DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security (Redacted)

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

OIG-07-16 **December 2006**

Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

December 8, 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 prepared as part of our oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of U.S. Customs and Border Protection (CBP) laptop computer security controls. It is based on interviews with CBP officials, direct observations, technical tests, 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
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ATL	Advanced Technology Laboratory
BIOS	Basic Input Output System
C&A	Certification and Accreditation
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
DAA	Designated Accrediting Authority
DCOM	Distributed Component Object Model

Table of Contents/Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act of 2002
ICE	U.S. Immigration and Customs Enforcement
IP	Internet Protocol
ISSM	Information Systems Security Manager
IT	Information Technology
LPO	Local Property Officer
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of Inspector General
OMB	Office of Management and Budget
PED	Portable Electronic Device
POA&M	Plan of Action and Milestones
SANS	SysAdmin, Audit, Network, Security
SBU	Sensitive But Unclassified
SP	Special Publication
ST&E	Security Test and Evaluation
VACIS	Vehicle and Cargo Inspection System

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We audited the Department of Homeland Security (DHS) and its organizational components' security program to evaluate the security and integrity of select government-issued laptop computers. This report focuses on U.S. Customs and Border Protection (CBP). Our objective was to determine whether CBP has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to its government-issued laptop computers.

Significant work remains for CBP to further strengthen the configuration, patch, and inventory management controls necessary to protect its government-issued laptop computers. Specifically, CBP has not established: (1) a standard configuration for its laptops that meets required minimum-security settings; (2) effective procedures to patch laptop computers; and (3) adequate inventory management procedures. As a result, sensitive information stored and processed on CBP's laptop computers may not be protected adequately. Further, because CBP uses the same procedures to develop a model for its desktop computers, the configuration weaknesses identified with laptop computers are relevant to all government-issued computers assigned within CBP.

To secure CBP data stored on government-issued laptop computers, we are making seven recommendations to the Commissioner of CBP. CBP officials stated that they have already taken or plan to take corrective action to address the weaknesses we identified. As our fieldwork was complete, we did not verify that the weaknesses had been remedied. In addition, plans of action and milestones (POA&Ms) will be created and tracked for the vulnerabilities we identified. CBP's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

As the weight and price of laptops have decreased and their computing power and ease of use have increased, so has their popularity for use by government employees. DHS is heavily reliant on laptop computers for conducting business. The mobility of laptops has increased the productivity of the workforce, but at the same time increased the risk of theft, unauthorized data disclosure, and virus infection. Thefts of laptop computers occur regularly from offices, airports, automobiles, and hotel rooms, and the incidence of laptop thefts is increasing. According to the DHS Computer Security Incident Response Center (CSIRC), 12 security incidents involving stolen DHS laptops were reported in 2005, including government-issued laptops from CBP, United States Secret Service, U.S. Immigration and Customs Enforcement, and the Science and Technology Directorate.

Government organizations that provide for the use of laptop computers must take steps to ensure that the equipment and the information that is stored on them are adequately protected. Such steps may include ensuring secure storage of laptop computers when they are not in use, encrypting data files stored on laptops, installing adequate security software applications such as firewalls and anti-virus software, disabling and controlling built-in wireless, Bluetooth, and infrared connection capabilities, and regularly updating operating system and application software.

DHS Sensitive Systems Policy Directive 4300A and *DHS National Security Systems Policy Directive 4300B* provide direction to DHS components regarding the management and protection of sensitive and classified systems, respectively.[1] These policies outline the management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity within the DHS information technology (IT) infrastructure and operations. DHS policy requires that its components ensure that strong inventory management, physical security, logical access, and wireless security controls are implemented for all systems processing sensitive or classified information. The department developed the *DHS 4300A Sensitive Systems Handbook* and *DHS 4300B National Security Systems Handbook* to provide specific techniques and procedures for implementing the requirements of DHS policy. Further, in November 2004, DHS published a series of secure baseline

[1] In this report, we refer to *DHS Sensitive Systems Policy Directive 4300A* and *DHS National Security Systems Policy Directive 4300B* collectively as "DHS policy."

configuration guides for certain operating system and software applications, such as Microsoft Windows XP.

The National Institute of Standards and Technology (NIST) has issued several publications related to laptop inventory management, physical security, logical access, and wireless security controls. Specifically, NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance for establishing adequate logical and physical access controls for sensitive government systems, including the use of strong passwords, encryption, and user administration practices. [redacted][2]

The *Federal Information Security Management Act of 2002* (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to provide security for its information and systems.[3] Policies should ensure that information security is addressed throughout the life cycle of each agency information system and determine minimally acceptable system configuration requirements.

Results of Audit

Standard Configuration Will Enhance Laptop Security

CBP does not have a secure standard configuration for its laptop computers. We evaluated the process used by CBP to develop a standard configuration for its laptop and desktop computers. Also, we conducted computerized and manual security tests of the model system to ensure that it was configured in conformance with DHS and federal guidelines. Finally, we tested a sample of 256 primary, secondary, and loaner laptop computers to determine whether CBP had effectively applied its model system.[4] These tests included:

[2] [redacted]

[3] FISMA is included under Title III of the E-Government Act of 2002 (Public Law 107-347).

[4] As the review focused on vulnerability assessment rather than penetration testing, the audit team was provided administrator access to the CBP model system and laptops, and any hard drive encryption or personal firewalls were disabled.

- Automated vulnerability assessment scans and port scanning of all 256 laptops to identify configuration weaknesses.
- Detailed technical testing for a subset of 69 laptops to confirm the automated testing results and determine account, audit, access privilege, and password parameter settings.
- Password strength analysis on a subset of 122 laptops that do not regularly connect to the network.
- Manual reviews for a subset of 75 laptops to verify the presence and configuration of installed software.

The laptop model system fails to establish the required minimum-security for laptop computers as directed by DHS. Because CBP uses the same process to develop the standard configuration for both its laptop and desktop computers, the configuration weaknesses are relevant to all CBP government-issued computers. In addition, CBP has not ensured that the model system is consistently implemented on all CBP laptops. As a result of the security issues identified, sensitive data may not be adequately protected.

SBU Model System Fails To Establish Minimum Security Settings

CBP has established a model system for the component's laptop computers. A model system, also referred to as a standard build or golden image, is a package of installed software with standardized configuration settings that is created for each major group of IT resources (e.g., routers, user workstations, file servers). The CBP model system was developed based on DHS server configuration guidelines for Microsoft Windows 2000; *CBP Information Systems Security Policies and Procedures Handbook 1400-05B*; National Security Agency (NSA) and Microsoft guidance; and the SysAdmin, Audit, Network, Security (SANS) Institute/Federal Bureau of Investigation (FBI) list of the twenty most critical internet security vulnerabilities. According to CBP, a security test and evaluation (ST&E) was conducted on the model system, and the results of the ST&E were incorporated in the certification and accreditation (C&A) of the system.

The CBP model system incorporates antivirus software, as well as a personal firewall for users that remotely access the CBP network. In addition, the model system employs hard drive encryption, which restricts access to BIOS settings. Also, any built-in wireless or infrared capabilities are disabled. Although these measures enhance the security of CBP's laptop computers, certain critical controls were not incorporated into its model system. Specifically, the model system does not:

- [redacted][5]
- [redacted]

According to CBP IT officials, the weaknesses in the model system configuration were either (1) necessary for the normal functioning of the computers, although CBP officials were not certain that the risk associated with these weaknesses was documented in the ST&E and formally accepted by the systems' designated accrediting authority (DAA); or (2) [redacted]. CBP officials stated that they plan to develop procedures to address configuration management of the model system and ensure compliance with the residual risks formally accepted by the DAA.

DHS Information Security Architecture Guidance and NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*, require that a model system be developed and implemented to ensure that a secure, standard configuration is implemented on desktop and laptop computers. According to NIST, standardized configurations reduce the labor involved in identifying, testing, and applying patches; and, ensure a higher level of consistency, which leads to improved security. DHS requires that each fully supported operating system have a model system from which every computer is built. Also, [redacted]

[5] [redacted]

---------- Finally, DHS policy and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, require that components explicitly accept the risk to agency operations, assets, or individuals associated with the operation of an IT system, based on the implementation of an agreed-upon set of security controls.

SBU Model System Has Not Been Implemented Uniformly

CBP has not implemented consistently its model system for SBU laptop computers. The Windows 2000-based model system is loaded onto a server as an image or copy and installed on new laptops prior to the computers being placed into operation. For the 256 laptops tested, 40 (16 percent) were not running the Microsoft Windows 2000 operating system. These 40 laptops were running seven different operating systems, including Windows 3.1, Windows 95, Windows 98, Windows ME, Windows NT, Windows XP, and Linux. Four of these laptops also allowed dual booting into different operating systems, such as Linux/Windows ME or Windows 98/Windows XP.

For the 216 laptops that were running the model operating system, 125 (58 percent) had configuration vulnerabilities not found on the model system. In addition, ----------

Table 1 illustrates the number of laptops running a non-standard operating system or having additional high and medium risk configuration vulnerabilities, listed by site and by type of laptop.[6]

[6] The tools that the OIG audit team employs assess a risk rating to each of the identified vulnerabilities. These ratings are interpretive and are derived from measures of their probability of occurrence and ease of execution, how well known they are, and the ease of addressing them. We provided the test results related to low risk vulnerabilities to the CBP CIO, but we do not include them in this report due to their low level of significance.

Table 1: Additional Configuration Vulnerabilities Identified

Site/Type	Number of Laptops Tested	Number Running Model System OS	Number Matching Model System[(a)]	Number of Laptops with Additional High or Medium Risk Configuration Weaknesses			
				1-3 Weaknesses	4 - 6 Weaknesses	7 or More Weaknesses	Total With 1 or More Weaknesses
Total							
Total	256	216 (84%)	**71 (28%)**	51 (24%)	41 (19%)	33 (15%)	**125 (58%)**
Weaknesses by CBP Component Office							
Air/Marine Operations	[redacted]						
Border Patrol	[redacted]						
Office of Field Operations	[redacted]						
Office of Strategic Trade	[redacted]						
Weaknesses by Region							
California	[redacted]						
Florida	[redacted]						
Puerto Rico	[redacted]						

(a) Numbers and percentages do not include laptops included in the review that we were unable to test due to software or hardware conflicts.

Source: OIG table based on the results of technical testing and interviews with CBP personnel.

In addition, for the 75 SBU laptops included in our manual review, [redacted] For the 122 laptops included in our password strength analysis, [redacted]

Further, of the 69 laptops included in our detailed technical testing [redacted] In addition, [redacted] Finally, [redacted]

According to CBP IT officials, the laptops that were either running a non-standard operating system or deviated significantly from the model system were largely the result of:

- Border Patrol sites not being connected to the CBP network. According to CBP, the component has not implemented the standard configuration for laptop computers at certain Border Patrol locations because they have not been connected to the CBP network. For example, the Border Patrol Sector Headquarters in San Diego, California is connected to the U.S. Immigration and Customs Enforcement (ICE) network, rather than the CBP network. According to IT officials, [redacted] CBP officials use locally created software images to configure laptop computers at the site. According to CBP, once these locations are connected to the CBP network the laptops will be converted to the standard configuration.
- Laptops placed into operation without being configured by CBP IT personnel. According to CBP IT officials, laptops purchased by local property officers (LPOs) are supposed to be turned over to IT personnel for configuration prior to use, but there is no process in place to enforce this requirement or ensure that IT personnel are notified when new laptops are purchased. The Office of Field Operations in Puerto Rico has implemented an informal process to mitigate this risk by notifying IT officials of computer equipment purchase orders, but this practice has not been established as a formal requirement and does not ensure that newly purchased equipment is provided to IT officials for configuration prior to being placed into operation.
- Special units that were not configured by CBP. Specifically, ICE provided several laptops used [redacted], but the laptops were not reviewed or configured by CBP IT officials prior to being placed into operation. According to CBP, these laptops have unique software and configuration requirements, and the use of these laptops is being documented and will be included in all future C&A packages for all regional local area networks.

- Laptops running an older version of the CBP model system. For example, 14 of 20 laptops at the San Juan Airport in Puerto Rico were not running the current version of the CBP model system. These laptops were not updated because CBP IT officials are not granted access to the official CBP laptop inventory. As a result, IT officials do not have procedures to track the version number of the image installed on issued laptops. Further, CBP IT officials cannot ensure that all laptops are updated appropriately when a new version of the image is released. According to CBP, the component has recognized this problem and is currently working on an automated process to ensure that the laptops connecting to its infrastructure meet minimum configuration requirements through modifications to the component's patch management software. Once the modifications are complete, the software will update any out-of-date laptops that connect to the CBP network. CBP intends to have these modifications implemented by the end of calendar year 2006. This process will not address laptops that do not regularly connect to the CBP network.
- Hardware limitations for older laptops. According to CBP officials, some of the laptops included in our review are no longer in use. The information contained on these laptops [redacted]

DHS policy requires that components establish, implement, and enforce change management and configuration management controls on all IT systems and networks. The DHS IT Security Architecture Guidance also advises that each fully supported operating system have a standard configuration from which every instance is built. According to NIST SP 800-40, standardized configurations reduce the labor involved in identifying, testing, and applying patches; and ensure a higher level of consistency, which leads to improved security. DHS and federal configuration guidelines also establish requirements related to security parameter settings, including account policy settings, access permissions, and renaming administrator and guest accounts. As a result of CBP not ensuring that all laptop computers are configured appropriately, [redacted][7]

[7] [redacted]

Improved Patch Management Will Increase Security

CBP has not established effective procedures to patch and update its laptop computers. We reviewed the CBP laptop model system to determine if all of the applicable operating system and application patches were installed. In addition, we conducted vulnerability assessment scans on a sample of 217 laptop computers to determine if all patches had been applied.[8] CBP has procedures to patch laptops prior to being placed into operation by including patches and updates as part of the model system installation process. For laptop and desktop computers in operation, patches and updates are distributed through the CBP network by patch management software.

There were patches and updates related to high and medium risk vulnerabilities that had not been applied. Specifically, ---

Table 2 illustrates the number of missing high and medium risk patches and updates on CBP laptops listed by site and by type of laptop.

[8] Although total of 256 laptops were tested, we were not able to obtain vulnerability assessment information for 39 laptops due to a software conflict.

Table 2: Missing Patches and Updates						
Site/Type	**Number of Laptops Tested**	**Number of Laptops with Missing Patches or Updates[(a)]**				
		3 or Fewer Patches	4 - 10 Patches	11 - 20 Patches	21 - 30 Patches	31 or More Patches
Total						
Total	217	84 (39%)	24 (11%)	18 (8%)	23 (11%)	47 (22%)
Weaknesses by CBP Component Office						
Air/Marine Operations	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Border Patrol	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Office of Field Operations	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Office of Strategic Trade	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Weaknesses by Region						
California	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Florida	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Puerto Rico	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

(a) Does not include laptops included in the review that we were unable to test due to software or hardware conflicts.

Source: OIG table based on the results of technical testing and interviews with CBP personnel.

Further, for 66 of the 75 laptops included in our manual reviews that had [redacted]

Patches and updates were missing because most of the CBP laptops included in our review are used as secondary or shared laptops that do not regularly connect to the CBP network. Specifically, for the 217 laptops included in our vulnerability assessments scans, only six laptops in Puerto Rico are assigned as a user's primary workstation. In addition, CBP offices in Puerto Rico were not able to rely on the component's patch management software because frequent lapses in connectivity to its network disrupted the software. Further, certain Border Patrol sites are connected to the ICE network, rather than the CBP

network, and thus are not linked to CBP's patch management software. CBP has not implemented adequate procedures for laptops that do not connect to the network. For example, CBP IT officials in Puerto Rico have created a CD-based process to patch laptop computers. Nonetheless, we found [redacted]

DHS policy requires that IT security patches be installed in accordance with configuration management plans or direction from DHS CSIRC. According to NIST SP 800-40, patching is critical to maintaining the operational availability, confidentiality, and integrity of information technology systems. NIST SP 800-40 recommends that organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches.

Because CBP had not applied all relevant patches and updates to its laptops, the computers were vulnerable to [redacted][9] For example, by [redacted]

Enhanced Inventory Management Is Needed For Property Accountability

CBP has not established effective inventory management procedures for its laptop computers. We evaluated CBP procedures for maintaining an accurate laptop inventory, returning equipment upon employee exit or transfer, handling lost or stolen laptops, clearing or sanitizing laptops before reuse or disposal, and the proper labeling of laptop computers. Also, we reviewed laptop physical security measures, and assessed the CBP laptop inventory by analyzing the integrity of inventory data and conducting verification tests on the 75 laptop computers included in our manual reviews.

[9] [redacted]

CBP has procedures to ensure that laptops are returned upon employee removal or transfer, as well as adequate laptop physical security measures. CBP has not implemented several critical inventory management controls. Specifically, CBP has not (1) maintained an accurate inventory; (2) ---------- ---------- ---------- (3) appropriately labeled its SBU laptops; or (4) ensured that lost or stolen laptops were reported to the appropriate officials. As a result of the weaknesses in CBP's inventory procedures, there is greater risk that laptop computers will not be configured and secured adequately. Further, access to classified and sensitive information may not be restricted appropriately.

Laptop Inventory Is Not Accurate

Although CBP has an inventory of its SBU laptops, it has not established procedures to ensure that inventory records are accurate. For example, 49 of 105 laptops at the Border Patrol facility in El Centro, California, had been locked in a storage room pending disposal. The status codes for the laptops in the CBP inventory indicate that the laptops are currently in use. Further, for the 75 laptops included in our manual review, 21 laptops had an incorrect or missing asset tag, serial number, and/or manufacturer information listed in the inventory. In addition, six laptops at the Border Patrol Sector Headquarters in Pembroke Pines, Florida, and two laptops at the Mayaguez Port in Puerto Rico were in use but not included in the CBP laptop inventory.

According to CBP officials, these discrepancies were largely the result of the component not:

- Managing effectively the transition of Border Patrol laptop computers from the ICE inventory to the CBP inventory. According to CBP officials, a number of errors were created in the CBP laptop computer inventory when laptops from the Border Patrol Sector Headquarters in Pembroke Pines, Florida were transferred to the CBP inventory in August 2005. Inventory records were not retained at the site following the transition, and the transfer of some property items to ICE was not properly recorded. CBP officials stated they do not have an official property officer, and the priority since the transition has been on resolving issues related to desktop computers and network connectivity.
- Conducting adequate inventory reviews. Although CBP requires that physical inventory reviews be conducted annually, these reviews do not include all laptop computers or an examination of installed software. The LPO stated that he has served in the position for four years but has

not received formal training in property management and performs the LPO function as a collateral duty.

DHS policy requires that components develop and maintain a property inventory of all portable electronic devices (PED), such as laptops. This inventory is to include serial numbers and/or seat numbers, user names, use, and location of all PEDs for accountability purposes.[10] Also, each DHS-owned PED is to have an asset tag, and asset tag numbers are to be included in the inventory. In addition, DHS policy requires that components conduct reviews, at least semiannually, of all equipment and software to ensure that only government-licensed software and equipment are being used, and that appropriate exceptions have been documented. As a result of these weaknesses in the CBP inventory, there is greater risk that laptop computers will not be configured and secured adequately.

Laptops Are Not -

CBP has not implemented procedures to ensure that sensitive data is ---------- ---------- ---------- of its SBU laptop computers.[11] Specifically:

- None of the sites using ---------- were periodically testing the equipment to verify that it is functioning properly.
- Laptops scheduled for reuse are usually re-imaged, ---------- ----------
- CBP allows laptops to be donated to an outside organization with the ---------- ---------- --------
- *CBP Information Systems Security Policies and Procedures Handbook 1400-05B* does not address the removal of all labels or markings prior to laptops being disposed.

According to CBP officials, the component plans to review its hardware clearing and disposal policies and procedures to ensure compliance with federal laws and regulations. In addition, ---- ----------

[10] A seat, also referred to as a "node," is an intelligent element like a processor that can communicate using interprocessor communications. A seat is where entities and ports reside.

[11] Clearing a hard drive requires overwriting all locations with a pseudo-random pattern twice, overwriting all locations with a known pattern, and then verifying the procedure by randomly re-reading (a minimum of 1 percent recommended) the overwritten information. Sanitizing a hard drive requires incineration or degaussing (see approved degausser list at http://www. nsa.gov/ia/government/mdg.cfm).

[redacted] in the upcoming revision of the *CBP Information Systems Security Policies and Procedures Handbook 1400-05*.

DHS policy requires that components ensure that any information system's storage medium containing sensitive information be [redacted] within the organization. DHS policy also requires that components ensure that any information system's storage medium containing sensitive information be [redacted] As a result of the weaknesses in the CBP process for [redacted] there is greater risk that access to sensitive information may not be limited adequately. For example, [redacted]

Laptops Are Not Marked Appropriately

CBP has not affixed external labels to its SBU laptops indicating that the laptops are not authorized for classified processing. According to CBP, the component's Office of Information Technology is in the process of coordinating with the CBP Office of Finance/Property Management to research the feasibility of purchasing and affixing the necessary labels.

DHS policy requires that all laptop computers not authorized to process classified information have a label affixed indicating, "This machine is not authorized for classified processing." DHS policy also requires that all equipment be marked with the highest classification level of the information that has been processed or stored on the device. Because these laptops were not appropriately marked, there is greater risk that classified information may have been processed on an unclassified system.

Lost Or Stolen Laptops Are Not Reported Appropriately

CBP has not ensured that lost or stolen laptops are reported to the DHS CSIRC. We identified five Border Patrol laptops from California and Florida that were lost or stolen during calendar year 2005. The laptop security incidents were investigated and reported to the Border Patrol Sector Headquarters, but were not reported to DHS CSIRC. CBP plans to issue a formal memorandum from the Assistant Commissioner, Office of Information Technology, addressing employee responsibilities for security incident reporting.

DHS policy requires that components report significant computer security incidents to the DHS CSIRC immediately upon identification and validation of incident occurrence. The DHS CSIRC is normally responsible for notifying appropriate law enforcement authorities of a security event, to pursue the investigation and recommend disciplinary action, if required. Because CBP had not reported these security incidents to the DHS CSIRC, senior DHS officials may not be aware of the extent or scope of laptop security issues at the department, and the appropriate corrective actions may not have been taken. Further, without an accurate and current inventory, CBP may be unaware of additional laptops that are missing.

Recommendations

To secure CBP data stored on government-issued laptop computers, we recommend that the Commissioner of CBP instruct the CIO to:

1. Remedy the existing critical vulnerabilities in the standard configuration for laptops, based on DHS and federal configuration guidelines. Further, the CIO should confirm whether similar vulnerabilities and remediation are applicable to all government-issued computers within CBP.
2. Establish procedures to ensure that model systems are configured to protect CBP data and verified prior to implementation.
3. Ensure that the updated model system is correctly implemented on all CBP laptop computers.
4. Implement procedures to ensure that all CBP laptops are patched and updated in a timely manner, including those that do not regularly connect to the CBP network, as well as all CBP government-issued computers.
5. Implement appropriate inventory management controls to ensure that an accurate laptop inventory is maintained, including effective inventory reviews and adequately trained local property officers.
6. [redacted], and ensure that SBU laptops are labeled appropriately, in accordance with DHS and federal guidelines.

7. Report computer security incidents to DHS CSIRC in a timely manner to ensure that the incidents are investigated and appropriate corrective action is taken.

Management Comments And OIG Analysis

CBP concurs with recommendation 1. CBP has taken steps to remedy deviations with access privileges and password controls on its laptop computers. By April 2007, CBP will implement a new certified and accredited model image. CBP's Information Systems Security Officers will insure that all government-issued laptop computers adhere to DHS policy on access privileges and password controls.

We accept CBP's response to implement corrective action plans for the existing vulnerabilities and to correct the deficiencies in access privileges and password controls.

CBP concurs with recommendation 2. CBP has taken steps to remedy deviations from standard configurations on its laptops. All future model images will be routinely verified for compliance with the applicable certification and accreditation before being implemented.

We accept CBP's response to implement corrective action plans for the existing vulnerabilities in its standard configuration.

CBP concurs with recommendation 3. CBP has taken steps to ensure that the updated model systems are correctly implemented on all CBP laptop computers. CBP has distributed guidance on its web page and through email to all CBP personnel reminding them of their responsibilities associated with laptop computers. By January 2007, CBP will decide on a technique to verify compliance. CBP will then conduct self-assessments every six months to measure compliance and take remediation action as necessary.

We accept CBP's response to ensure that the updated model systems are correctly implemented on all CBP laptop computers.

CBP concurs with recommendation 4. CBP has taken steps to ensure that laptop computers are patched and updated. CBP has distributed guidance on its web page and through email to all CBP personnel reminding them of their

responsibilities associated with laptop computers. This includes information necessary for receiving patches to the standard configuration.

We accept CBP's response to ensure that the updated model systems are correctly implemented on all CBP laptop computers.

CBP concurs with recommendation 5. In November 2006, CBP began conducting laptop inventories semiannually. Also, CBP will conduct mandatory quality assurance reviews during every site visit for laptop computers assigned to its location. Site visits will be prioritized based on overall property loss rates experienced during the FY06 inventory.

We accept CBP's response to implement appropriate controls to manage its inventory. However, we maintain that CBP should provide adequate training to its local property officers.

CBP concurs with recommendation 6. During its semiannual inventories and quality assurance reviews, CBP property specialists will ensure that the requirements in the CBP Personal Property Handbook regarding ---------- ------- ---------- -- have been completed. In September 2006, the Department amended DHS 4300A to make labeling of SBU computers "recommended" rather than "required." CBP has no plans to put labels on its computers at this time.

We accept CBP's response to ---------- ------- ---------- ---------- Further, although DHS 4300A no longer requires computer labeling, we maintain that because of CBP's diverse and sensitive mission, CBP should consider applying labels to its laptop computers. The use of warning banners serves as a reminder to all users that the computers that they are accessing are government computers used to process sensitive information and must be used in accordance with good security practices.

CBP concurs with recommendation 7. CBP has already taken steps to remind all CBP personnel to report security incidents to Office of Information Technology and DHS CSIRC in a timely manner. In addition, a process will be developed so that the results of the laptop surveys performed by local property officers will be compared to reports received by DHS CSIRC.

We accept CBP's response to report computer security incidents to DHS CSIRC in a timely manner to ensure that the incidents are investigated and appropriate corrective action is taken.

Purpose, Scope, and Methodology

The objective of this audit was to determine whether CBP had implemented adequate and effective security policies and procedures related to the physical security of and logical access to its government-issued laptop computers. Specifically, we determined whether CBP had implemented adequate (1) policies and procedures for inventory management; (2) physical security measures; (3) logical access controls; and, (4) wireless security measures for sensitive data contained in its government-issued laptops. Our focus was to test the development and implementation of an adequate model system for the laptop computers processing and storing sensitive or classified DHS data, as well as the procedures used to patch and update laptops once placed into operation. In addition, we obtained FISMA information required for the OIG's annual independent evaluation.

To identify sensitive laptop computers, we analyzed the CBP laptop computer inventory as of January 2006. Based on our review of the laptop inventory, we selected the following CBP sites for testing:

CBP Testing Locations and Laptop Computers

Region	***256 SBU Laptops (17 sites)***			
	California	**Florida**	**Puerto Rico**	***Total***
Air/Marine Operations	10 Laptops (1 site)	-	-	**10 Laptops (1 site)**
Border Patrol	56 Laptops (3 sites)	19 Laptops (1 site)	8 Laptops (1 site)	**83 Laptops (5 site)**
Office of Field Operations	19 Laptops (1 site)	58 Laptops (3 sites)	65 Laptops (5 sites)	**142 Laptops (9 site)**
Office of Strategic Trade	21 Laptops (2 sites)	-	-	**21 Laptops (2 sites)**
Total	**106 Laptops (7 sites)**	**77 Laptops (4 sites)**	**73 Laptops (6 sites)**	**256 Laptops (17 sites)**

We performed automated vulnerability assessment scans and port scanning of all 256 laptops to identify configuration weaknesses and missing patches; detailed technical testing for a subset of 69 laptops to confirm the automated testing results and determine account, audit, access privilege, and password parameter settings; password strength analysis on a subset of 122 laptops that do not regularly connect to the network; and manual reviews for a subset of

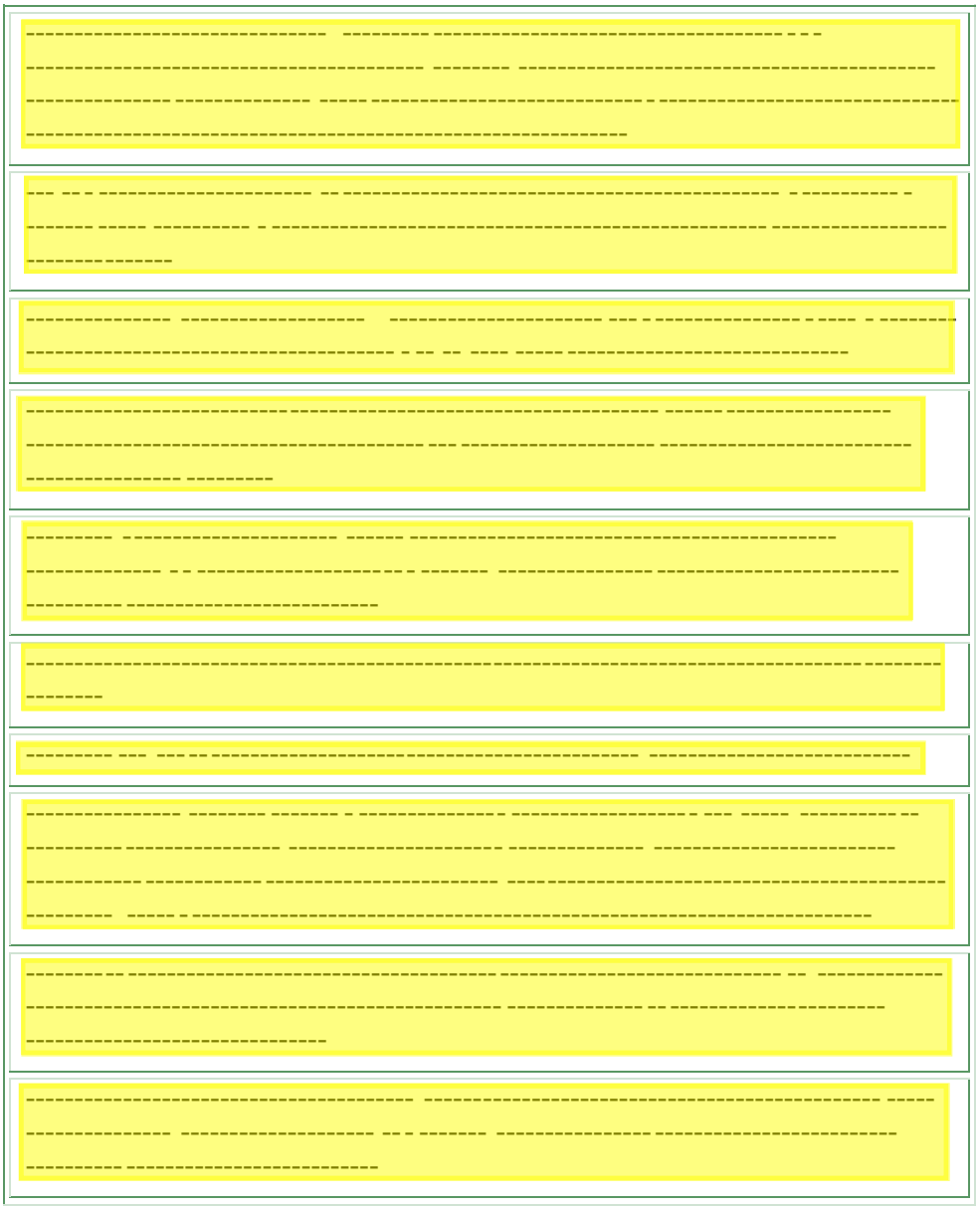
75 laptops to verify the presence and configuration of installed software. Upon completion of the tests, we provided component officials with technical reports detailing the specific vulnerabilities detected on their system and the actions needed for remediation.

We conducted fieldwork at CBP facilities in Washington, DC; El Centro, Long Beach, and San Diego, CA; Fort Lauderdale, Miami, and Pembroke Pines, FL; Aguadilla, Mayaguez, and San Juan, PR; and the OIG Advanced Technology Laboratory (ATL).[12] We conducted our audit from February to May 2006 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 D.

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

[12] The ATL supports our capability to perform effective and efficient technical assessments of DHS information systems in diverse operating environments. The ATL is a collection of hardware and software that allows the simulation, testing, and evaluation of the computing environments that are most commonly used within DHS.

We used 10 testing tools to conduct internal security tests to evaluate the effectiveness of controls implemented for the systems:



Source: OIG auditors conducting security scans on laptop computers in Fort Lauderdale, Florida.

Source: OIG auditors conducting security scans on laptop computers in Fort Lauderdale, Florida.

Source: CBP Vehicle and Cargo Inspection System (VACIS) vehicle.

Source: CBP laptop computer mounted in VACIS vehicle.

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

U.S. Customs and
Border Protection

September 14, 2006

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

FROM: Director
Office of Policy and Planning

SUBJECT: Response to the Office of Inspector General's Draft Report - *Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security*

Thank you for providing us with a copy of your draft report entitled *Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security* and the opportunity to discuss the issues in this report. The draft report assesses whether U.S. Customs and Border Protection (CBP) has established and implemented adequate and effective security policies and procedures related to the physical security and logical access to its laptop computers. The CBP appreciated the opportunity to work with the auditors in constructing a balanced and accurate document.

The Office of Inspector General (OIG) concluded that CBP has not developed adequate policies and procedures to ensure physical security and logical access to its laptop computers. CBP needs to strengthen configuration, patch, and inventory management controls necessary to protect its laptop computers. The OIG recommended that the Commissioner direct the Chief Information Officer (CIO) to develop and implement policy and procedures that address these security concerns. CBP concurs with the findings and recommendations and is already taking corrective measures. Additionally, CBP is conducting research to determine the best method for verifying user compliance to the requirement to have their laptops regularly updated with the most current updates and patches.

Attached are comments specific to the recommendations. 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."

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Janiene Jones, Audit Liaison, Office of Policy and Planning, at (202) 344-2169.

Response to the Office of Inspector General's Draft Report -*Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security*

RECOMMENDATION 1: Remedy the existing critical vulnerabilities in the standard configuration for laptops, based on DHS and federal configuration guidelines. Further, the CIO should confirm whether similar vulnerabilities and remediation are applicable to all government–issued computers within CBP.

Response: CBP concurs with the OIG and recommendation and has already taken steps to remedy the auditor's concerns with access privileges and password controls on CBP laptops. A new model image, PC Client 3.01, has been developed and its compliance with the applicable certification and accreditation is being verified. Implementation of this model image is scheduled to begin by January 2007. For non-laptop computers, Information System Security Officers (ISSOs) routinely work to insure that they adhere to DHS policy on access privileges and password controls.

Due Date: April 30, 2007

RECOMMENDATION 2: Establish procedures to ensure that model systems are configured to protect CBP data and verified prior to implementation.

Response: CBP concurs with the OIG and recommendation and has already taken steps to remedy the auditor's concerns regarding deviations from standard configurations on CBP laptops. OIT is testing a new laptop model image for compliance with the applicable certification and accreditation (C&A). This pre implementation testing will be completed by Dec 15, 2006. Deployment is expected to begin by January 2007. All future model images will be routinely verified for compliance with the applicable C&A before being implemented.

Due Date: April 30, 2007

RECOMMENDATION 3: Ensure that the updated model system is correctly implemented on all CBP laptop computers.

Response: CBP concurs with the finding and recommendation and has already taken steps to remedy deviation from standard configurations. OIT has distributed guidance via posting to the CBP Web Page and Mass (email) Mailings to all CBP personnel reminding them of their responsibilities associated with laptop computers. This includes the information necessary for initial configuration.

OIT is currently considering two techniques to verify compliance and will select one by January 1, 2007. Implementation will begin in the March 2007 timeframe.

In April 2007, OIT will conduct a random sampling self-assessment to measure compliance and take remediation action as necessary. Thereafter, OIT will conduct random sampling audits every 6 months to measure compliance.

Due Date: April 30, 2007

RECOMMENDATION 4: Implement procedures to ensure that all CBP laptops are patched and updated in a timely manner, including those that do not regularly connect to the CBP network, as well as all CBP government-issued computers.

Response: CBP concurs with the finding and recommendation and has already taken steps to remedy deviation from standard configurations. OIT has distributed guidance via posting to the CBP Web Page and Mass (email) Mailings to all CBP personnel reminding them of their responsibilities associated with laptop computers. This includes the information necessary for receiving patches to the standard configuration.

OIT is currently considering two techniques to verify compliance and will select one by January 1, 2007. Implementation will begin in the March 2007 timeframe. In April 2007, OIT will conduct a random sampling self-assessment to measure compliance and take remediation action as necessary. Thereafter, OIT will conduct random sampling audits every 6 months to measure compliance.

Due Date: April 30, 2007

RECOMMENDATION 5: Implement appropriate inventory management controls to ensure that an accurate laptop inventory is maintained, including effective inventory reviews and adequately trained local property officers.

Response: CBP Property Management Branch will begin conducting laptop inventories semiannually starting in November 2006. Additionally, Property Management Branch will also conduct mandatory quality assurance reviews (QARs) during every site visit to a CBP field location (Assistance visit, Training Visit, etc) of laptops computers assigned to that location. At a minimum, Property Management Branch will conduct these visits monthly. Site visits will be prioritized based on overall property loss rates experienced during the FY06 inventory. Office of Finance will provide reports as necessary to respective Assistant Commissioners.

Due Date: September 30, 2007

RECOMMENDATION 6: and ensure that SBU laptops are labeled appropriately, in accordance with DHS and federal guidelines.

Response: During the QARs specified in the response to #5 above, CBP property specialists will review disposal documentation on file for laptop computers to verify that actions specified in the CBP Personal Property Handbook regarding [redacted] have been completed, and Office of Finance will provide reports as necessary to respective Assistant Commissioners. In researching the recommendation for "Sensitive But Unclassified" labeling of laptops computers, the CBP Office of Information and Technology notified Office of Finance that the DHS reference that required this labeling (DHS 4300A) changed in September 2006, making this labeling "recommended" versus "required". OIT noted the recommendation, but has no plans to make it a requirement within CBP at this time.

Due Date: September 30, 2007

RECOMMENDATION 7: Report computer security incidents to DHS CSIRC in a timely manner to ensure that the incidents are investigated and appropriate corrective action is taken.

Response: CBP concurs with the finding and recommendation and has already taken steps to remind all CBP personnel of current policy and their responsibilities concerning laptop computers to include the need to report security incidents to OIT and DHS CSIRC in a timely manner. In addition, a process will be developed so that the results of laptop surveys performed by local property officers (LPOs) will be compared to reports received by DHS CSIRC. This will measure compliance with the policy on reporting loss of laptops. These comparisons between property and CSIRC incident records will permit trend analysis and better focusing of corrective actions The Executive Director of the OIT Technical Operations Division, is the accountable official.

Due Date: January 31, 2007

FISMA Requirements

Title III of the *E-Government Act*, entitled FISMA, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets.[13] The agency's security program should provide security for the information as well as the systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

To comply with the Office of Management and Budget's (OMB) FISMA reporting requirements, we evaluated the effectiveness of CBP's information security program and practices as implemented for SBU laptop computers to determine whether DHS continues to make progress in implementing its agency-wide information security program. We collected information relative to C&A, system impact level determination, NIST SP 800-26 annual assessment, assessment of E-authentication risks, specialized security training, and Plan of Action and Milestones (POA&Ms).[14]

Our evaluation of the CBP laptop systems shows that the component has implemented many key security management practices into its information security program, as required by FISMA.

[13] The E-Government Act of 2002 (Public Law 107-347), December 17, 2002.
[14] As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, and NIST 800-63, *Electronic Authentication Guideline.*

Table 4: FISMA Compliance Metrics

FISMA Reporting Requirements	NE Field LAN	NW Field LAN	SE Field LAN	SW Field LAN	Notes
Does the system have a complete and current C&A?	Yes	Yes	Yes	Yes	The systems were granted authority to operate (ATO) in April and May 2006.
Has the system's impact level been determined according to Federal Information Processing Standard Publication 199 criteria?	Yes	Yes	Yes	Yes	Each system's impact level was determined to be Moderate for confidentiality, integrity, and availability.
Does the system have a complete and current NIST SP 800-26 annual assessment?	Yes	Yes	Yes	Yes	Self-assessments were completed in September 2005.
Does the system have a security plan and risk assessment?	Yes	Yes	Yes	Yes	System security plans were completed on March 17, 2006, and risk assessments were completed in 2005.
Were the system's security controls tested and evaluated in the last year?	Yes	Yes	Yes	Yes	Each system completed a ST&E between March to May 2006.
Has a system contingency plan been established and tested?	**No**	**No**	**No**	**No**	The systems have contingency plans dated 2005, but the plans have not been tested within the past year.
Has an assessment of E-Authentication risk been performed for the system?	N/A	N/A	N/A	N/A	Remote users do not authenticate to the systems for the purposes of conducting government business electronically.
Have personnel with significant security responsibilities obtained specialized security training?	Yes	Yes	Yes	Yes	As of May 13, 2006, 610 of the 637 personnel with significant security responsibilities had received specialized security training.
Have individuals involved in the administration of IT systems, or with significant security responsibilities, obtained specialized privacy training?	N/A	N/A	N/A	N/A	According to CBP, the systems do not contain privacy data.
Are POA&Ms created and managed for the system?	Yes	Yes	Yes	Yes	POA&Ms have been created and entered into the DHS FISMA reporting system for each of the systems.

Source: OIG table based on interviews with CBP personnel and analysis of DHS FISMA reporting system data.

Information Security Audits Division
Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Jason Bakelar, Audit Team Leader
William Matthews, Auditor
Eugene Yu, Auditor
Anthony Nicholson, Referencer

Advanced Technology Division
Chris Hablas, Senior Security Engineer
Marcus Badley, Senior Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Policy
DHS GAO/OIG Audit Liaison
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative and Intergovernmental Affairs
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison
Audit Liaison, U.S. Customs and Border Protection
Chief Privacy Officer

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 e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.