DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Administration Can Enhance Science and Technology 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.

Office of Information Technology

OIG-06-42 June 2006

Office of Inspector General

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

Homeland
Security

June 29, 2006

Preface

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

This report assesses the strengths and weaknesses of the Science and Technology Directorate's (S&T) laptop computer security controls. It is based on interviews with S&T 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

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
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IP	Internet Protocol
ISSM	Information Systems Security Manager

Table of Contents/Abbreviations

IT	Information Technology
LAN	Local Area Network
MANPADS	Man-Portable Air Defense Systems
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PED	Portable Electronic Device
POA&M	Plan of Action and Milestones
S&T	Science and Technology Directorate
SP	Special Publication
ST&E	Security Test and Evaluation

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 the Science and Technology Directorate (S&T). Our objective was to determine whether S&T has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptop computers.

Significant work remains for S&T to further strengthen the configuration, patch, and inventory management controls necessary to secure its data stored on government-issued laptop computers. Specifically, S&T has not established: (1) a standard configuration that meets required minimum-security settings, for its laptops; (2) effective procedures to patch laptop computers that do not regularly connect to the network or that were released without a standard image; and, (3) adequate inventory management procedures. As a result, sensitive information stored and processed on S&T's laptop computers may not be protected adequately. Further, because S&T uses the same procedures to develop a model for its laptop and desktop computers, the configuration weaknesses identified with laptop computers are relevant to all government-issued computers assigned within S&T.

S&T officials stated that they have already taken or plan to take corrective action to address many of the weaknesses we identified, including the implementation of an updated standard configuration for the laptops at one of the S&T field offices reviewed. As our fieldwork was complete, we did not verify that the weaknesses had been remedied.

We recommend that the Under Secretary for S&T instruct the S&T Chief Information Officer (CIO) to:

- Remedy the existing critical vulnerabilities in the standard model configuration for laptops. Further, the S&T CIO should confirm whether similar vulnerabilities and remediation are applicable to all S&T issued computers.
- Ensure that the updated model system is correctly implemented.
- Develop procedures to ensure that all S&T laptops are patched and updated in a timely manner.
- Implement appropriate inventory management controls, including effective inventory reviews, physical security controls, and classification labeling.

Fieldwork was conducted from December 2005 to January 2006 at S&T headquarters in Washington, DC; S&T field offices in Arlington and Alexandria, VA; and the OIG Advanced Technology Laboratory (ATL). See Appendix A for our purpose, scope, and methodology.

In response to our draft report, the Under Secretary for S&T (Acting) concurred with our recommendations and is in the process of implementing corrective measures. In addition, plans of action and milestones (POA&Ms) will be created and tracked for the vulnerabilities we identified. S&T'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 S&T, U.S. Customs and Border Patrol, United States Secret Service, and U.S. Immigration and Customs Enforcement.

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 Publication 4300A and *DHS National Security Systems Policy Publication 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 Sensitive Systems Handbook and National Security Systems Handbook to provide specific techniques and procedures for implementing the requirements of DHS policy. Further, in August 2005, DHS issued a series of secure baseline configuration guides for

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

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

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. Further, [redacted]

The *Federal Information Security Management Act of 2002* 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

S&T does not have a standard configuration that effectively protects laptop computers. We evaluated the process used by S&T to develop a model 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 50 primary, secondary, and loaner laptop computers to determine whether S&T had effectively applied its model system.[4] These tests included:

[redacted]

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

[4] To adequately perform the tests, the audit team was provided administrator access to the S&T model system and laptops, and disabled any personal firewalls on the laptops.

- Automated vulnerability assessment testing and port scanning of all 50 laptops to identify configuration weaknesses.
- Detailed technical testing for a subset of 22 laptops to confirm the automated testing results and determine account, audit, access privilege, and password parameter settings.
- Password strength analysis on a subset of nine laptops settings that do not regularly connect to the network.
- Manual reviews for a subset of 20 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. For example, [redacted] Finally, because S&T uses the same procedures to develop a model for its laptop and desktop computers, the configuration weaknesses identified with laptop computers are relevant to all government-issued computers assigned within S&T. As a result of the security issues identified, sensitive data may not be adequately protected.

Model System Fails To Establish Minimum Security Settings

S&T has implemented a model system to configure consistently its laptop computers. A model system, also referred to as a standard build or golden image, is a package of installed software with standard configuration settings that is created for each major group of IT resources (e.g., routers, user workstations, file servers). A model system is a read-only mechanism that is used to build new instances of the system. S&T relies on DHS' Office of Infrastructure Operations (DHS Infrastructure Operations) for developing and implementing the model system used on S&T computers.[5] S&T's laptop and desktop computers are connected to the DHS Infrastructure Operations Local Area Network (LAN) A system. The LAN A is a general support system that provides sensitive but unclassified electronic communications, word processing, and data transfer for all Headquarters DHS personnel within the Washington, DC metropolitan area. Although it uses the infrastructure provided by DHS,

[5] Infrastructure Operations specifies, designs, implements, and operates the consolidated DHS IT infrastructure of behalf of the department.

S&T is responsible for ensuring that its data is protected in accordance with DHS minimum security requirements.

The model system for S&T's laptop and desktop computers was developed by DHS Infrastructure Operations based on DHS and NIST configuration guidelines, as well as the requirements established in DHS policy. The model system incorporates antivirus software, and includes the disabling of any built-in wireless capabilities. However, the DHS provided model system does not incorporate certain critical controls. Specifically, the model system does not:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted] because these controls were not included in the image provided by DHS Infrastructure Operations. S&T has not requested that DHS Infrastructure Operations modify the image to incorporate these controls. DHS Infrastructure Operations is exploring ways to implement [redacted] but is also

[redacted]

working on the implementation of a new laptop image as an interim measure that would be used for remote users outside of the DHS Headquarters network environment. S&T's configuration weaknesses were the result of [redacted] by DHS on the model system. DHS Infrastructure Operations plans to deploy a new image to address these configuration weaknesses by October 2006.

DHS and NIST 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, standard configurations reduce the labor involved in identifying, testing, and applying patches; and, encourage a higher level of consistency that generally leads to improved security. Further, DHS requires that each fully supported operating system have a model system used to configure every computer.

DHS and NIST recommend that the [redacted] be set on sensitive systems to reduce the possibility of exploitation by an attacker with physical access to the laptop. DHS and NIST require that sensitive information stored on laptop computers that may be used in a residence or on travel be [redacted]

As a result of the critical vulnerabilities and configuration weaknesses in the model system, S&T laptops and data are not protected adequately. For example, [redacted]

[redacted]

Model System Has Not Been Implemented Uniformly

S&T has not implemented consistently its model system for laptop computers. A model system is loaded onto a server as an "image" or copy. The image is then installed on new laptops prior to the computers being placed into operation. For the 50 laptops tested, 12 (24 percent) had configuration vulnerabilities not found on the model system. This includes seven of the nine laptops tested at the Counter-Man-Portable Air Defense Systems (MANPADS) office, as well as four of the eight loaner laptops and one user assigned laptop at the S&T Headquarters facility.

Table 1 illustrates the number of additional high and medium risk configuration vulnerabilities on S&T laptops listed by site and by type of laptop.[8]

Table 1: Additional Configuration Vulnerabilities Identified

Site/Type	Number of Laptops Tested	Number Matching Model System	Number of Laptops with Additional High or Medium Risk Configuration Weaknesses				
			1 Weakness	2 - 5 Weaknesses	6 - 10 Weaknesses	11 or More Weaknesses	Total With 1 or More Weaknesses
Total							
Total	50	**38 (76%)**	1 (2%)	0	3 (6%)	8 (16%)	**12 (24%)**
Weaknesses by Site							
Headquarters	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
BioWatch	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Counter-MANPADS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Weaknesses by Type of Laptop							
Primary	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Loaner/Shared	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

[8] The tools used by the OIG assessed 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 the low risk vulnerabilities to the S&T CIO, but we do not include them in this report due to their low level of significance.

In addition, for the 20 laptops included in our manual reviews, there were three with [redacted] Also, nine of the 20 laptops did not have a [redacted] The S&T model system incorporates a [redacted]

Further, of the 22 laptops included in our detailed testing:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

According to DHS Infrastructure Operations, the laptops included in our automated vulnerability assessment scans, manual reviews, and detailed testing that deviated significantly from the model system were the result of (1) laptops running an older image that was implemented prior to the laptops becoming part of the LAN A network system; or, (2) laptops in which the current model system was not implemented correctly. DHS Infrastructure Operations is in the process of re-imaging these laptops.

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

[9] [redacted]

fully supported operating system have a standard configuration from which every instance is built. According to NIST, standard configurations reduce the labor involved in identifying, testing, and applying patches; and, encourage a higher level of consistency, which generally leads to improved security. DHS and federal configuration guidelines also establish requirements related to security parameter settings, including account policy settings, shares, and access permissions. As a result of S&T not ensuring that all laptop computers are configured appropriately, [redacted]

Improved Patch Management Will Increase Security

S&T has not established effective procedures to patch and update its laptop computers. We reviewed the S&T laptop model system to determine if all of the applicable operating system and application patches had been applied. In addition, we tested a sample of 50 primary, secondary, and loaner laptop computers to determine if all appropriate patches had been applied. Laptops are patched prior to being placed into operation, as part of the model system installation process. For laptops already in operation, DHS Infrastructure Operations patches and updates these laptops through the LAN A network. DHS Infrastructure Operations downloads patches from the Microsoft website based on CSIRC and vendor recommendations, tests the patches on a base software image, and then distributes them to connected laptop and desktop computers through the use of patch management software. Antivirus software is also updated to connected computers through the network. The patch and virus update management software applications also track certain connected computers that have not been patched and updated.

There were patches and updates related to high and medium risk vulnerabilities that had not been applied. Specifically, S&T has not:

- Applied all relevant patches and updates to laptops that regularly connect to the network. Specifically, [redacted] Further, six of the 13 user

[redacted]

assigned laptops included in our manual reviews had [redacted] According to the S&T CIO, the laptops at the [redacted] were not receiving regular patches and updates through the network because they were operating on an older standard configuration that was not compatible with DHS Infrastructure Operations' patch management software. In addition, DHS Infrastructure Operations does not currently have a process to [redacted] S&T officials stated that subsequent to the completion of our fieldwork, the updated model system was installed on the laptops at this location.

- Patched laptops that do not regularly connect to the network. Specifically, four loaner laptops were [redacted] Further, all five of the loaner and shared laptops included in our manual reviews had [redacted] The DHS Infrastructure Operations Information Systems Security Manager (ISSM) was not aware of any existing procedures to [redacted]

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

Table 2: Missing Patches and Updates							
Site/Type	Number of Laptops Tested	Number With no Missing Patches	Number of Laptops with Missing Patches or Updates				
			1 – 3 Patches	4 - 10 Patches	11 - 20 Patches	21 - 30 Patches	Total Missing 1 or More Patches
Total							
Total	50	**38 (76%)**	1 (2%)	5 (10%)	3 (6%)	3 (6%)	**12 (24%)**
Patches by Site							
Headquarters	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
BioWatch	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Counter-MANPADS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Patches by Type of Laptop							
Primary	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Loaner/Shared	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

DHS policy requires that IT security patches be installed in accordance with configuration management plans or direction from higher authorities. According to NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*, patching is critical to the operational availability, confidentiality, and integrity of information technology systems. NIST recommends that organizations have an explicit and documented patching and vulnerability policy as well as a systematic, accountable, and documented process for handling patches.

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

[redacted]

[redacted]

Enhanced Inventory Management Is Needed For Property Accountability

S&T has not established effective inventory management procedures. We evaluated S&T procedures related to maintaining an accurate laptop inventory, returning equipment upon employee exit or transfer, handling lost or stolen laptops, and the proper labeling of laptop computers. Also, we reviewed laptop physical security measures, and assessed the S&T laptop inventory by analyzing the integrity of inventory data and conducting verification tests on the 20 laptop computers included in our manual review. We did not evaluate the process for clearing or sanitizing S&T laptops before reuse or disposal, as the DHS Program Management Office performs this function.[14]

S&T, through support provided by DHS Infrastructure Operations, has procedures to ensure that newly ordered laptops are entered into the inventory, and that laptops are returned upon employee removal or transfer. S&T utilizes a contract to procure and provide managed services for laptops. The DHS CIO's Program Management Office manages all equipment for this contract. S&T orders new equipment through the Program Management Office, which receives all new laptops and scans them into an inventory control system. The laptops are then shipped to S&T Headquarters, where they are scanned again and listed in the inventory as assigned to S&T. When a laptop is assigned to a user, a hand-receipt is completed and the laptop is once again scanned and the user's information (name, office location, phone, etc.) is entered into the inventory database. Upon employee exit or transfer, laptops are turned in to the S&T CIO office, rescanned, and annotated as being unassigned.

S&T has not implemented several critical inventory management controls. Specifically, S&T has not:

- Conducted adequate inventory reviews. Periodic inventory reviews are not conducted by the contractor, which maintains the laptop inventory, because this task was not included in the service level agreement

[14] Clearing requires overwriting all areas of the hard drive three times and then verifying the procedure by randomly re-reading the overwritten information. Sanitizing a hard drive requires incineration or degaussing (see approved degausser list at http://www. nsa.gov/ia/government/mdg.cfm).

negotiated by DHS as part of the contract. S&T has implemented a manual process to conduct ad hoc reviews approximately every quarter. However, S&T does not have a process to update the inventory based on the results of these reviews, because the component is limited to read-only access to the inventory database. Further, these reviews do not include an examination of installed software.

- Maintained an accurate inventory. For the 20 laptops included in our manual reviews, two loaner laptops were not listed on the inventory, and one laptop was listed under one individual's name but assigned to another. According to the S&T CIO, the inaccuracies in the inventory are the result of S&T not being able to ensure that the results of its inventory reviews are used to update the inventory database.
- Implemented sufficient physical security controls for unassigned laptops. [redacted]
- Appropriately labeled sensitive but unclassified laptops. S&T's laptops do not have a label affixed stating: "This machine is not authorized for classified processing." According to the S&T CIO, DHS Infrastructure Operations should have affixed the stickers.
- Established procedures to ensure that the written approval of the office director is obtained before a laptop is taken overseas. The S&T CIO stated that her office has recommended procedures for enforcing this policy, but these procedures are under consideration by S&T management.

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.[15] 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. Further, DHS policy requires that the approval of the office director be obtained prior to a laptop being taken overseas, and that all laptop computers not authorized to process classified information have a label affixed

[15] 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.

indicating, “This machine is not authorized for classified processing.” As a result of the weaknesses in S&T’s inventory procedures, there is greater risk that laptop computers will not be configured and secured adequately, and access to classified and sensitive information may not be restricted appropriately.

Recommendations

To secure S&T data stored on government-issued laptop computers, we are recommending that the Under Secretary for S&T 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 S&T.
2. Ensure that the updated model system is correctly implemented on all S&T laptop computers.
3. Develop procedures to ensure that all S&T laptops are patched and updated in a timely manner, including loaner and secondary unit laptops, as well as all government-issued computers.
4. Implement appropriate inventory management controls, including effective inventory reviews, physical security controls, and classification labeling.

Management Comments and OIG Analysis

S&T concurs with recommendation 1. S&T has begun implementing corrective action plans for the laptop vulnerabilities we identified. Specifically, S&T and the DHS Office of the Chief Information Officer (OCIO) will [redacted]. However, S&T does not accept the DHS OCIO’s plan to employ [redacted]. Nonetheless, the DHS OCIO has outlined a nine-month timeframe for full [redacted] and will assess alternative means to support the S&T requirement to have [redacted]

We accept S&T and the DHS OCIO's response to implement corrective action plans for the existing vulnerabilities in the standard configuration of laptop computers.

S&T concurs with recommendation 2. S&T has begun implementing corrective action plans to ensure that an updated model system is correctly implemented on the S&T laptop computers we tested. Specifically, S&T and the DHS OCIO have re-imaged the laptops assigned to the [redacted] as well as certain laptops at the [redacted]. In addition, S&T and the DHS OCIO have taken or plan to take corrective action to address identified vulnerabilities, including ensuring that [redacted] In addition, the DHS LAN A security team will conduct periodic scans for the S&T directorate to confirm that vulnerabilities have been remediated.

We accept, in part, S&T and the DHS OCIO's response to implement corrective action plans. We appreciate the steps taken to remediate this recommendation. However, we believe the intent of this recommendation has not been fully addressed. The discrepancies noted for this finding demonstrate how the model system has not been implemented uniformly. We maintain that the model system, once the discrepancies in finding 1 are remedied, be applied to all S&T laptop computers, not just the laptops tested during our review.

S&T concurs with recommendation 3. S&T has patched and updated its laptop computers with the standard DHS patch management software. The DHS OCIO is evaluating a process to effectively manage and track patches in accordance with CSIRC.

We agree that the action S&T and the DHS OCIO have taken and plan to take satisfies the intent of the recommendation.

S&T concurs with recommendation 4. S&T has taken corrective action regarding physical security [redacted] In addition, S&T and the DHS OCIO have begun implementing corrective action plans for classification labeling and for establishing approval procedures for employees taking laptops outside the United States. The DHS OCIO indicated that inventory sweeps, bar coding, and ongoing scanning are conducted as items are deployed or moved. S&T will request that the DHS OCIO conduct quarterly inventory reviews and use the results to update S&T’s inventory in the DHS headquarters inventory management system.

We accept S&T and the DHS OCIO’s response for physical security, classification labeling, and procedures for approving overseas travel with laptop computers. S&T’s response did not indicate that the inventory reviews would include an examination of installed software. Although S&T and the DHS OCIO will conduct periodic inventories, the response does not indicate whether these reviews will include an assessment on the type of software installed on its assets. We maintain that S&T and the DHS OCIO should conduct inventory reviews, at least semiannually, of all equipment and software to ensure that only government-licensed software and equipment are being used and that systems are appropriately labeled.

Purpose, Scope, and Methodology

The objective of this audit was to determine whether S&T had implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptop computers. Specifically, we determined whether S&T 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 but unclassified 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 S&T laptop computer inventory as of November 2005. Based on our review of the laptop inventory, we selected the following S&T sites for testing:

S&T Testing Locations and Laptop Computers

Location	*50 Laptops*	
	User Assigned	*Loaner/ Shared*
S&T Headquarters, Washington, DC	**20**	**9**
BioWatch Facility, Alexandria, VA	**11**	**0**
Counter-MANPADS Facility, Arlington, VA	**8**	**2**

In addition, we performed extensive manual security parameter checks on select laptop computers to confirm the results of our scans and identify any additional security weaknesses. 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 S&T headquarters in Washington, DC; S&T field offices in Alexandria and Arlington, VA; and, the OIG's ATL.[16] We conducted our audit from December 2005 through January 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 F.

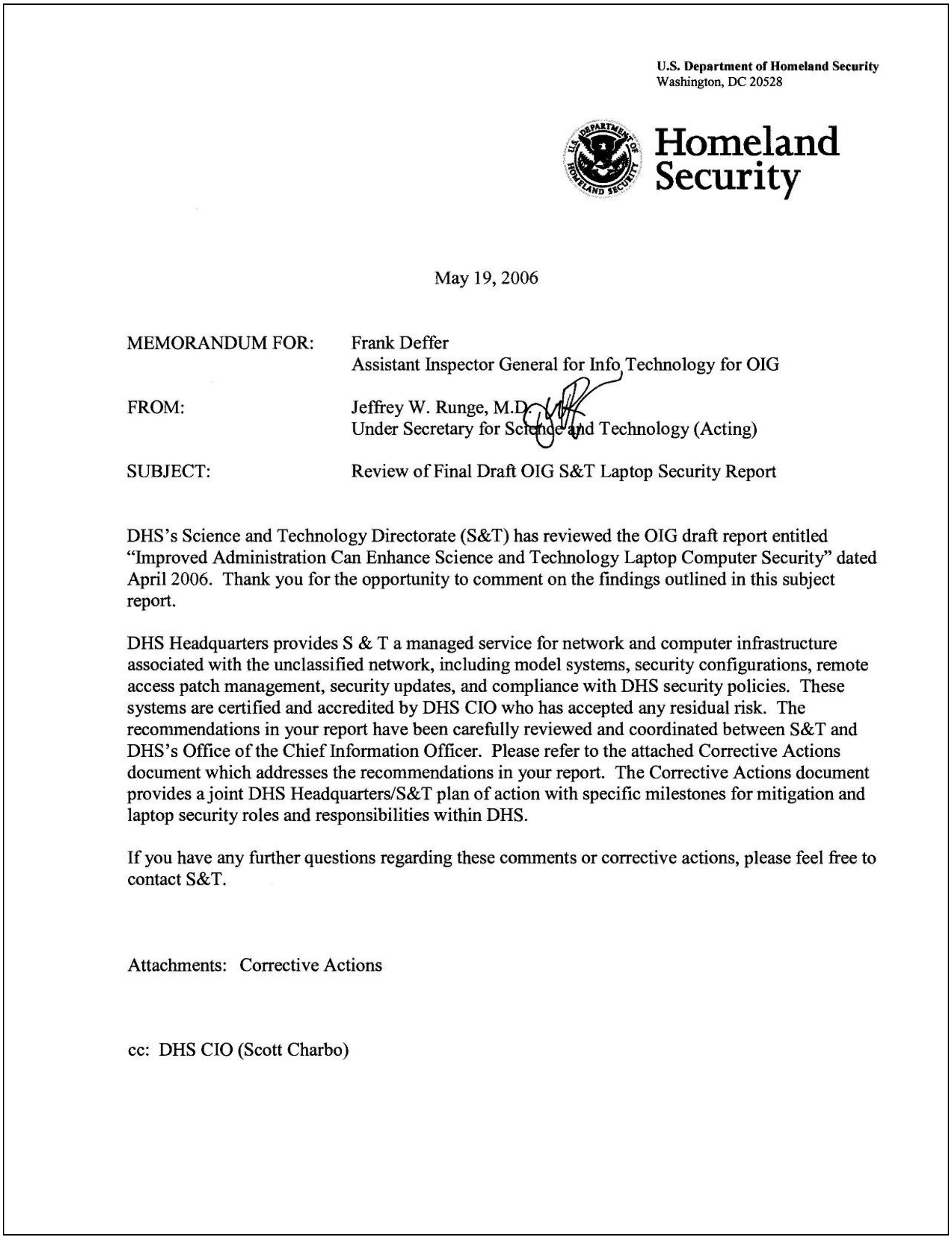
Our principal points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits at (202) 254-4100 and Edward G. Coleman, Director, Information Security Audit Division at (202) 254-5444.

[16] 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:

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted]



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

Homeland
Security

May 19, 2006

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Info Technology for OIG

FROM: Jeffrey W. Runge, M.D.
Under Secretary for Science and Technology (Acting)

SUBJECT: Review of Final Draft OIG S&T Laptop Security Report

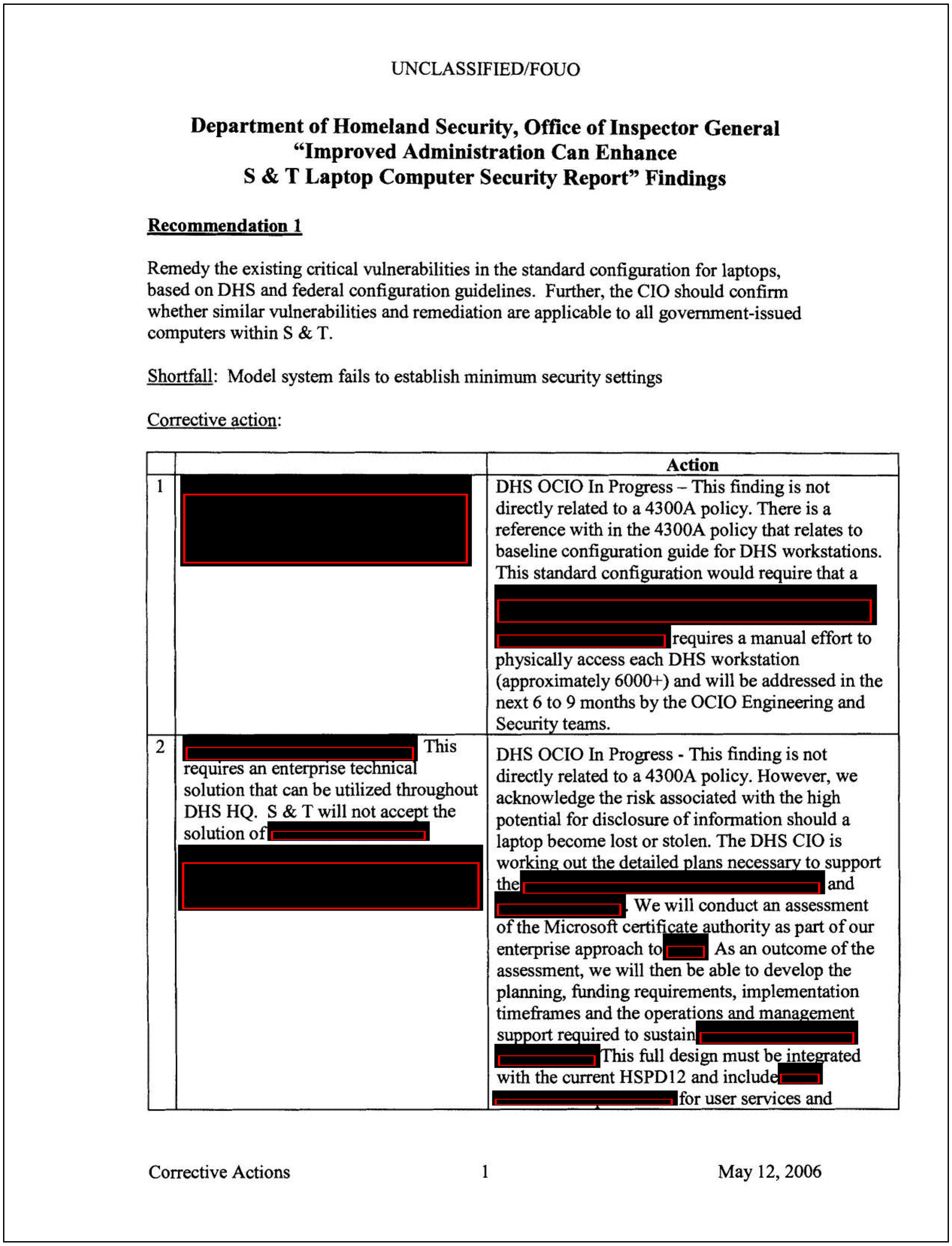
DHS's Science and Technology Directorate (S&T) has reviewed the OIG draft report entitled "Improved Administration Can Enhance Science and Technology Laptop Computer Security" dated April 2006. Thank you for the opportunity to comment on the findings outlined in this subject report.

DHS Headquarters provides S & T a managed service for network and computer infrastructure associated with the unclassified network, including model systems, security configurations, remote access patch management, security updates, and compliance with DHS security policies. These systems are certified and accredited by DHS CIO who has accepted any residual risk. The recommendations in your report have been carefully reviewed and coordinated between S&T and DHS's Office of the Chief Information Officer. Please refer to the attached Corrective Actions document which addresses the recommendations in your report. The Corrective Actions document provides a joint DHS Headquarters/S&T plan of action with specific milestones for mitigation and laptop security roles and responsibilities within DHS.

If you have any further questions regarding these comments or corrective actions, please feel free to contact S&T.

Attachments: Corrective Actions

cc: DHS CIO (Scott Charbo)



UNCLASSIFIED/FOUO

Department of Homeland Security, Office of Inspector General "Improved Administration Can Enhance S & T Laptop Computer Security Report" Findings

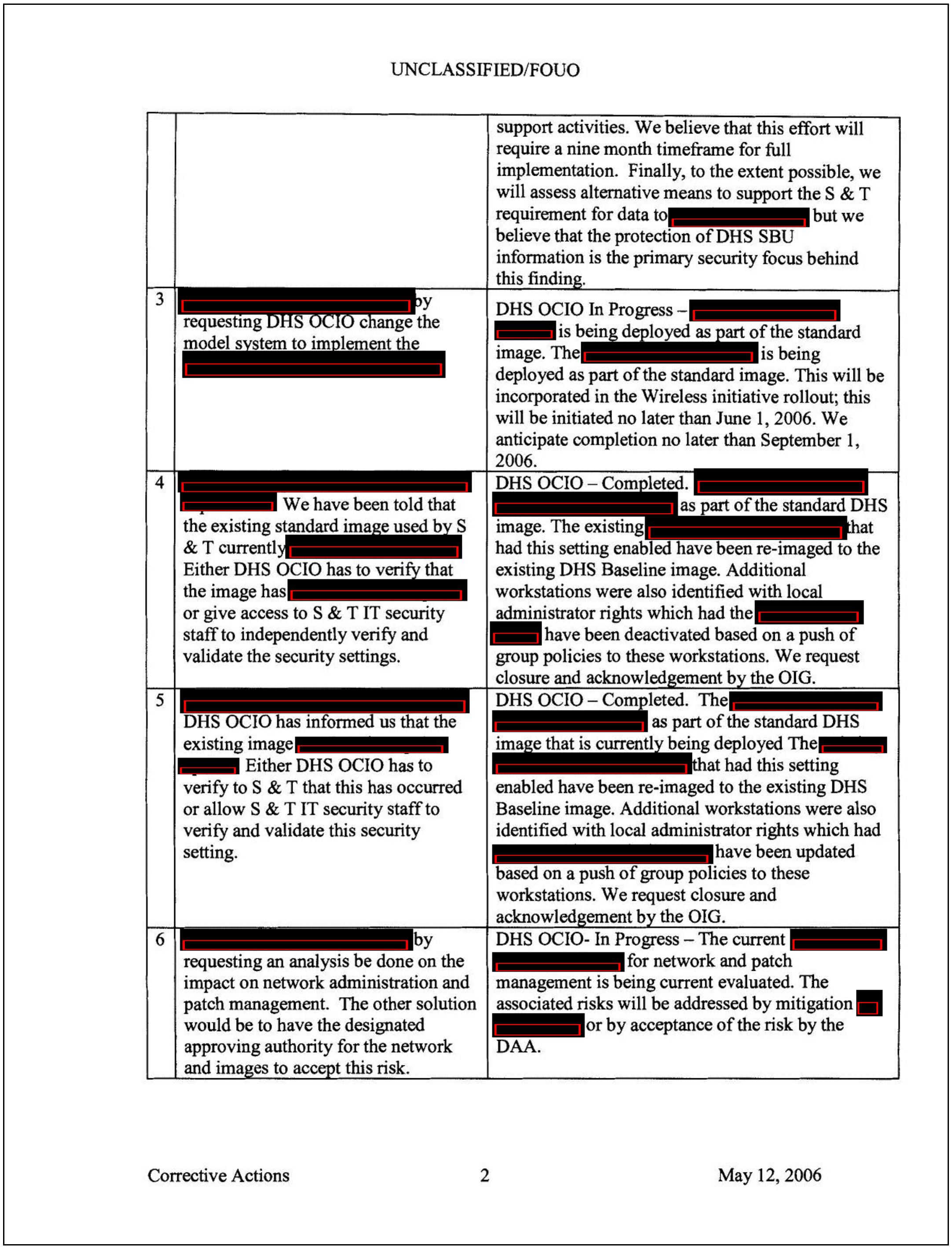
Recommendation 1

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 S & T.

Shortfall: Model system fails to establish minimum security settings

Corrective action:

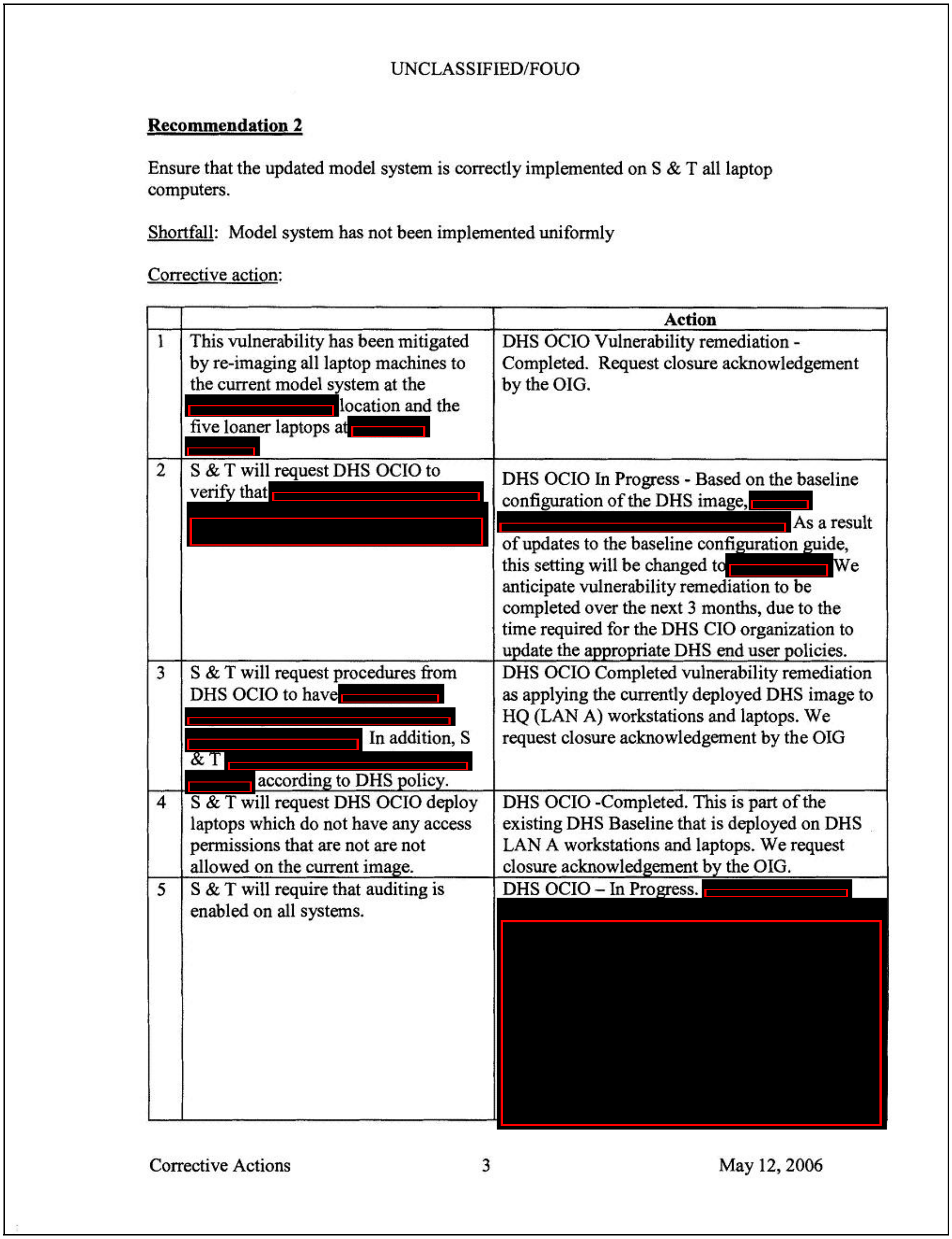
		Action
1	[redacted]	DHS OCIO In Progress – This finding is not directly related to a 4300A policy. There is a reference with in the 4300A policy that relates to baseline configuration guide for DHS workstations. This standard configuration would require that a [redacted] requires a manual effort to physically access each DHS workstation (approximately 6000+) and will be addressed in the next 6 to 9 months by the OCIO Engineering and Security teams.
2	[redacted] This requires an enterprise technical solution that can be utilized throughout DHS HQ. S & T will not accept the solution of [redacted] [redacted]	DHS OCIO In Progress - This finding is not directly related to a 4300A policy. However, we acknowledge the risk associated with the high potential for disclosure of information should a laptop become lost or stolen. The DHS CIO is working out the detailed plans necessary to support the [redacted] and [redacted]. We will conduct an assessment of the Microsoft certificate authority as part of our enterprise approach to [redacted] As an outcome of the assessment, we will then be able to develop the planning, funding requirements, implementation timeframes and the operations and management support required to sustain [redacted] This full design must be integrated with the current HSPD12 and include [redacted] [redacted] for user services and



UNCLASSIFIED/FOUO

		support activities. We believe that this effort will require a nine month timeframe for full implementation. Finally, to the extent possible, we will assess alternative means to support the S & T requirement for data to [redacted] but we believe that the protection of DHS SBU information is the primary security focus behind this finding.
3	[redacted] by requesting DHS OCIO change the model system to implement the [redacted]	DHS OCIO In Progress – [redacted] [redacted] is being deployed as part of the standard image. The [redacted] is being deployed as part of the standard image. This will be incorporated in the Wireless initiative rollout; this will be initiated no later than June 1, 2006. We anticipate completion no later than September 1, 2006.
4	[redacted] [redacted] We have been told that the existing standard image used by S & T currently [redacted] Either DHS OCIO has to verify that the image has [redacted] or give access to S & T IT security staff to independently verify and validate the security settings.	DHS OCIO – Completed. [redacted] [redacted] as part of the standard DHS image. The existing [redacted] that had this setting enabled have been re-imaged to the existing DHS Baseline image. Additional workstations were also identified with local administrator rights which had the [redacted] [redacted] have been deactivated based on a push of group policies to these workstations. We request closure and acknowledgement by the OIG.
5	[redacted] DHS OCIO has informed us that the existing image [redacted] [redacted] Either DHS OCIO has to verify to S & T that this has occurred or allow S & T IT security staff to verify and validate this security setting.	DHS OCIO – Completed. The [redacted] [redacted] as part of the standard DHS image that is currently being deployed The [redacted] [redacted] that had this setting enabled have been re-imaged to the existing DHS Baseline image. Additional workstations were also identified with local administrator rights which had [redacted] have been updated based on a push of group policies to these workstations. We request closure and acknowledgement by the OIG.
6	[redacted] by requesting an analysis be done on the impact on network administration and patch management. The other solution would be to have the designated approving authority for the network and images to accept this risk.	DHS OCIO- In Progress – The current [redacted] [redacted] for network and patch management is being current evaluated. The associated risks will be addressed by mitigation [redacted] [redacted] or by acceptance of the risk by the DAA.

Corrective Actions 2 May 12, 2006



UNCLASSIFIED/FOUO

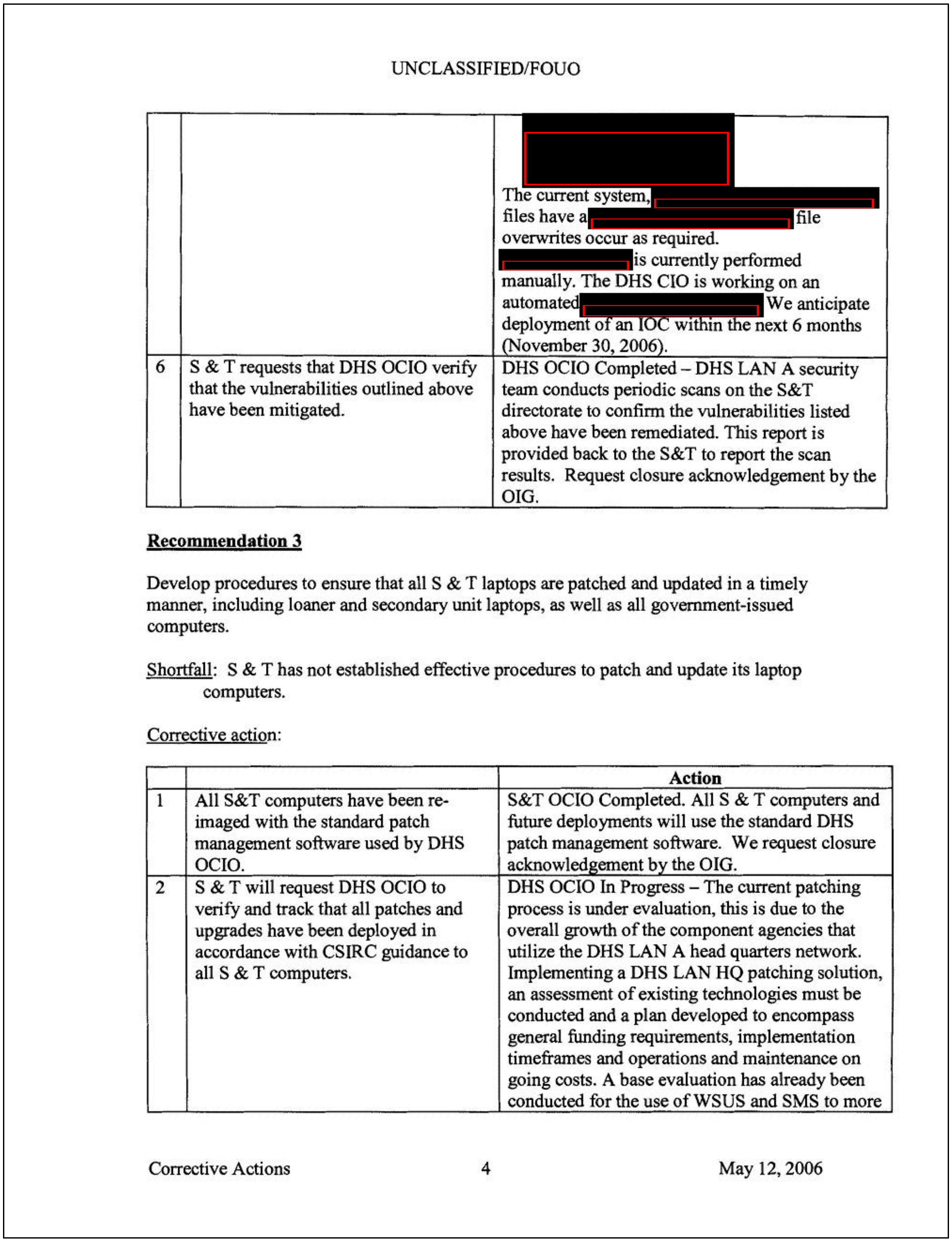
Recommendation 2

Ensure that the updated model system is correctly implemented on S & T all laptop computers.

Shortfall: Model system has not been implemented uniformly

Corrective action:

		Action
1	This vulnerability has been mitigated by re-imaging all laptop machines to the current model system at the [redacted] location and the five loaner laptops at [redacted]	DHS OCIO Vulnerability remediation - Completed. Request closure acknowledgement by the OIG.
2	S & T will request DHS OCIO to verify that [redacted]	DHS OCIO In Progress - Based on the baseline configuration of the DHS image, [redacted] As a result of updates to the baseline configuration guide, this setting will be changed to [redacted] We anticipate vulnerability remediation to be completed over the next 3 months, due to the time required for the DHS CIO organization to update the appropriate DHS end user policies.
3	S & T will request procedures from DHS OCIO to have [redacted] In addition, S & T [redacted] according to DHS policy.	DHS OCIO Completed vulnerability remediation as applying the currently deployed DHS image to HQ (LAN A) workstations and laptops. We request closure acknowledgement by the OIG
4	S & T will request DHS OCIO deploy laptops which do not have any access permissions that are not are not allowed on the current image.	DHS OCIO -Completed. This is part of the existing DHS Baseline that is deployed on DHS LAN A workstations and laptops. We request closure acknowledgement by the OIG.
5	S & T will require that auditing is enabled on all systems.	DHS OCIO – In Progress. [redacted]



		[redacted] The current system, [redacted] files have a [redacted] file overwrites occur as required. [redacted] is currently performed manually. The DHS CIO is working on an automated [redacted] We anticipate deployment of an IOC within the next 6 months (November 30, 2006).
6	S & T requests that DHS OCIO verify that the vulnerabilities outlined above have been mitigated.	DHS OCIO Completed – DHS LAN A security team conducts periodic scans on the S&T directorate to confirm the vulnerabilities listed above have been remediated. This report is provided back to the S&T to report the scan results. Request closure acknowledgement by the OIG.

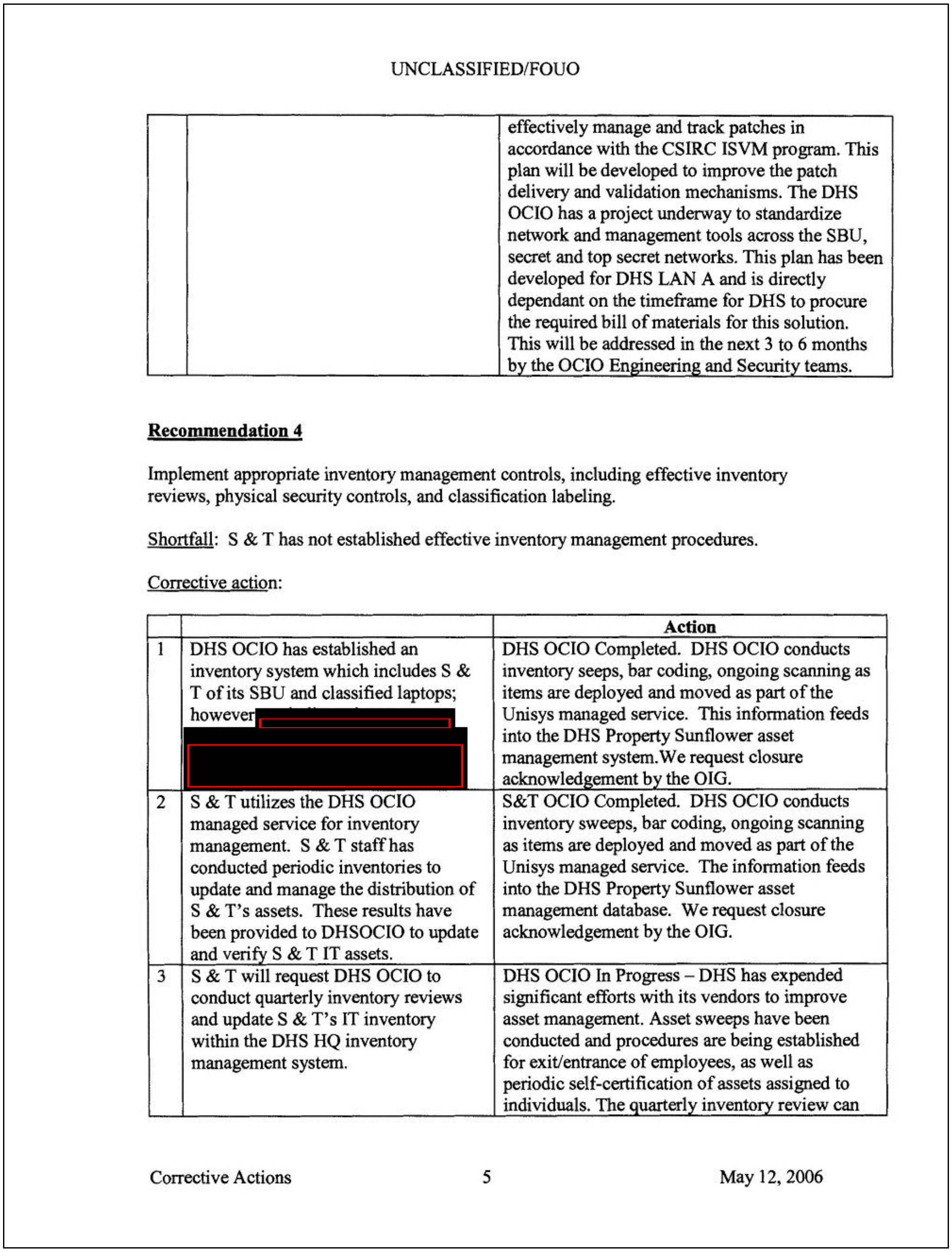
Recommendation 3

Develop procedures to ensure that all S & T laptops are patched and updated in a timely manner, including loaner and secondary unit laptops, as well as all government-issued computers.

Shortfall: S & T has not established effective procedures to patch and update its laptop computers.

Corrective action:

		Action
1	All S&T computers have been re-imaged with the standard patch management software used by DHS OCIO.	S&T OCIO Completed. All S & T computers and future deployments will use the standard DHS patch management software. We request closure acknowledgement by the OIG.
2	S & T will request DHS OCIO to verify and track that all patches and upgrades have been deployed in accordance with CSIRC guidance to all S & T computers.	DHS OCIO In Progress – The current patching process is under evaluation, this is due to the overall growth of the component agencies that utilize the DHS LAN A head quarters network. Implementing a DHS LAN HQ patching solution, an assessment of existing technologies must be conducted and a plan developed to encompass general funding requirements, implementation timeframes and operations and maintenance on going costs. A base evaluation has already been conducted for the use of WSUS and SMS to more



		effectively manage and track patches in accordance with the CSIRC ISVM program. This plan will be developed to improve the patch delivery and validation mechanisms. The DHS OCIO has a project underway to standardize network and management tools across the SBU, secret and top secret networks. This plan has been developed for DHS LAN A and is directly dependant on the timeframe for DHS to procure the required bill of materials for this solution. This will be addressed in the next 3 to 6 months by the OCIO Engineering and Security teams.

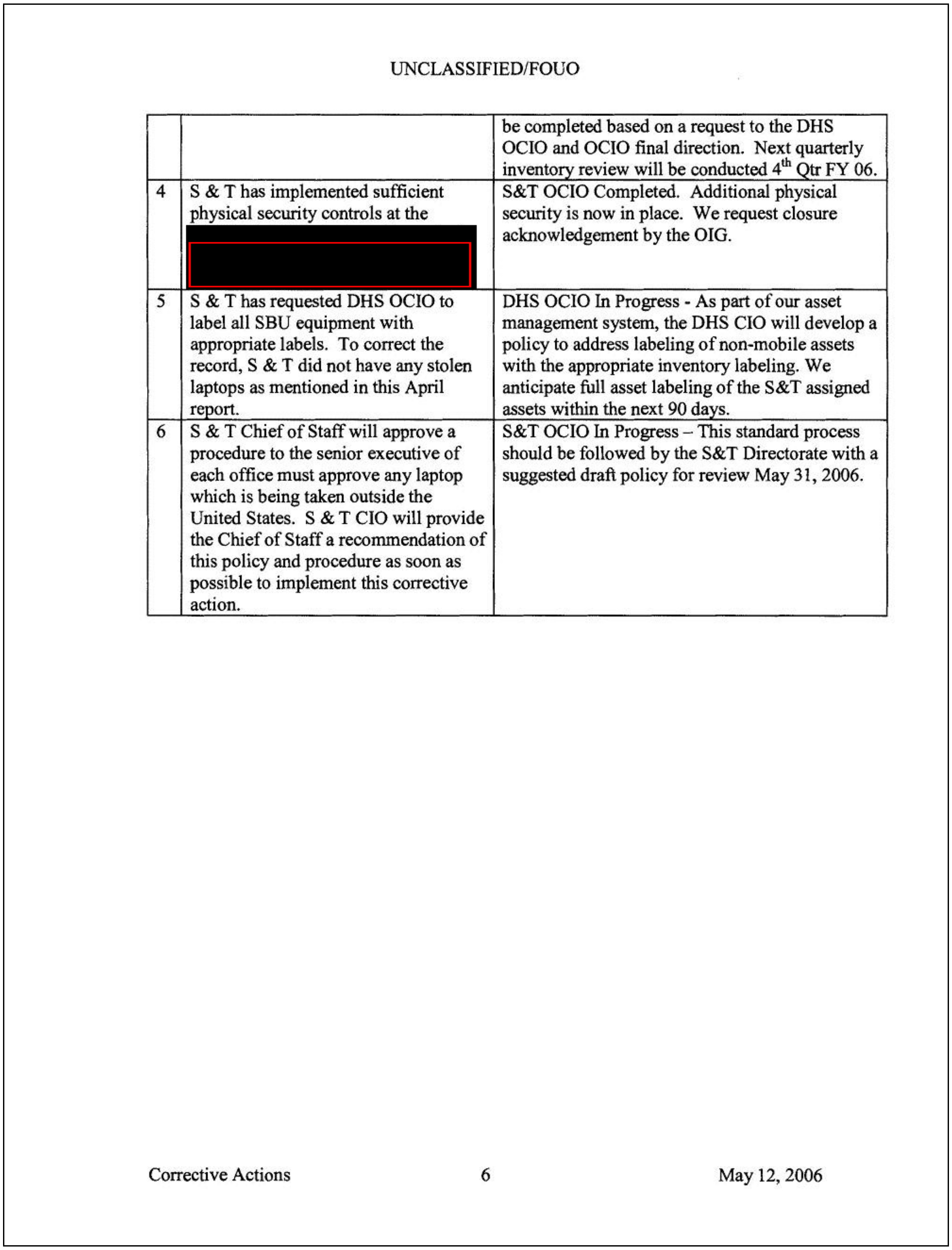
Recommendation 4

Implement appropriate inventory management controls, including effective inventory reviews, physical security controls, and classification labeling.

Shortfall: S & T has not established effective inventory management procedures.

Corrective action:

		Action
1	DHS OCIO has established an inventory system which includes S & T of its SBU and classified laptops; however [redacted]	DHS OCIO Completed. DHS OCIO conducts inventory seeps, bar coding, ongoing scanning as items are deployed and moved as part of the Unisys managed service. This information feeds into the DHS Property Sunflower asset management system.We request closure acknowledgement by the OIG.
2	S & T utilizes the DHS OCIO managed service for inventory management. S & T staff has conducted periodic inventories to update and manage the distribution of S & T's assets. These results have been provided to DHSOCIO to update and verify S & T IT assets.	S&T OCIO Completed. DHS OCIO conducts inventory sweeps, bar coding, ongoing scanning as items are deployed and moved as part of the Unisys managed service. The information feeds into the DHS Property Sunflower asset management database. We request closure acknowledgement by the OIG.
3	S & T will request DHS OCIO to conduct quarterly inventory reviews and update S & T's IT inventory within the DHS HQ inventory management system.	DHS OCIO In Progress – DHS has expended significant efforts with its vendors to improve asset management. Asset sweeps have been conducted and procedures are being established for exit/entrance of employees, as well as periodic self-certification of assets assigned to individuals. The quarterly inventory review can



		be completed based on a request to the DHS OCIO and OCIO final direction. Next quarterly inventory review will be conducted 4th Qtr FY 06.
4	S & T has implemented sufficient physical security controls at the [redacted]	S&T OCIO Completed. Additional physical security is now in place. We request closure acknowledgement by the OIG.
5	S & T has requested DHS OCIO to label all SBU equipment with appropriate labels. To correct the record, S & T did not have any stolen laptops as mentioned in this April report.	DHS OCIO In Progress - As part of our asset management system, the DHS CIO will develop a policy to address labeling of non-mobile assets with the appropriate inventory labeling. We anticipate full asset labeling of the S&T assigned assets within the next 90 days.
6	S & T Chief of Staff will approve a procedure to the senior executive of each office must approve any laptop which is being taken outside the United States. S & T CIO will provide the Chief of Staff a recommendation of this policy and procedure as soon as possible to implement this corrective action.	S&T OCIO In Progress – This standard process should be followed by the S&T Directorate with a suggested draft policy for review May 31, 2006.

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.[18] 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 OMB's FISMA reporting requirements, we evaluated the effectiveness of the information security program and practices as implemented for DHS Infrastructure Operations LAN A system, which incorporates S&T's laptop and desktop computers, to determine whether DHS continues to make progress in implementing its agency-wide information security program. We collected information relative to certification and accreditation (C&A), system impact level determination, NIST SP 800-26 annual assessment, assessment of E-authentication risks, specialized security training, and POA&Ms.[19]

Our evaluation of the DHS Infrastructure Operations LAN A system shows that the component has implemented key security management practices into its information security program, as required by FISMA.

[18] The E-Government Act of 2002 (Public Law 107-347), signed into law on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.

[19] As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, and NIST 800-63, *Electronic Authentication Guideline.*

Appendix C
FISMA Metrics

Table 3: FISMA Compliance Metrics

FISMA Reporting Requirements	Yes/No	Notes
Does the system have a complete and current C&A?	Yes	The DHS Infrastructure Operations LAN A system was granted authority to operate on July 8, 2005.
Has the system's impact level been determined according to FIPS-199 criteria?	Yes	The system impact levels were determined to be Moderate for Confidentiality, Integrity, and Availability.
Does the system have a complete and current NIST SP 800-26 annual assessment?	Yes	A self-assessment was completed on June 30, 2005.
Does the system have a security plan and risk assessment?	Yes	A system security plan was completed on dated July 4, 2005 and a risk assessment on June 30, 2005.
Were the system's security controls tested and evaluated in the last year?	Yes	A security test and evaluation (ST&E) was completed on June 30, 2005.
Has a system contingency plan been established and tested?	Yes	A system contingency plan has been completed and was tested on April 25, 2005.
Has an assessment of E-Authentication risk been performed for the system?	N/A	Remote users do not authenticate to the S&T Network for the purposes of conducting government business electronically.
Have personnel with significant security responsibilities obtained specialized security training?	Yes	As of February 15, 2006, 10 of 12 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	According to DHS Infrastructure Operations, a privacy impact assessment is not applicable to this system.
Are POA&Ms created and managed for the system?	Yes	As of February 15, 2006, 27 POA&Ms were entered into the DHS FISMA reporting system.

Source: OIG table based on interviews with S&T personnel and analysis of database documentation.

Appendix D
Major Contributors to this Report

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

Advanced Technology Division
Chris Hablas, Senior Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary, Science and Technology
Chief Information Officer
Chief Information Security Officer
Assistant Secretary for Legislative and Intergovernmental Affairs
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
DHS GAO OIG Audit Liaison
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison
Audit Liaison, Science and Technology

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.