DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Additional Controls Can Enhance the Security of the Automated Commercial Environment System (Redacted)

NOTICE: The Department of Homeland Security, Office of Inspector General (OIG), has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.

OIG-08-64

June 2008

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 4, 2008

Preface

The Department of Homeland Security, Office of Inspector General, 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 addresses the strengths and weaknesses of the U.S. Customs and Border Protection's Automated Commercial Environment System. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, technical scans, and a review of applicable documents.

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. 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

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ACE	Automated Commercial Environment
C&A	Certification and Accreditation
CBP	U. S. Customs and Border Protection
COTS	Commercial-off-the-shelf
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
e-Manifest	ACE Truck Manifest System
ESM	Enterprise Systems Management
FISMA	Federal Information Security Management Act
ISSO	Information Systems Security Officer
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
SAT	Security Acceptance Testing
SCOs	Field Security Control Officers
SP2	Service Pack 2

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

The Automated Commercial Environment (ACE) is the commercial trade processing system that is being developed by U.S. Customs and Border Protection (CBP) to facilitate legitimate trade while strengthening border security. The system is part of a multi-year CBP modernization effort and is being deployed in releases.

We evaluated the system to determine whether the Department of Homeland Security (DHS) had implemented adequate and effective security controls over ACE to ensure the efficient collection, processing, and analysis of commercial import and export data. We determined whether adequate controls had been implemented to protect sensitive data from unauthorized access, disclosure, modification or destruction; security acceptance testing was performed when new technologies, system interfaces, or increments were deployed; and the system was complying with Federal Information Security Management Act (FISMA) requirements.

Generally, CBP has made good progress in implementing controls to protect the information stored and processed on ACE. For example, CBP certified and accredited ACE in August 2007. A change control process has been established to ensure that system and software changes are reviewed, authorized, and tested prior to being implemented on ACE. Additionally, CBP has implemented adequate physical controls to restrict access to the system to authorized users. Furthermore, CBP completed a privacy impact assessment to outline what type of information is being collected, the intended use of the information, and with whom the information collected will be shared. Finally, the system is generally in compliance with FISMA requirements.

Even with these controls in place, more effort is needed by CBP to improve the security posture of ACE. Specifically, weaknesses were found in security acceptance testing during the system development process; user account management process; [redacted]. Further, security

vulnerabilities were discovered as a result of ineffective patch management and inconsistent implementation of the DHS Security Baseline Configuration on selected servers. These security related issues could compromise the confidentiality, integrity, and availability of the information processed by the system if they are not remediated.

We are making four recommendations to the Commissioner, to direct the Chief Information Officer, to improve the areas of management, operational and technical controls. CBP concurred with our recommendations. The component's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

CBP protects our nation's borders from terrorism, human and drug smuggling, illegal migration, and agricultural pests while simultaneously facilitating the flow of legitimate travel and trade. CBP is developing ACE as its commercial trade processing system to facilitate legitimate trade while strengthening border security. The initial work on the design and development of ACE began in August 2001. When fully implemented, ACE will:

- Allow trade participants access to and management of their trade information;
- Expedite legitimate trade by providing CBP with tools to efficiently process imports/exports and move goods quickly across the border;
- Improve communication, collaboration, and compliance efforts between CBP and the trade community;
- Facilitate efficient collection, processing, and analysis of commercial import and export data; and
- Provide an information-sharing platform for trade data throughout government agencies.

On August 6, 2002, Congress enacted the *Trade Act of 2002* (P.L. 107-210), which requires CBP to establish a safe and secure system of aviation, maritime, and surface transportation of cargo for import into and export out of the United States. In addition, the legislation requires CBP to establish an advanced electronic system for all truck carriers to submit manifests detailing shipment, carrier, and other information necessary to enter the United States. The ACE Truck Manifest System (also known as "e-Manifest") is CBP's approved electronic data interchange for the transmission of required electronic cargo information. The e-Manifest helps create a secure and streamlined environment for processing cargo at the land borders.

In June 2003, 41 importers established accounts during the initial deployment of ACE. In October 2003, the ACE Secure Data Portal was introduced. Currently, any importer or broker doing business with CBP is required to open an ACE Portal Account. The creation of ACE Portal Accounts provides the trade community and CBP with a consolidated approach for tracking import activity. The ACE Portal has three major user categories: (1) CBP, (2) trade community, and (3) participating government agencies.

ACE is being developed and implemented in a series of releases, each of which builds on the functionality of the prior release. Future releases will include account enhancements and reference data, as well as new business process functionality. Also scheduled for the future are Cargo Control and Release functions for all modes of transportation. See Appendix C for a brief description of each release.

[redacted]

As of December 2007, nearly 14,000 ACE portal accounts have been established, including more than 1,300 importer accounts, nearly 800 broker accounts, and nearly 11,800 carrier accounts. More than $14 billion in duties and fees have been collected via ACE since the first payment was made in July 2004. The budget for ACE in fiscal year 2007 was approximately $300 million.

Results of Audit

CBP Has Taken Actions to Secure ACE

CBP has taken various actions to secure ACE. These measures are designed to reduce the risks associated with the intentional and unintentional actions of system users that could potentially result in the loss and misuse of the data processed and stored by the system. For example, CBP has:

- Certified and accredited ACE in August 2007. Our review of ACE certification and accreditation package revealed no significant deficiencies. Generally, we found ACE is in compliance with FISMA requirements.
- Enabled point-to-point encryption to protect the data transmitted through the ACE Portal from unauthorized access.
- Established an interconnection security agreement with an external agency. The agreement stipulates the responsibilities between both agencies and the safeguards implemented to protect the transmission of information shared between the systems connected.
- Established a change control process to ensure that system and software configuration changes are reviewed, authorized, and tested prior to being implemented on the system.
- Completed an assessment to ensure that ACE use is consistent with applicable privacy policy. The privacy assessment outlines what type of information is to be collected, why the information is being collected, the intended use of the information, and with whom the information collected will be shared.
- Implemented adequate physical controls to restrict access to the system to authorized personnel and reduce the potential risks of theft, destruction, sabotage, or compromise of equipment.
- Implemented procedures to ensure that ACE sensitive data are backed up periodically and can be restored at an alternate recovery location in the event of emergency.

Generally, the implementation of these measures reduces the potential risks of unauthorized access to the system. However, as discussed in the following sections, CBP can make further improvements to the security posture of ACE.

Security Acceptance Testing Must Be Performed During System Development

CBP did not perform adequate security acceptance testing (SAT) to assess the potential impact to the overall security of the system before ACE drop A1 was implemented. Specifically, the developer did not perform security acceptance testing in accordance with the terms stated in the task order to ensure that implemented controls are not weakened as a result of the changes introduced by the new release. As a result, an increased risk exists for individuals to exploit potential new vulnerabilities in order to gain unauthorized access to the system.

Security acceptance testing is a method of determining if the system being developed provides adequate and effective controls to protect information processed and stored. During this phase, independent testing is conducted to ensure that the controls implemented are effective and working to protect the system being developed.

Consideration of security in the system development lifecycle is essential to implementing and integrating a comprehensive strategy for managing risk for all information technology assets in an organization. To accomplish this, security must be made an integral part of the testing performed as new features and functionality are introduced into a system. Certification and Accreditation (C&A) on the other hand is a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Both security acceptance testing and C&A play specific and unique roles in providing and ensuring information system security.

CBP uses the system C&A process to determine whether ACE security requirements are being met. CBP did not perform security testing while the ACE system was under development and upon acceptance of each new release. Our review of the security acceptance testing report prepared for ACE drop A1 revealed that only a functional demonstration was performed during the system's development to confirm the following security related features:

- ACE shall provide authorized users with add, delete, change, and query capabilities.
- Records of changes to import transaction data shall indicate new and old data.
- Retrieving data shall be available based on user ID, transaction, account number, entry number, time, date, and function delimiters.

According to the task order, the developer is required to perform specialized and selective security testing of the commercial-off-the-shelf (COTS) products to verify that key security controls are present and working, and to identify any configuration errors that may constitute valid concerns. Specifically, the developer is required to identify active accounts for any users that have left the program; default passwords for COTS products, monitor super users' account activities (i.e. "root"); and ensure that unnecessary ports and services are disabled. These security tests were not performed.

According to the ACE Information Systems Security Officer (ISSO), to satisfy security-testing requirements, a vulnerability assessment was performed in April 2007 on ACE to identify missing security patches and configuration weaknesses. CBP's testing did not reveal that: (1) some security patches that were issued between 2004 and 2006 were missing, and (2) there existed configuration problems that could potentially allow unauthorized users to read, copy, change, and modify data on Unix servers. These weaknesses were identified from the vulnerability assessment that we performed on the ACE system during the audit.

DHS requires that information security be best managed if it is planned for throughout the IT system life cycle. In addition, National Institute of Standards and Technology (NIST) recommends that, to be most effective, information security must be integrated into the system development life cycle from its inception. Security acceptance testing of the security properties of the contractor-developed system is a prerequisite to security testing as part of the certification and accreditation process. Determination of the efficacy of these organization-implemented security controls is part of C&A testing. The purpose of the certification and accreditation process is to confirm the assumptions that security controls implemented are adequate and effective to reduce the residual risks to an acceptable level.

Since CBP is developing ACE with more than 150 COTS products, performing security acceptance testing to ensure that no new vulnerability is introduced to the system with each release becomes more critical. Without comprehensive tests and evaluations of security controls, CBP has limited assurance that controls implemented on ACE are working as intended or not weakened as a result of introducing changes to the system with the new releases. Security acceptance testing can lead to the discovery of potential vulnerabilities and reduces the likelihood of systems being compromised. The security controls developed for each ACE release must be tested and evaluated prior to deployment to ensure that they are working as intended and effective.

Recommendation

We recommend that the Commissioner, U.S. Customs and Border Protection, direct the Chief Information Officer to:

Recommendation #1: Develop, update, and implement policies and procedures to ensure that security acceptance testing is performed on ACE to assess the potential impact to the overall security posture of the system before the new release is put in production.

Management Comments and OIG Analysis

CBP concurred with recommendation 1. CBP has recently implemented a new policy requiring that an independent security testing and evaluation be performed during SAT before any projects are moved into a production environment. In addition, a large number security regression tests are being added to the Quality Center tool to strengthen the security testing during SAT. CBP expects to complete this action by July 11, 2008.

We agree that the steps CBP is taking, and plans to take, begin to satisfy this recommendation.

Improvements in Technical Controls Can Reduce Vulnerabilities

To assess the security posture of ACE, we interviewed information technology and contractor personnel at CBP’s National Data Center and contractor’s facility. In addition, we performed vulnerability assessments using (1) NESSUS on selected servers, (2) AppSecInc's Application Detective on IBM DB2 database servers, (3) Fluke Handheld Wireless Scanner to detect unauthorized wireless access points, (4) Center for Internet Security's Router Auditing Tool; and (5) WebInspect application vulnerability scanner on ACE Web Portal. Finally, we reviewed configuration settings on selected Unix and Windows servers for compliance with applicable DHS and Defense Information Systems Agency's checklists.

Overall, CBP has implemented adequate security controls over ACE. However, in assessing the effectiveness of controls implemented, we identified vulnerabilities in patch management, which could be used to exploit and gain inappropriate access to the information stored and processed by the system. In addition, we identified weaknesses in security configuration settings, [redacted] Without eliminating these weaknesses, CBP cannot ensure that only legitimate users can access the system.

Patch Management Process Is Not Effective

While a patch management process has been established for ACE, our scan results revealed that the process needs improvement.[1] For example, we identified the following system vulnerabilities, which are due to

[redacted]

[redacted]

[1] Patch management, which is a component of configuration management, is a critical process used to mitigate security vulnerabilities that have been identified.

[redacted]

[redacted] [redacted]

DHS requires security patches be installed in a timely and expeditious manner. NIST also recommends that agencies have an explicit and documented patching and vulnerability policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches. The policy should specify what techniques an agency will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring.

Without an effective patch management process for ACE, CBP cannot ensure that all security vulnerabilities have been mitigated before malicious users exploit these vulnerabilities to gain uncontrolled access to the sensitive information collected and processed by the system. Applying security patches is critical for securing ACE and protecting sensitive data from unauthorized access, manipulation, and misuse.

DHS Security Baseline Configurations Have Not Been Implemented

CBP has not completely configured [redacted] based on DHS configuration guidelines. The results of our vulnerability assessment indicate that the configuration settings applied on ACE do not effectively ensure that the system is securely configured. Specifically:

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

DHS has developed configuration guidelines, which are a set of procedures to ensure a minimum baseline of security when installing or configuring network devices, such as Windows 2000/2003/XP/Vista/Active Directory, Solaris, Unix, Linux, and Cisco routers. Components are required to ensure that the installation of hardware and software products meets the requirements specified in applicable DHS secure baseline configuration guides. NIST also recommends that agencies develop standardized configurations to reduce the labor involved in identifying, testing, and applying security patches.

[redacted]

[redacted]

[2] A virus is a self-replicating malicious program segment that attaches itself to legitimate applications, programs, operating system commands, or other executable system components and spreads from one system to another. Antivirus signature is the binary pattern of the machine code of a particular virus. As new viruses are discovered by the antivirus vendor, their binary patterns are added to a signature database that allows users to download and update their antivirus programs regularly. Antivirus programs compare their database of virus signatures with the files on the hard disk and removable media for known computer viruses.

[redacted]

[redacted]

[redacted]

[redacted]

Audit trails can track the identity of each user attempting to access the network device, the time and date of access, and time of log off. In addition, audit trails can capture all activities performed during a session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards.

[redacted]

[redacted]

Recommendation

We recommend that the Commissioner, U.S. Customs and Border Protection, direct the Chief Information Officer to:

Recommendation #2: Establish a process to ensure that critical patches and service packs are tested and applied timely to ACE, DHS Security Baseline Configurations are implemented on the system, [redacted]

Management Comments and OIG Analysis

CBP concurred with recommendation 2. CBP's Cargo Systems Program Office will establish processes to address the deficiencies identified. CBP expects to complete this action by September 8, 2008.

We agree that the steps CBP is taking, and plans to take, begin to satisfy this recommendation.

User Account Management Process Needs Strengthening

CBP does not have an effective user account management process to ensure that only authorized users are granted access to the information stored and processed by ACE. As a result, there is greater risk that security controls implemented to protect ACE may be circumvented. For example, CBP does not have a documented process to grant system access to users located at the ports of entry. Furthermore, an excessive number of users have been granted administrator privileges, which grants that user the ability to modify configuration settings on Unix servers. In addition, CBP does not always follow DHS' policy when granting users system access. Finally, CBP does not have a formalized process to review and disable inactive accounts periodically.

<u>Documented Process Has Not Been Established to Grant System Access at the Ports of Entry</u>

CBP does not have a documented or formalized user account management process for granting, monitoring, and disabling system access for users at the ports of entry. Specifically, access authorization requests are not prepared, reviewed, and approved before granting system access to these users. At the various ports of entry, system access is administered by Field Security Control Officers (SCOs) who have been assigned the responsibility to add or delete users and who also assign various system accesses based on the users job roles and responsibilities. As a result, the access permissions granted to users can be varied among different ports. Finally, the ACE system owner or designated staff does not approve user access requests or review their permissions periodically to ensure they remain proper.

We interviewed three Field SCOs at Andrade California; Vanceboro, Maine; and Laredo, Texas, to determine their process for granting users system access. According to the Field SCOs, access request forms are not used at the ports of Vanceboro, ME; and Laredo, TX. User access privileges vary at the ports as they are granted at the discretion of Field SCOs. For example, the port of Andrade, California, does not process cargo and therefore users do not require ACE to perform their job responsibilities. However, CBP personnel at that location were granted system access to ACE. Further, their accounts have not been suspended even after one year of inactivity.

DHS requires the system owner or designated representative to ensure that (1) users have a valid requirement to access its systems, and (2) user access privileges are approved and reviewed periodically. NIST requires agencies develop an account management process that identifies authorized users of the information system and specifies access rights or privileges. The process should define the (1) requesting, establishing, issuing, and closing of user accounts; and (2) tracking users to their respective access authorizations. Periodic reviews should be conducted to examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, and whether management authorizations are up to date.

The ACE ISSO acknowledged that CBP does not have a uniform process to grant system access to users at ports of entry. After discussion with CBP management officials, we were informed that the Program Office will initiate actions with the Office of Field Operations to develop and document a formalized process to grant user access at the ports of entry.

Excessive Number of Users with Administrator Privileges

CBP does not restrict the number of users with administrator access to ACE. Specifically, a total of 137 users have been granted "Super User" (i.e., "root") administrator roles on ACE Unix servers. This privilege allows the users the capability to bypass security features and have unmonitored access to modify system configuration settings and data. We identified similar findings on different CBP systems in prior OIG audits.[3] The ACE ISSO indicated that the "Unix Super User" role has been given to a large number of individuals having expertise with various software products in order to support ACE's deployment, correct problems, add enhancements, and perform troubleshooting during an outage.

Elevated account access, such as that granted to system administrators, is only appropriate for a limited number of users. Restricting the number of users with administrator access can limit the damage that can result from accident, error, or unauthorized use.

Process to Monitor and Disable Inactive Users Has Not Been Established

CBP does not have a formal process to ensure that inactive user accounts are disabled periodically. We requested a list of CBP ACE users to evaluate the current status and determined whether inactive user accounts had been disabled. Our analysis identified 2,450 user accounts that have not been disabled after more than 45 days of inactivity.

[redacted]

[3] OIG-06-41, *Information Technology Management Letter for the FY 2005 Customs and Border Protection Balance Sheet Audit*, dated June 2006.

DHS requires components to disable user accounts after 30 days of inactivity for systems with a high impact in the confidentiality security objective, such as ACE. Further, NIST requires periodic reviews of user access to ensure that unnecessary accounts are removed or disabled.

As user access privileges may change over time, it is imperative that reviews are conducted periodically to disable inactive accounts. [redacted]

<u>Non-U.S. Citizens with Administrator Access to ACE</u>

CBP has granted 34 non-U.S. citizens administrator access to ACE without obtaining an “Exception to Citizenship Requirement” waiver. These waivers need to be approved by the DHS Office of Security prior to granting system access.

Dating back to 2004, CBP granted a number of administrators system access to ACE who were non-U.S. citizens. At that time, no waivers for exception were submitted. CBP did not begin submitting waiver requests for these administrators until November 2007. While most of these administrators are either eligible or in the process of applying for U.S. citizenship, five of these administrators are not eligible and not planning to apply.

DHS policy stipulates that system access can only be granted to government and contractor personnel when (1) the individual is a legal permanent resident of the United States or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State, (2) any necessary background check have been satisfactorily completed, (3) a compelling reason exists for using this individual instead of a U.S. citizen, (4) the exception to the U.S. citizenship requirement is in the best interest of the U.S. Government, and (5) the DHS Chief Security Officer and the Chief Information Officer or their designees concur in approving access for the individual.

ACE system security is important particularly considering CBP’s vital mission to the country. Correcting the above weaknesses can help further strengthen system security and provide additional assurance to CBP that unauthorized users are not circumventing security controls implemented to have unmonitored access to the ACE system. When an account management process has not been established, access authorizations may be left to personnel who are not authorized or in the best position to determine users' access needs. Such personnel may give users privileges that are not necessary in carrying out their job responsibilities, defeating the purpose of access controls. Depending on the sensitivity of the resources involved, a user may then have the opportunity to gain unauthorized access to sensitive information. When elevated account access is not administered effectively, there is an increased risk that unauthorized activities and erroneous actions will go undetected.

These weaknesses are an indication that ACE user account management process may not be effective to control access to CBP sensitive data. To protect against threats involving potential misuse, it is imperative that CBP management establish a documented process to grant users system access, and actively monitor and disable accounts periodically.

Recommendations

We recommend that the Commissioner, U.S. Customs and Border Protection, direct the Chief Information Officer to:

Recommendation #3: Develop, update, and implement policies and procedures to ensure that a formalized user account management process for ACE is established to grant, monitor, and disable user access at ports of entry. The process established should be in compliance with applicable DHS policies. In addition, the system owner or designated staff should approve user access requests and disable inactive accounts.

Recommendation #4: Evaluate the need for users with administrator access to ACE. When appropriate, system administrator access should be restricted to a limited number of users to minimize the potential of misuse.

Management Comments and OIG Analysis

CBP concurred with recommendation 3. CBP will develop, update, and implement policies and procedures to ensure that a formalized user account management process for ACE is established to grant, monitor, and disable user access at ports of entry. The process established will be in compliance with applicable DHS policies. In addition, the system owner or designated staff should approve user access requests and disable inactive accounts periodically. CBP expects to complete this action by November 30, 2008.

We agree that the steps CBP is taking, and plans to take, begin to satisfy this recommendation.

CBP concurred with recommendation 4. CBP's Cargo Systems Program Office will improve the current process for granting administrator access and review current administrator access privilege. CBP expects to complete this action by November 30, 2008.

We agree that the steps CBP is taking, and plans to take, begin to satisfy this recommendation.

Appendix A
Purpose, Scope and Methodology

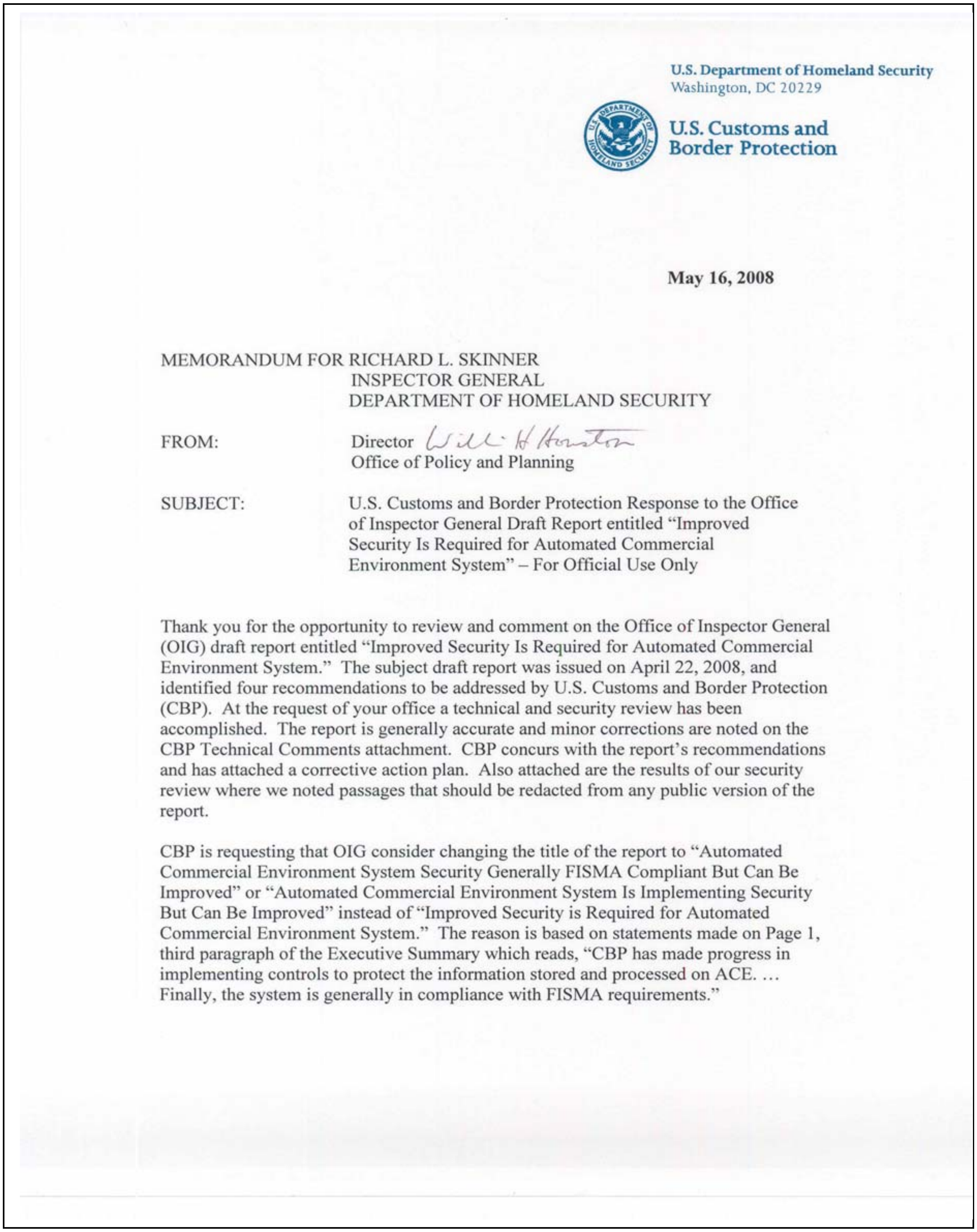
Our objective was to determine whether CBP had implemented adequate controls over ACE to ensure the efficient collection, processing, and analysis of commercial import and export data. Specifically, we determined whether (1) adequate controls had been implemented to protect sensitive data from unauthorized access, use, disclosure, disruption, modification or destruction, (2) security acceptance testing was performed when new technologies, system interfaces, or increments are deployed on the system, and (3) ACE was in compliance with FISMA requirements.

To accomplish our audit, we interviewed personnel at CBP National Data Center and contractor's facility. In addition, we reviewed and evaluated DHS and CBP security policies, procedures, and other appropriate documentation. During the audit, we used software tools, such as NESSUS, Application Detective, and WebInspect to detect, analyze, and evaluate the effectiveness of controls implemented on selected servers, workstations, network printers, switches, and web application. Upon completion of the assessments, we provided CBP the technical reports detailing the specific vulnerabilities detected on their network devices and the actions needed for remediation.

We conducted our audit between October 2007 and February 2008 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix E.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General, Office of Information Technology at (202) 254-4100; and Edward G. Coleman, Director, Information Security Audits Division at (202) 254-5444.

Appendix B
Management Comments to the Draft Report



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

U.S. Customs and
Border Protection

May 16, 2008

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

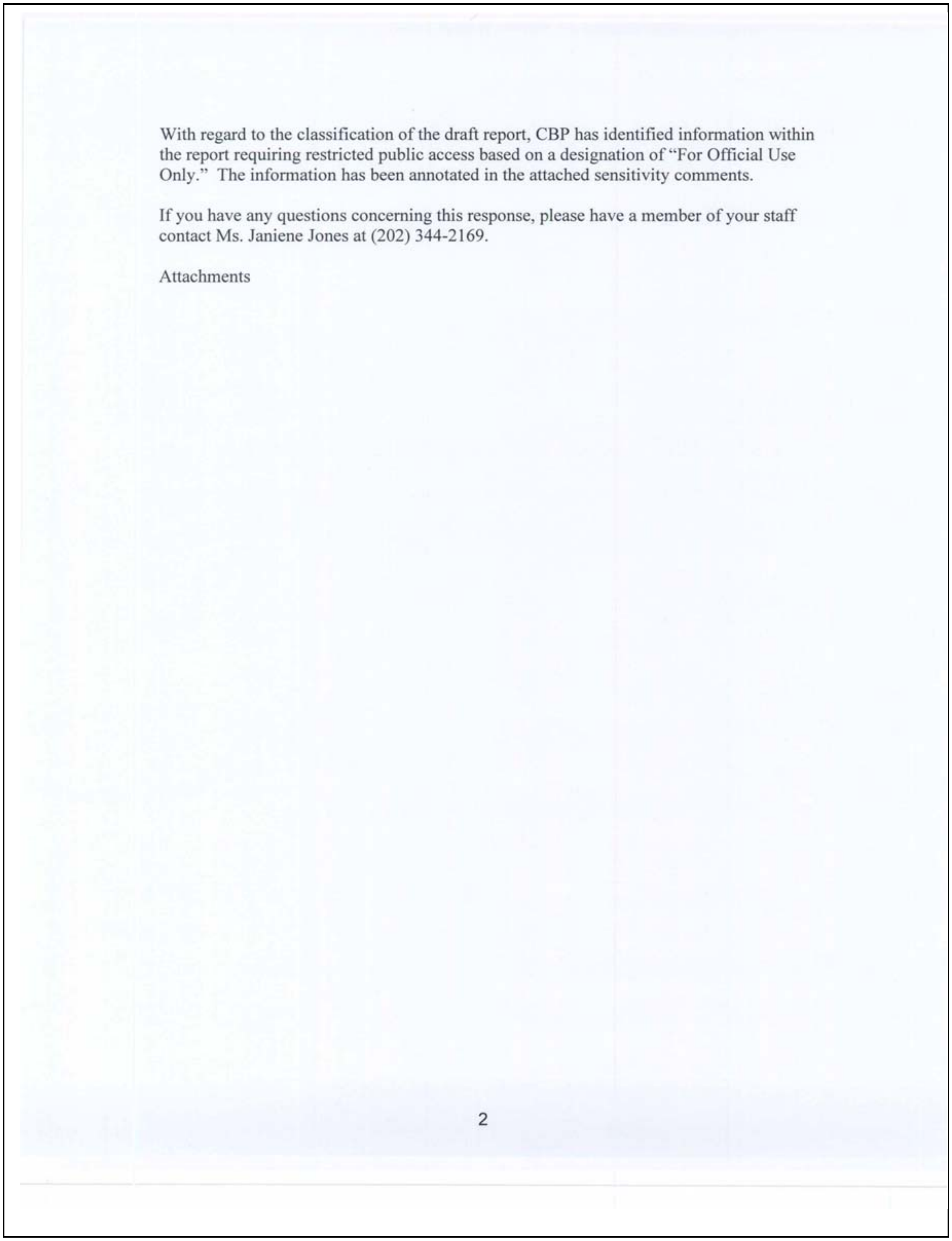
FROM: Director Willie H Houston
Office of Policy and Planning

SUBJECT: U.S. Customs and Border Protection Response to the Office of Inspector General Draft Report entitled "Improved Security Is Required for Automated Commercial Environment System" – For Official Use Only

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled "Improved Security Is Required for Automated Commercial Environment System." The subject draft report was issued on April 22, 2008, and identified four recommendations to be addressed by U.S. Customs and Border Protection (CBP). At the request of your office a technical and security review has been accomplished. The report is generally accurate and minor corrections are noted on the CBP Technical Comments attachment. CBP concurs with the report's recommendations and has attached a corrective action plan. Also attached are the results of our security review where we noted passages that should be redacted from any public version of the report.

CBP is requesting that OIG consider changing the title of the report to "Automated Commercial Environment System Security Generally FISMA Compliant But Can Be Improved" or "Automated Commercial Environment System Is Implementing Security But Can Be Improved" instead of "Improved Security is Required for Automated Commercial Environment System." The reason is based on statements made on Page 1, third paragraph of the Executive Summary which reads, "CBP has made progress in implementing controls to protect the information stored and processed on ACE. … Finally, the system is generally in compliance with FISMA requirements."

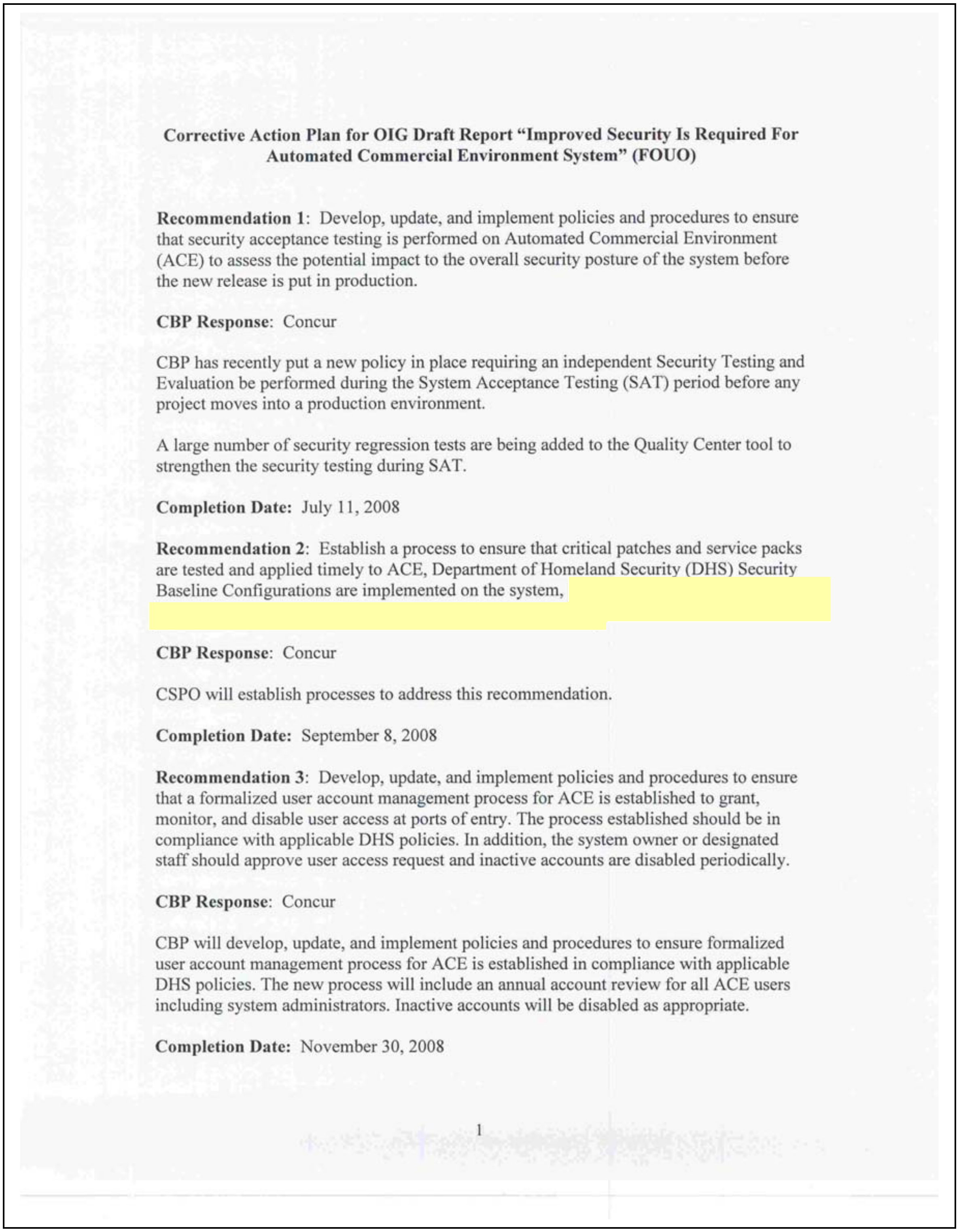
Appendix B
Management Comments to the Draft Report



With regard to the classification of the draft report, CBP has identified information within the report requiring restricted public access based on a designation of "For Official Use Only." The information has been annotated in the attached sensitivity comments.

If you have any questions concerning this response, please have a member of your staff contact Ms. Janiene Jones at (202) 344-2169.

Attachments



Corrective Action Plan for OIG Draft Report "Improved Security Is Required For Automated Commercial Environment System" (FOUO)

Recommendation 1: Develop, update, and implement policies and procedures to ensure that security acceptance testing is performed on Automated Commercial Environment (ACE) to assess the potential impact to the overall security posture of the system before the new release is put in production.

CBP Response: Concur

CBP has recently put a new policy in place requiring an independent Security Testing and Evaluation be performed during the System Acceptance Testing (SAT) period before any project moves into a production environment.

A large number of security regression tests are being added to the Quality Center tool to strengthen the security testing during SAT.

Completion Date: July 11, 2008

Recommendation 2: Establish a process to ensure that critical patches and service packs are tested and applied timely to ACE, Department of Homeland Security (DHS) Security Baseline Configurations are implemented on the system, [redacted]

CBP Response: Concur

CSPO will establish processes to address this recommendation.

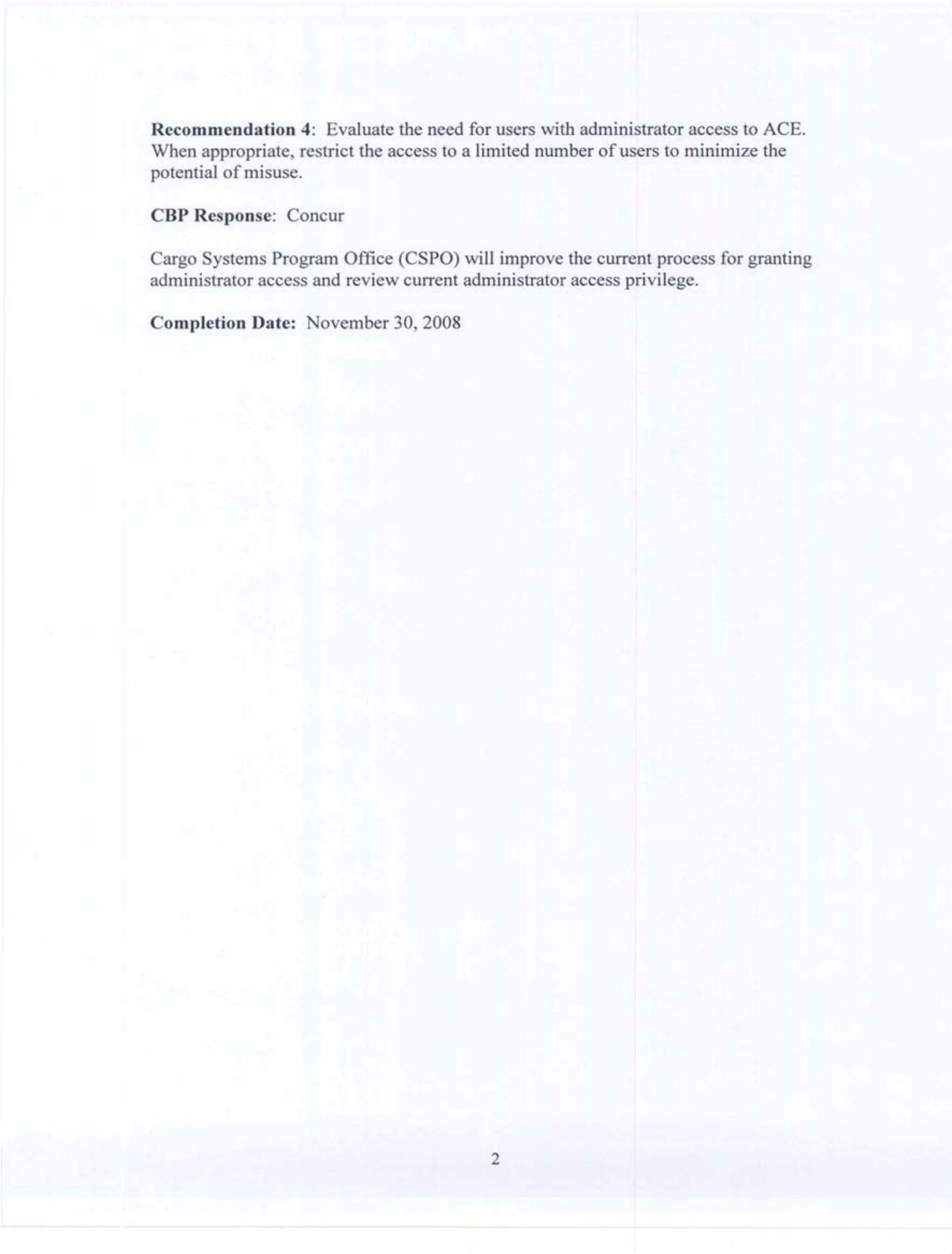
Completion Date: September 8, 2008

Recommendation 3: Develop, update, and implement policies and procedures to ensure that a formalized user account management process for ACE is established to grant, monitor, and disable user access at ports of entry. The process established should be in compliance with applicable DHS policies. In addition, the system owner or designated staff should approve user access request and inactive accounts are disabled periodically.

CBP Response: Concur

CBP will develop, update, and implement policies and procedures to ensure formalized user account management process for ACE is established in compliance with applicable DHS policies. The new process will include an annual account review for all ACE users including system administrators. Inactive accounts will be disabled as appropriate.

Completion Date: November 30, 2008



Recommendation 4: Evaluate the need for users with administrator access to ACE. When appropriate, restrict the access to a limited number of users to minimize the potential of misuse.

CBP Response: Concur

Cargo Systems Program Office (CSPO) will improve the current process for granting administrator access and review current administrator access privilege.

Completion Date: November 30, 2008

2

Appendix C
Description of ACE System Releases

- **ACE Foundation (Release 1):** Provided the first infrastructure investment for the ACE deployment platform and established security measures that are consistent across ACE. Began deploying in January 2003.
- **Account Creation (Release 2):** Provided Internet access via the ACE Secure Data Portal. This release delivered an importer account Web portal that facilitates collaboration and communication among the various groups and provides CBP account managers and selected importers (and authorized service providers) controlled access to information, such as the account trade activity. This release laid the initial foundation for an account management structure that will eventually encompass all segments of the trade community, and it will become a principal tool for CBP officers to assess national compliance and supply chain data. Implemented in October 2003.
- **Periodic Payment (Release 3):** Expanded the account management framework to a larger trade community audience, such as brokers and carriers, and the CBP officers overseeing those areas. Implemented in June 2004.
- **e-Manifest: Trucks (Release 4):** Provided an electronic truck manifest and a primary inspector interface and expedited import processing. Began deploying in October 2006.
- **Entry Summary, Accounts, and Revenue (Release 5):** Build upon ACE Releases 2, 3, and 4 by adding functionality to existing account management, periodic payment, ledger, and screening processing. In addition, impacted the trade community and participating government agencies associated with the admissibility process. Entry summary is a primary communication vehicle and data record between the trade community and CBP in the commercial importation process.
- **Cargo Control and Release (Release 6):** This release will establish the repository for Multi-Modal Manifest, and automate release processing and enhancing enforcement processes for the rail, sea, and air environments. It will provide services to support the conveyance entrance and clearances processes, and incorporate the Conveyance Management System and Release 4 into the ACE multi-modal capability. Currently in development and is scheduled to be in full operational capability by July 2010.
- **Export and Cargo Control (Release 7):** In this release, ACE will be in its full operational capability by August 2011.

Information Security Audits Division

Edward G. Coleman, Director
Jeff Arman, Audit Manager
Chiu-Tong Tsang, Audit Manager
Maria Rodriguez, Audit Team Leader
Swati Mahajan, IT Specialist
Amanda Strickler, IT Specialist

Sharell Matthews, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Commissioner, U.S. Customs and Border Protection
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight Program
Information Systems Security Manager, CBP
Director, GAO/OIG Liaison Office
Audit Liaision, CBP
Chief Information Officer Audit Liaison
Director, OIG Information Security Audits Division
ACE Audit Manager, OIG Information Security Audits Division

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) 254-4199, 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.