exceptions from the guidance provided in the memorandum should be formally approved and</p>

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

NFR #	Condition	Recommendation
		documented.
CBP-IT-05-19	A number of separated employees' names appeared on the [redacted] active user access listing.	<p>Determine whether the potential matches are actual matches. Delete the accounts of any confirmed terminated employees.</p> <p>Continue to use the payroll feed to determine if a [redacted] user has terminated employment.</p> <p>Disable user accounts of separated employees and contractors as stated in CBP and NIST guidance.</p>
CBP-IT-05-20	<p>No process existed to formally document test plans, test cases, and test results for [redacted] security and configuration changes.</p> <p>The [redacted] Change Control Board was not performing formal business and customer impact analyses for [redacted] change requests.</p>	<p>Formally document test plans, test cases, and test results for all [redacted] changes.</p> <p>Formally document business and customer impact analyses for [redacted] change requests.</p>
CBP-IT-05-21	<p>Logging of critical tables within [redacted] has not been activated.</p> <p>A formal analysis of the tables that should be logged in the [redacted] environment has not been performed, solely relying on recommendations of a previous audit.</p>	<p>Perform a formally documented assessment of the tables that should be logged by [redacted]</p> <p>Complete the implementation of table logging within [redacted]</p>
CBP-IT-05-22	A certification and accreditation package for all components of the [redacted] LAN has not been completed. Specifically, a security control assessment was not conducted for the [redacted] LAN as a whole within the last year. Also, a formal risk assessment was not conducted for all [redacted] LAN components.	Complete a security control assessment for all [redacted] LAN components and complete a risk assessment for all [redacted] LAN components.
CBP-IT-05-23	NIST 800-26 assessments for the seven business areas within the seven Administrative Applications have not been completed. No efforts have been made to evaluate the need for a separate C&A for the applications remaining in the seven business process areas defined in the Administrative Applications C&A. Also, additional improvements in consolidated guidance were necessary to address the issue of linking risks/threats to requirements.	<p>Using federal guidelines outlining what constitutes a major application, consider reviewing the sensitivity of applications classified as part of [redacted] administrative systems separately to determine which applications warrant individual C&As as major applications, and which applications should remain as part of the current Administrative C&A process. Based on results of the sensitivity review, perform separate C&As, where appropriate.</p> <p>In accepting risks associated with [redacted], consider establishing a relationship of identified risks to defined security requirements in [redacted]. This will assist in understanding what risks are mitigated by existing controls and what residual risks remain that management is willing to accept.</p> <p>Given that the [redacted] deployment may not be</p>

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

NFR #	Condition	Recommendation
		<p>completed by the end of the current [redacted] certification period, incorporate a risk-based approach for any re-certification efforts performed, where threats identified are tied to security requirements and mitigating controls.</p> <p>Consider development of definitive guidance for risk assessments and security plan criteria. These criteria should be applied to tie identified risks and threats to security requirements and controls that mitigate risks to acceptable levels. This will allow for the adequate tracking and evaluation of risks and requirements throughout a system's lifecycle. Therefore, management should be able to definitively recognize what acceptable risks remain.</p>
<p>CBP-IT-05-24</p>	<p>A centralized listing of separated contract personnel was not maintained. The only method employed to track terminated contractors was the use of a report of users that had their mainframe account deleted. This list was not representative of all terminated contractors since terminated contract personnel might not have had mainframe access or their access might not have been removed after their termination.</p>	<p>Develop a formal centralized process for tracking the termination of contract personnel.</p> <p>Deactivate all systems access for terminated contractors immediately upon separation.</p> <p>Periodically distribute a listing of terminated contract personnel to information system administrators so they remove user access and periodically assess contractor access to systems.</p>
<p>CBP-IT-05-25</p>	<p>The mainframe disconnected idle sessions after 30 minutes of inactivity rather than the prescribed 20 minutes of inactivity noted in the <i>U.S. Customs and Border Protection, Information Systems Security Policies and Procedures Handbook</i>.</p>	<p>Modify the setting on the [redacted] to disconnect idle sessions as specified by agency policy or ensure the policy is accurate. (Note: [redacted])</p> <p>[redacted]</p>
<p>CBP-IT-05-26</p>	<p>[redacted] did not have an automated mechanism to detect and deactivate users that had not logged on for 90 days. Procedures to perform a monthly review for inactive accounts in July 2005 were implemented. However, for majority of FY 2005, this procedure was not in place.</p>	<p>Continue to review and deactivate inactive accounts on a monthly basis.</p> <p>Implement an automated mechanism to detect and deactivate inactive accounts.</p>
<p>CBP-IT-05-27</p>	<p>The formal process to grant VPN access using an authorization form was recently implemented. However, VPN access authorization forms were not available for the majority of employees selected. Also, VPN employee accounts were not periodically re-certified.</p>	<p>Continue to use the official authorization form for new VPN users. Re-certify all VPN employee accounts on a periodic basis and document results.</p>
<p>CBP-IT-05-28</p>	<p>Action has not been taken to address the prior-year issue that users with access to [redacted]</p>	<p>Re-certify users with access [redacted] and document the evidence of the re-certification.</p>

Department of Homeland Security - Customs and Border Protection
Information Technology Management Letter
 September 30, 2005

NFR #	Condition	Recommendation
	<p>[redacted] may be excessive.</p>	
CBP-IT-05-29	<p>In FY 2004, issues with access to [redacted]. Some profiles with access to modify the [redacted] [redacted] represented a segregation of duties conflict.</p> <p>In FY 2005, [redacted] was replaced by [redacted]. KPMG attempted to determine whether the same issue existed in [redacted]. Information regarding whether [redacted] (or equivalent) were appropriately segregated could not be provided.</p>	<p>Document that access to the [redacted] [redacted] (or equivalent) is properly segregated. This includes a review [redacted] access to determine if the current granted access is appropriate.</p>
CBP-IT-05-30	<p>Action has not been taken to address the prior-year finding that the number of users with access to [redacted], Recovery, and Backup datasets may be excessive.</p>	<p>Re-certify users with access to [redacted] Recovery, and Backup datasets. Document the evidence of the re-certification.</p>
CBP-IT-05-31	<p>As part of the Common Local Area Network (LAN) Operating Environment (CLOE) type accreditation to perform formal risk assessments, [redacted] LANs dispersed across many field sites were not to be visited. As a result, management asserted that they were requiring each field site on the 'non-recommended' listing to submit a formal NIST 800-26 assessment for their LAN. Based on this, a sample of 15 field sites were selected from the non-recommended field site listing and we requested evidence of the NIST 800-26 review of their LAN. In a sample of 15 field sites, three site assessments were not provided.</p>	<p>Continue to develop a formal process to ensure that all non-recommended field sites submit a NIST 800-26 LAN self-assessment in a timely manner.</p>

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Appendix C

**Status of Prior Year Notices of Findings and Recommendations
And Comparison To
Current Year Notices of Findings and Recommendations**

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

**Status of Prior Year Notices of Findings and Recommendations
 And Comparison To
 Current Year Notices of Findings and Recommendations**

Ref	Condition	Status
CBP-IT-04-01	Inconsistent [REDACTED] to include excessive access to high-level functions	Issue noted in FY 2005. See NFRs CBP-IT-05-02 and CBP-IT-05-03.
CBP-IT-04-02	Inconsistent application certification and accreditation for all applications in the seven business process areas defined as Administrative Applications	Issue noted in FY 2005. See NFR CBP-IT-05-23.
CBP-IT-04-03	Continuity of critical [REDACTED] operational functions is in question at CBP alternate processing site	This condition has been corrected.
CBP-IT-04-04	Excessive assignment of [REDACTED] sensitive functions and high-risk combinations	Issue noted in FY 2005. See NFR CBP-IT-05-18.
CBP-IT-04-05	Controls in [REDACTED] can be overridden without supervisory approval	Issue noted in FY 2005. See NFR CBP-IT-05-04.
CBP-IT-04-06	Excessive access to [REDACTED]	This condition has been corrected.
CBP-IT-04-07	Inconsistent field site security program management	Issue noted in FY 2005. See NFR CBP-IT-05-31.
CBP-IT-04-08	Weaknesses identified in system logical access controls over network assets	Issue noted in FY 2005. See NFR CBP-IT-05-09.
CBP-IT-04-09	Excessive access to [REDACTED] vendor/bank tables	Issue noted in FY 2005. See NFR CBP-IT-05-29.
CBP-IT-04-10	Incomplete interconnection security agreements (ISAs)	Issue noted in FY 2005. See NFR CBP-IT-05-11.
CBP-IT-04-11	Inconsistent and incomplete [REDACTED] risk assessment	This condition has been corrected.
CBP-IT-04-12	Weaknesses identified in CBP's on-line Transaction Processing System Security [REDACTED]	Issue noted in FY 2005. See NFR CBP-IT-05-28.

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

Ref	Condition	Status
CBP-IT-04-13	Weaknesses in [REDACTED] Segregation of Duties	Issue noted in FY 2005. See NFR CBP-IT-05-01.
CBP-IT-04-14	Weaknesses exist in CBP's Incident Response Capability, specifically related to Detection and Incident Initiation; Response and Recovery; and Incident Server Patch Management Reporting.	Issue noted in FY 2005. See NFR CBP-IT-05-16.
CBP-IT-04-15	Inconsistent review of [REDACTED] logging documentation	This condition has been corrected.
CBP-IT-04-16	[REDACTED] Materials Management access control weakness regarding inconsistently documented authorizations	Issue noted in FY 2005. See NFR CBP-IT-05-05.
CBP-IT-04-17	[REDACTED] General Controls Environment for Materials Management Module: System access, user account management, and configuration weaknesses identified	Issue noted in FY 2005. See NFR CBP-IT-05-09.
CBP-IT-04-18	Inconsistent use of least privilege principles regarding Mainframe User Groups' access to sensitive datasets/utilities	Issue noted in FY 2005. See NFR CBP-IT-05-30.

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Appendix D

Management Response to Draft CBP IT Management Letter

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

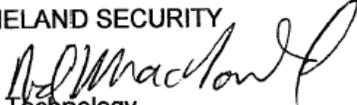
U.S. Department of Homeland Security
Washington, DC 20229



U.S. Customs and
Border Protection

MAR - 2 2006

MEMORANDUM FOR THE ASSISTANT INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Assistant Commissioner 
Office of Information and Technology

SUBJECT: Draft Audit Report – Information Technology Management
Letter for the FY 2005 Customs and Border Protection
Financial Statement Audit

This is in reply to your memorandum dated January 23, 2006, requesting comments on the subject draft audit report. As the findings and recommendations in your report are being addressed by the Customs and Border Protection Office of Information and Technology, OIT is providing the following comments for CBP.

Entity-wide Security Program Planning and Management

CBP concurs with KPMG's recommendations in this area. We are taking steps to ensure that entity-wide security program planning and management controls are in place to establish a framework and continuing cycle of activity to manage security risk. These steps will include regular security risk assessments, information security planning efforts consistent with OMB and NIST, consistently applied security awareness training, and the implementation of a real-time automated reporting process for security incidents. Plans of actions and milestones (POAMs) have been developed for the Notices of Findings and Recommendations (NFRs) included in Appendix B of this report. As part of our response, we have included the target completion dates for each NFR in Appendix B.

Access Controls

CBP concurs with KPMG's recommendations in this area. We will work to ensure that the assignment of sensitive functions is legitimate, that the weaknesses that can lead to a control override in certain systems is mitigated, and that physical and electronic access to sensitive CBP systems is secured and carefully monitored. POAMs have been developed for the NFRs included in Appendix B of this report. As part of our response, we have included the target completion dates for each NFR in Appendix B.

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Segregation of Duties

CBP concurs with the majority of KPMG's recommendations in this area. We will continue to develop applicable policies and procedures to ensure that certain duties are separated, as necessary, and to monitor user roles and new user or access requests to prevent segregation of duty conflicts from occurring in the future. POAMs have been developed for the NFRs included in Appendix B of this report. As part of our response, we have included the target completion dates for each NFR in Appendix B. With regard to Security Administration functions reporting to operations, CBP does not concur with the KPMG recommendation. While the Security Operations Center is part of the Technology Operations Division, they are organizationally separated from Data Center Operations. Additionally, the Information Systems Security Manager (ISSM) has oversight responsibility for the SOC. The ISSM reports to a separate division within OIT and has a direct reporting relationship to the OIT Assistant Commissioner for security issues.

Service Continuity

CBP concurs with KPMG's recommendations in this area. We will work to ensure that the Continuity of Operations Plan (COOP) is as current as possible, and that the alternate processing site has the hardware and support necessary to continue operations in the event of an emergency. POAMs have been developed for the NFRs included in Appendix B of this report. As part of our response, we have included the target completion dates for each NFR in Appendix B

Application Software Development and Change Control

CBP concurs with KPMG's recommendations in this area. Proper separation of roles between the development and production environments will be established. codes will be configured for the "Productive" setting. Configuration management and change control measures will continue to be upgraded for the program. POAMs have been developed for the NFRs included in Appendix B of this report. As part of our response, we have included the target completion dates for each NFR in Appendix B

If you have any questions concerning our comments, please contact Judy Wright, at 703 286-4155.

Attachment

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-01</p>	<p>A number of [redacted] Ids had a segregation of duties conflict.</p>	<p>Coordinate with each filed office that has a segregation of duties conflict to either (1) correct the problem by removing the conflicting roles, or (2) sign a waiver to accept responsibility for issues arising from the segregation of duties conflict. Continue to prevent new IDs with a segregation of duties conflict from being created.</p>	<p>Completed 7/25/05</p>	
<p>CBP-IT-05-02</p>	<p>Three [redacted] [redacted] [redacted] to specify security modes for individual users without a justified business need.</p> <p>Two [redacted] with [redacted] had full security administration privileges, which violated separation of duties principles.</p> <p>One SCA account had not been utilized since August 6, 2004.</p>	<p>Remove unnecessary privileges and/or accounts given the exceptions we noted related to the authorities/functions granted to certain [redacted].</p> <p>Accesses granted should be based on the least privilege concept to the minimum number of personnel with a defined and documented need.</p> <p>As an alternate means of providing availability to functions not used on a regular basis, continue implementation of a [redacted] [redacted] for use by authorized individuals during pre-determined circumstances. Establishment of a [redacted] [redacted] would enable the removal of privileges from individuals who do not regularly require such access. [redacted] are controlled through the use of a hardcopy log, secure storage of passwords, auditing of all [redacted] activities, and suspension after each use.</p>	<p>Completed 8/1/05</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-03</p>	<p>After the reorganization of the Office of Information Technology (OIT), security administration functions at the [redacted] including mainframe security, network securities, and incident response, were not independent of the operations functions. Rather, the Security Operations Center reported to Technology Operations, which was not an independent security function.</p>	<p>Ensure that security administration functions remain independent of operations. In order to maintain independence, the security administration function should not report to operations management.</p>	<p>CBP did not concur</p>	
<p>CBP-IT-05-04</p>	<p>Due to the design of [redacted] certain controls could be overridden without supervisory approval. Management plans to implement functionality in the [redacted] to prevent the override capability. KPMG noted that although [redacted] will eventually replace [redacted] would not be implemented in FY 2005.</p>	<p>Develop a process to mitigate the systemic [redacted]-weakness that certain controls can be overridden without supervisory approval. Considering the number of years necessary to fully replace [redacted]-functionality with [redacted] this process should be designed in a manner to ensure supervisory review of [redacted] overrides while maintaining a minimal burden on management. CBP should ensure that the new [redacted] system has the appropriate requirements for such controls and that these controls are applied prior to implementation.</p>	<p>Target completion date 7/31/08</p>	
<p>CBP-IT-05-05</p>	<p>Formal procedures for granting access to sensitive [redacted] technical team member roles have not been developed.</p>	<p>Formally establish a process for granting [redacted] access to sensitive technical team roles (e.g. basis and security team members) and consistently apply these processes. The procedures should include requirements for documenting the authorization request and include the exact roles that should be granted. Additionally, the procedures should require a periodic documented recertification of the user roles within [redacted]</p>	<p>Completed 12/1/05</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-06</p>	<p>The [redacted] contingency plan has not been updated with the results of the FY 2004 continuity of operations plan (COOP) tests. Additionally, the COP has not undergone the annual re-evaluation as required. Also, implementation of the new financial management system changed the mainframe environment to a client-server based [redacted] environment. However, the plan has not been updated and, therefore, might contain outdated and improper contingency procedures for information systems and data.</p>	<p>Update the [redacted] COOP with the most recent test results. Additionally, re-evaluate the COOP for overall contingency planning procedures on an annual basis, especially in the event of a major system change or upgrade, such as [redacted]</p>	<p>Completed 12/29/05</p>	
<p>CBP-IT-05-08</p>	<p>The requirement for initial security awareness training for employees and contractors was not consistently applied.</p>	<p>Consistently apply the requirements for initial security awareness training for all employees and contractors upon initially establishing LAN/mainframe accounts to information systems.</p>	<p>Target completion date 8/31/06</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-09</p>	<p>Improvements were still needed in security controls affecting [redacted] management and staff's system access to applications and data.</p>	<p>Coordinate with DHS in developing enterprise-wide solutions for improving network and host-based system configuration design(s) to reduce the risks of compromise.</p> <p>Consider use of system administrator-level security management monitoring tools to detect and correct security deficiencies in preventing possible intrusions. Use of such tools should include a planned "prioritized" schedule for checking all servers.</p> <p>Proceed with the implementation of [redacted].</p> <p>Provide and approve more robust standards for [redacted] for a standard and sustainable baseline set of system management security controls.</p> <p>Consider development of a compliance-level policy that provides for adherence to agency password management policies. This policy should be developed at [redacted] where local system administrators and help desk staff may apply such policies (e.g. changing password age, account lockout, password uniqueness, password length, etc.).</p> <p>For [redacted], review, justify, and ensure that the level of access is based on strict adherence to least privilege principles where the absolute minimum level necessary is applied. As CBP moves with DHS toward more</p>	<p>Target completion date 3/31/07</p>	<p>Two years ago CBP began an effort to upgrade our Novell Netware infrastructure from version 5.0 to version 6.5 in order to address the password recommendation and gain other improvements. More recently, CBP has initiated a project to convert to [redacted] in order to support DHS enterprise standards for network operating systems and desktop applications. This project will allow CBP to enforce strong passwords incrementally as [redacted] is deployed to individual sites. Discontinuing the Novell upgrade and putting our efforts into the [redacted] Active Directory deployment will allow CBP to comply with both the password recommendation and DHS standards sooner.</p>
---------------------	--	---	---------------------------------------	--

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

		technologically efficient enterprise-wide solutions (e.g. centralized means of managing network assets), the ability to reduce current levels will be enhanced.		
CBP-IT-05-10	[redacted] security audit log reviews were not evidenced for the majority of FY 2005.	Continue to review the audit logs daily and maintain documented evidence. Complete efforts to identify all connections with the [redacted] and formally establish ISAs with these entities.	Completed 5/31/05	
CBP-IT-05-11	[redacted] administrator staff has not documented ISAs for all entities that connect with the [redacted]. Although there was a [redacted] of all [redacted] of all partners that have an ISA with CBP, this database failed	Complete efforts to identify [redacted] connections that are considered "legacy" connections and formally establish ISAs with these entities. Complete efforts to identify all	Target completion date 6/1/06	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

	to capture all connections with [REDACTED]. The majority of financial institutions connected to [REDACTED] have not formally established ISAs.	connections with the [REDACTED] and formally establish ISAs with these entities.		
CBP-IT-05-12	The "equipment" and "priority of service" requirements have not been annually updated. As a result, the agreement was outdated and did not reflect the current operating environment at [REDACTED].	Formally update the alternate processing site agreement to accurately reflect the current hardware and support that will be required of the alternate processing site vendor in the event of an emergency.	Target completion date 3/31/06	
CBP-IT-05-13	Nor formal process exists to confirm or enforce compliance with the [REDACTED]. [REDACTED] Although field site administrators were trained to perform the recertifications every six months, there was no management oversight to ensure that the field site administrators were performing the recertifications.	Formalize the process to confirm or enforce compliance with the [REDACTED] at the field sites and formally document the verification of the field site [REDACTED].	Completed 9/12/05	
CBP-IT-05-14	Procedures have not been adequately implemented for restricting access to the data center located in [REDACTED]. Specifically, nineteen out of thirty-two individuals selected did not have proper authorizations documented for access to the data center.	Perform a formal review of all personnel who have access to the [REDACTED] to determine those who do not have a formal user access form in place. Establish a formally authorized user access form for each person identified. Confirm that current personnel with data center access actually need this access to perform their job functions. Promptly remove physical access rights to the [REDACTED] facility when an employee is terminated, thus restricting access to the data center.	Target completion date 3/31/07	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-15</p>	<p>[REDACTED] had access to the production environment.</p>	<p>Develop a formally documented process for granting normal and emergency access for [REDACTED] to the [REDACTED] production environment. The access request and authorization should include specific justification for their access and be documented and retained.</p>	<p>Completed 8/1/05</p>	
<p>CBP-IT-05-16</p>	<p>Improvements were still needed in CBP's Incident Handling and Response Capability. Specifically, issues still exist related to incident prevention, response, recovery, and reporting.</p> <p>[REDACTED]</p> <p>A formal automated reporting capability does not exist to report, in a timely manner, on the servers and workstations with identified vulnerabilities, the number that have been patched, and the number of servers that remain vulnerable.</p> <p>There is a process in place for tracking incidents. However, the weekly incident report process is not consistent and/or complete. Incidents were not included on requested weekly reports and incident documentation was missing. Sample information or evidence was not available for system flaw notifications.</p>	<p>Develop a process to identify the workstations that have yet to install the [REDACTED].</p> <p>Continue to test and implement a standard real-time automated reporting process whereby information can be generated on all incidents, response, and recovery activities on a regular basis for servers and workstations.</p> <p>Develop a consistent process to respond to system flaw notifications and track reported security incidents.</p>	<p>Target completion date to be determined</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-17</p>	<p>[redacted] was not configured to indicate a company code setting of "productive."</p>	<p>Perform a formal analysis of the company code setting to determine if it should be set to "productive." This will prevent users with "mass deletion/change" access the ability to accidentally or purposely delete transactional data.</p>	<p>Completed 10/31/05</p>	
<p>CBP-IT-05-18</p>	<p>An excessive number of users had access to sensitive [redacted] functions and high-risk combinations of functions.</p>	<p>Ensure that the assignment of sensitive functions and high-risk combinations of functions to non-supervisory users is based on a documented business need and approved by a supervisory official. Exceptions from the guidance provided in the memorandum should be formally approved and documented.</p>	<p>Target completion date 3/31/06</p>	
<p>CBP-IT-05-19</p>	<p>A number of separated employees' names appeared on the [redacted] active user access listing.</p>	<p>Determine whether the potential matches are actual matches. Delete the accounts of any confirmed terminated employees. Continue to use the payroll feed to determine if a [redacted] user has terminated employment. Disable user accounts of separated employees and contractors as stated in CBP and NIST guidance.</p>	<p>Completed 1/24/06</p>	
<p>CBP-IT-05-20</p>	<p>No process existed to formally document test plans, test cases, and test results for [redacted] security and configuration changes. The [redacted] Change Control Board was not performing formal business and-----omer impact analyses for [redacted] change requests.</p>	<p>Formally document test plans, test cases, and test results for all [redacted] changes. Formally document business and customer impact analyses for [redacted] change requests.</p>	<p>Completed 1/24/06</p>	
<p>CBP-IT-05-21</p>	<p>Logging of critical tables with [redacted] has not been activated. A formal analysis of the tables that should be logged in the [redacted] environment has not been performed, solely</p>	<p>Perform a formally documented assessment of the tables that should be logged by [redacted]. Complete the implementation of table logging within [redacted]</p>	<p>Completed 1/25/06</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

	relying on recommendations of a previous audit.			
CBP-IT-05-22	A certification and accreditation package for all components of the [redacted] LAN has not been completed. Specifically, a security control assessment was not conducted for the [redacted] LAN as a whole within the last year. Also, a formal risk assessment was not conducted for all [redacted] LAN components.	Complete a security control assessment for all [redacted] LAN components and complete a risk assessment for all [redacted] LAN components.	Target completion date 7/1/06	
CBP-IT-05-23	NIST 800-26 assessments for the seven business areas with the seven Administrative Applications have not been completed. No efforts have been made to evaluate the need for a separate C&A for the applications remaining in the seven business process areas defined in the Administrative Applications C&A. Also, additional improvements in consolidated guidance were necessary to address the issue of linking risks/threats to requirements.	Using federal guidelines outlining what constitutes a major application, consider reviewing the sensitivity of applications classified as part of the [redacted] administrative systems separately to determine which applications warrant individual C&As as major applications, and which applications should remain as part of the current Administrative C&A process. Based on results of the sensitivity review, perform separate C&As, where appropriate. In accepting risks associated with [redacted] consider establishing a relationship of identifying risks to defined security requirements in [redacted]. This will assist in understanding what risks are mitigated by existing controls and what residual risks remain that management is willing to accept. Given that the [redacted] deployment may not be completed by the end of the current [redacted] certification period, incorporate a	Completed 8/15/05	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

		<p>risk-based approach for any recertification efforts performed, where threats identified are tied to security requirements and mitigating controls.</p> <p>Consider development of definitive guidance for risk assessments and security plan criteria. These criteria should be applied to tie identified risks and threats to security requirements and controls that mitigate risks to acceptable levels. This will allow for the adequate tracking and evaluation of risks and requirements throughout a systems lifecycle. Therefore, management should be able to definitely recognize what acceptable risks remain.</p>		
<p>CBP-IT-05-24</p>	<p>A centralized listing of separated contract personnel was not maintained. The only method employed to track terminated contractors was the use of a report of users that had their mainframe account deleted. This list was not representative of all terminated contractors since terminated contract personnel might not have had mainframe access or their access might not have been removed after their termination.</p>	<p>Develop a formal centralized process for tracking the termination of contract personnel.</p> <p>Deactivate all system access for terminated contractors immediately upon separation.</p> <p>Periodically distribute a listing of terminated contract personnel to information system administrators so they remove user access and periodically assess contractor access to systems.</p>	<p>Target completion date 3/31/07</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

<p>CBP-IT-05-25</p>	<p>The mainframe disconnected idle sessions after 30 minutes of inactivity rather than the prescribed 20 minutes of inactivity noted in the U.S. Customs and Border Protection Information Systems Security Policies and Procedures Handbook.</p>	<p>Modify the setting on [redacted] to disconnect idle sessions as specified by agency policy or ensure the policy is accurate. (Note: [redacted])</p>	<p>Completed 9/29/05</p>	
<p>CBP-IT-05-26</p>	<p>[redacted] did not have an automated mechanism to detect and deactivate users that had not logged on for 90 days. Procedures to perform a monthly review for inactive accounts in July 2005 were implemented. However, for the majority of FY 2005, this procedure was not in place.</p>	<p>Continue to review and deactivate inactive accounts on a monthly basis. Implement an automated mechanism to detect and deactivate inactive accounts.</p>	<p>Target completion date 5/31/06</p>	
<p>CBP-IT-05-27</p>	<p>The formal process to grant VPN access using an authorization form was recently implemented. However, VPN access authorization forms were not available for the majority of employees selected. Also, VPN employee accounts were not periodically recertified.</p>	<p>Continue to use the official authorization form for new VPN users. Recertify all VPN employee accounts on a periodic basis and document results.</p>	<p>Target completion date to be determined</p>	
<p>CBP-IT-05-28</p>	<p>Action has not yet been taken to address the prior-year issue that users with access to [redacted] may be excessive.</p>	<p>Recertify users with access [redacted] and document the evidence of the recertification.</p>	<p>Completed 11/1/05</p>	
<p>CBP-IT-05-29</p>	<p>In FY 2004, issues with access to [redacted] were reported. Some profiles with access to modify the [redacted] represented a segregation of duties conflict. In FY 2005, [redacted] was replaced by [redacted] KPMG attempted to determine whether the same issue</p>	<p>Document that access to the [redacted] (or equivalent) is properly segregated. This includes a review of [redacted] access to determine if the current granted access is appropriate.</p>	<p>Completed 8/30/05</p>	

Department of Homeland Security
Information Technology Management Letter
 September 30, 2005

	<p>existed in [redacted] Information regarding whether-[redacted] (or equivalent) were appropriately segregated could not be provided.</p>			
CBP-IT-05-30	<p>Action has not been taken to address the prior-year finding that that number of users with access to [redacted], Recovery, and Backup datasets may be excessive.</p>	<p>Recertify users with access to [redacted] Recovery, and Backup datasets. Document the evidence of the recertification.</p>	Completed 8/11/05	
CBP-IT-05-31	<p>As part of the Common Local Area Network (LAN) Operating Environment (CLOE) type accreditation to perform formal risk assessment, [redacted] LANs dispersed across many field sites were not to be visited. As a result, management asserted that they were requiring each field site on the "non-recommended" listing to submit a formal NIST 800-26 assessment for their LAN. Based on this, a sample of 15 field sites was selected from the non-recommended field site listing and we requested evidence of the NIST 800-26 review of their LAN. In a sample of 15 field sites, three site assessments were not provided.</p>	<p>Continue to develop a formal process to ensure that all non-recommended field sites submit a NIST 800-26 LAN self-assessment in a timely manner.</p>	Completed 9/9/05	

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Executive Secretariat
Under Secretary, Management
Commissioner, CBP
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Information Officer, CBP
Assistant Secretary, DHS Public Affairs
Assistant Secretary, DHS Policy
DHS Audit Liaison
Chief Information Officer Audit Liaison
CBP 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, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, 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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.