Department of Homeland Security

Office of Inspector General

U.S. Citizenship and Immigration Services' Laptop Safeguards Need Improvements

OIG-12-83

May 2012

Office of Inspector General

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

Homeland Security

May 4, 2012

Preface

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

This report addresses the strengths and weaknesses of the U.S. Citizenship and Immigration Services program to safeguard its laptops. This report is based on interviews with employees and officials of relevant agencies and institutions, direct observations, 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. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
Directive 4300A	DHS Sensitive Systems Policy Directive 4300A
OIG	Office of Inspector General
OIT	Office of Information Technology
SAMS	Sunflower Asset Management System
WSUS	Windows Server Update Services
USCIS	U.S. Citizenship and Immigration Services

Executive Summary

We conducted an audit of laptop security at U.S. Citizenship and Immigration Services (USCIS). Our audit objective was to determine whether USCIS has implemented an effective program to safeguard its laptop computers and the information they contain.

We reviewed inventory information and performed onsite inspections in USCIS offices in Washington, DC, and in a contractor's New Jersey shipping facility. We also interviewed departmental staff and examined the operating systems and encryption software on a statistically valid, random sample of laptops.

USCIS' laptop controls did not sufficiently safeguard its laptops from loss or theft and did not protect the data on the laptops from disclosure. Specifically, USCIS did not have an accurate and complete inventory of its laptops, nor were inventory data reported accurately and consistently in electronic databases. Additionally, many laptops were not assigned to specific users. USCIS also did not provide adequate physical security for its laptops. Finally, not all of USCIS' laptops were using the latest encryption software or operating systems and associated service packs.

We are recommending that USCIS take steps to improve its laptop inventory and configuration management processes. Specifically, USCIS property custodians should enter laptop data consistently into its property management system, and record laptops provided to contractors as government-furnished equipment. Additionally, we are recommending that USCIS ensure that it has installed the latest operating systems and encryption software on its laptops. Our last recommendation is that USCIS develop procedures to ensure that users' laptops are connected to its network on a monthly basis so that software updates may be applied.

Background

USCIS has more than 18,000 employees and contractors working at 250 offices around the world. It uses laptop computers to help fulfill its mission of overseeing lawful immigration to the United States. Additionally, USCIS contractors are issued laptops as government-furnished equipment to access USCIS systems.

The mobility of laptops increases workforce productivity. However, this same mobility increases the risk of theft and unauthorized data disclosure. The increased risk of theft of laptop computers is associated with both cost and security. For example, replacing the hardware and restoring the information is costly. Additionally, when laptops are stolen, there is a security risk of data disclosure.

A USCIS property custodian takes possession of each incoming laptop and enters its information into the Department of Homeland Security's (DHS) Sunflower Asset Management System (SAMS), which USCIS uses to track and maintain its inventory electronically. The property custodian, using SAMS, then assigns the laptop to a USCIS employee or contractor. A USCIS Desktop Server Management employee customizes the laptop for that specific location, including manually entering the computer name into the laptop's system properties. This internal computer name includes the location and barcode number. As of October 20, 2011, USCIS had 6,659 laptops recorded in SAMS.

USCIS has additional processes to safeguard its laptops. For example, USCIS performs an annual wall-to-wall, floor-to-ceiling inventory of its assets, including laptops, to verify the accuracy of data in SAMS. USCIS also uses configuration management software, Windows Server Update Services (WSUS), to provide laptops with authorized Microsoft systems and software updates.

USCIS follows DHS policy for safeguarding laptops, found in *DHS Sensitive Systems Policy Directive 4300A*, Version 9.0, October 11, 2011 (Directive 4300A). Directive 4300A outlines policies for operational, technical, and management controls necessary to ensure confidentiality, integrity, availability, authenticity, and nonrepudiation in DHS' information technology infrastructure and operations.

Results of Audit

USCIS Needs To Improve Its Laptop Inventory Management Process

USCIS did not have an accurate inventory of its laptops. Specifically, property custodians did not consistently enter laptop data into the property management system, and data in different systems did not always agree. Furthermore, not all laptops were assigned to specific users, and USCIS did not adequately track which laptops were provided to contractors. Finally, USCIS did not enhance physical security controls by providing cables and locks for laptops. These deficiencies increased the risk of loss or theft of USCIS laptops.

Inventory Is Inaccurate and Needs Updating

USCIS uses SAMS to maintain its inventory of assets such as laptops. However, USCIS staff did not always adhere to published guidance when entering laptop information into SAMS, which led to inconsistent and unreliable information in the system. Without reliable information in SAMS, USCIS cannot locate all of its laptops, increasing the risk that they could be lost or stolen.

The inconsistent laptop data entered in SAMS made it more difficult to determine a laptop's user and location. USCIS property custodians sometimes entered the user's name in other data fields, such as the "Comment" field. During our site visit to one Washington, DC, facility, USCIS staff were not able to physically locate all the laptops that were listed in SAMS as being in that facility. For several of these laptops, the SAMS user name was "Unassigned."

Additionally, USCIS was unable to provide us with the number of laptops that had been provided initially to contractors as government-furnished equipment. Specifically, USCIS did not have a consistent method for identifying in SAMS which laptops were assigned to contractors. For example, some USCIS property custodians denoted the laptop as government-furnished equipment by entering the contractor's name in the "Steward" field.

According to the *USCIS Personal Property Management Instruction Handbook, USCIS IHB 119-002-01,*

> Equipment purchased by the government for use by a contractor is normally received through the acquisition

> channels and maintained in their approved system of record or as an agreement asset in SAMS.

According to the USCIS Office of Information Technology (OIT) *End User Services Division Personal Property Handbook*, December 2010,

> Ensure all OIT employees are entered into Sunflower as users for accounting purposes.
>
> GFE [government-furnished equipment] at a contractor site shall be entered into SAMS in the "Agreement Module."

Without accurate and reliable information, USCIS could not always use SAMS data to alert specific users that their laptop software was out of date. Specifically, laptop barcode data in SAMS did not always match the barcode data in WSUS, the system USCIS uses to provide Microsoft-related software updates to laptops. For example, 2.79 percent of our random sample of laptops had a WSUS computer name that did not match the barcode, and 6.27 percent had nonstandard internal computer names.[1]

According to USCIS staff, the lack of consistency in data entry was partly the result of the manual process for updating SAMS. However, during our fieldwork, we were informed that USCIS had begun to use hand-held barcode scanners to increase the accuracy of the SAMS inventory.

Physical Security Controls for Laptops Need Improvement

The mobility of laptops increases the risk of theft, and thus raises the risk of data disclosure; however, USCIS did not guard against theft by providing locks and cables to enhance physical security. Specifically, according to USCIS staff, locks and cables are provided only if the laptop's user requests these safeguards.

To prevent unauthorized individuals from removing laptops from unsecured facilities, USCIS should implement stronger physical security controls by issuing locking cables for its laptops. According to Directive 4300A,

[1] See appendix C, Statistical Analysis of USCIS Laptops.

> When unattended, laptop computers and other mobile computing devices shall be secured in locked offices, secured with a locking cable, or in a locked cabinet, or desk.

Recommendations

We recommend that the USCIS Chief Information Officer (CIO)

Recommendation #1: Ensure that laptop data are entered consistently into the USCIS property management system.

Recommendation #2: Develop a consistent process to record when laptops are initially provided as government-furnished equipment.

Recommendation #3: Provide appropriate locks and cables for laptops that may not be secured in locked offices, in a locked cabinet, or desk when unattended.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director of USCIS. We have included a copy of the comments in their entirety at appendix B. The Director of USCIS concurred with all five recommendations.

Recommendation #1

USCIS concurs with this recommendation. Beginning in this fiscal year, when verifying their annual inventory, USCIS Accountable Property Officers must certify that all equipment is assigned to an end user and all end users have signed receipts for all issued property.

OIG Analysis

The actions being taken satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCIS provides documentation to support that the planned corrective actions are completed.

Recommendation #2

USCIS concurs with this recommendation. USCIS will review agency policies and procedures governing the management of government-furnished equipment; ensure that all agency contracts include proper government-furnished equipment language; and standardize the process for recording, maintaining, reporting, and retrieving government-furnished equipment in accordance with Federal and Department standards.

OIG Analysis

The actions being taken satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCIS provides documentation to support that the planned corrective actions are completed.

Recommendation #3

USCIS concurs with this recommendation. USCIS will update current policies and instructions to specifically address laptop security, including the use of a lock and cable system when appropriate.

OIG Analysis

The actions being taken satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCIS provides documentation to support that the planned corrective actions are completed.

USCIS Needs To Improve Its Laptop Configuration Management Process

The USCIS configuration management process for providing software upgrades to its laptop computers needs improvement. Not all USCIS laptops had the latest encryption software, operating systems, or service packs. Furthermore, not all laptops received technical updates in a 30-day period. These deficiencies increased the risk that identified laptop vulnerabilities would not be resolved in a timely manner.

Encryption Software

The data on USCIS laptops were not always secured with the latest encryption software. In our random sample of 287 laptops shown in table 1, 8 percent were running older releases of the encryption software, and 4.5 percent either did not have encryption software installed or had inactive encryption software.

Table 1: Encryption Software Installed on Randomly Selected Laptops

Encryption Version	Number of Laptops	Sample Percentage
Laptops with older versions of encryption software	23	8.01%
Laptops with latest version of encryption software	149	51.92%
Not active/None	13	4.53%
Unknown*	102	35.54%
Total	287	100%

*USCIS did not provide encryption software information for laptops in storage, those that had not been assigned to staff, and those that were excessed or planned to be excessed.

According to USCIS staff, there were two situations where, by design, the standard USCIS encryption software was not active on the laptops: laptops used for classified processing and laptops used for training. USCIS staff noted that classified laptops do not use the standard encryption software, but rather the laptops used for classified processing conform to the rules of the classified system.

When encryption software was running on training laptops, if a user rebooted, someone would need to be called to log in past encryption before the class could continue. According to USCIS staff, the training laptops do not need to be encrypted because they do not leave DHS facilities.

According to Directive 4300A,

> Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption.…

Laptop computers that are not running the most recent encryption software might not be adequately protecting the security and privacy of USCIS data, potentially putting data confidentiality, integrity, and availability at risk.

Operating Systems and Associated Service Packs

Not all USCIS laptops were running the latest operating systems with the most up-to-date service packs. Table 2 indicates that

4 percent of the laptops in our random sample were not running the latest release of the operating system and service pack.

Table 2: Operating Systems Installed on Randomly Selected Laptops

Operating System and Service Pack	Number of Laptops	Sample Percentage
Older release	12	4.18%
Latest release	173	60.28%
Unknown*	102	35.54%
Total	287	100%

*USCIS did not provide operating system information for laptops in storage, those that had not yet been assigned to staff, or those that were either excessed or planned to be excessed.

According to Directive 4300A,

> Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

According to USCIS staff, when an unassigned laptop was assigned to a new user, USCIS provided that laptop with the latest approved operating system and service pack. However, USCIS was not adequately managing the automated software updates to ensure that the laptops in use were running the latest release of Microsoft Windows products. For example, USCIS used WSUS to provide Windows-related updates to its laptops, but did not use WSUS to upgrade operating systems or install associated service packs.

Furthermore, not all laptops received WSUS monthly updates, even though USCIS policy requires these updates. According to the USCIS Rules of Behavior that all users sign when issued a laptop, USCIS staff are required to connect their USCIS laptop computers to the USCIS network at least every 30 days to receive patches and antivirus updates. Laptop computers without the latest operating systems and associated service packs are at increased risk of malware due to inherent and unpatched vulnerabilities associated with the older system software. However, WSUS reports showed that only 2,530 laptops had been attached to the network in the previous 30 days. During the same period, the USCIS property management system contained an inventory of 6,659 laptops.

Recommendations

We recommend that the USCIS CIO:

Recommendation #4: Ensure that USCIS configuration management software and processes enable the updating of laptops' operating systems and encryption software with the latest releases.

Recommendation #5: Develop procedures to ensure that USCIS assigned laptops are connected to its network for system and software updates on a monthly basis.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director of USCIS. We have included a copy of the comments in their entirety at appendix B. The Director of USCIS concurred with all five recommendations.

Recommendation #4

USCIS concurs with this recommendation. USCIS will update its configuration management policies, procedures, and processes. USCIS also will develop a process to update non-networking laptops manually. Additionally, USCIS will update its procedures for naming laptops and will ensure that laptops are updated with the new name when they are turned in for reuse.

OIG Analysis

The actions being taken satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCIS provides documentation to support that the planned corrective actions are completed.

Recommendation #5

USCIS concurs with this recommendation. USCIS will develop a process to identify which laptops are configured to be connected to the network. Also, USCIS will ensure that these laptops automatically receive updates every month. For laptops not configured to be used on the network, USCIS will develop procedures to update those laptops manually. USCIS will also increase its communications to USCIS personnel concerning their responsibilities for properly maintaining their laptops.

OIG Analysis

The actions being taken satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCIS provides documentation to support that the planned corrective actions are completed.

The objective of our audit was to determine whether USCIS has implemented an effective program to protect the security and integrity of its laptop computers. Specifically, we—

- Determined whether the current process that USCIS has in place to maintain its inventory of laptops is adequate;

- Determined whether USCIS' current process of updating laptop images and security patches is adequate;

- Determined whether USCIS has a process to protect personally identifiable information stored on laptops; and

- Assessed whether USCIS follows appropriate procedures and takes appropriate corrective actions to address decommissioned, damaged, excessed, lost, or stolen laptops.

Our audit focused on the requirements outlined in Directive 4300A. We also reviewed component-specific guidance, including USCIS *Personal Property Management Handbook*, USCIS *Personal Property Physical Inventory Guidance*, USCIS Management Directive 144-001 *Board of Survey*, and the *USCIS Rules of Behavior* for users of Federal Government information technology resources.

We interviewed USCIS personnel, including property custodians, information technology specialists, personal property managers, and contractors. We also conducted a site visit of the contractor's New Jersey facility where USCIS laptops are received, configured, and then shipped to staff. Additionally, we performed site visits at two USCIS facilities in Washington, DC, to observe laptops at those locations. We also conducted a laptop sample to verify host names, operating systems, service packs, and encryption versions.

Our previous laptop security audits included onsite visits and the technical scanning of selected laptops.[2] However, our planning for this audit emphasized minimizing our impact on USCIS while expanding our scope to include a more representative sample of laptops. To that end, we selected a random sample of laptops from USCIS' complete laptop inventory. We then requested that USCIS staff provide screen prints from this sample showing each laptop's

[2] *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security (Redacted)*, OIG-07-50, June 2007.

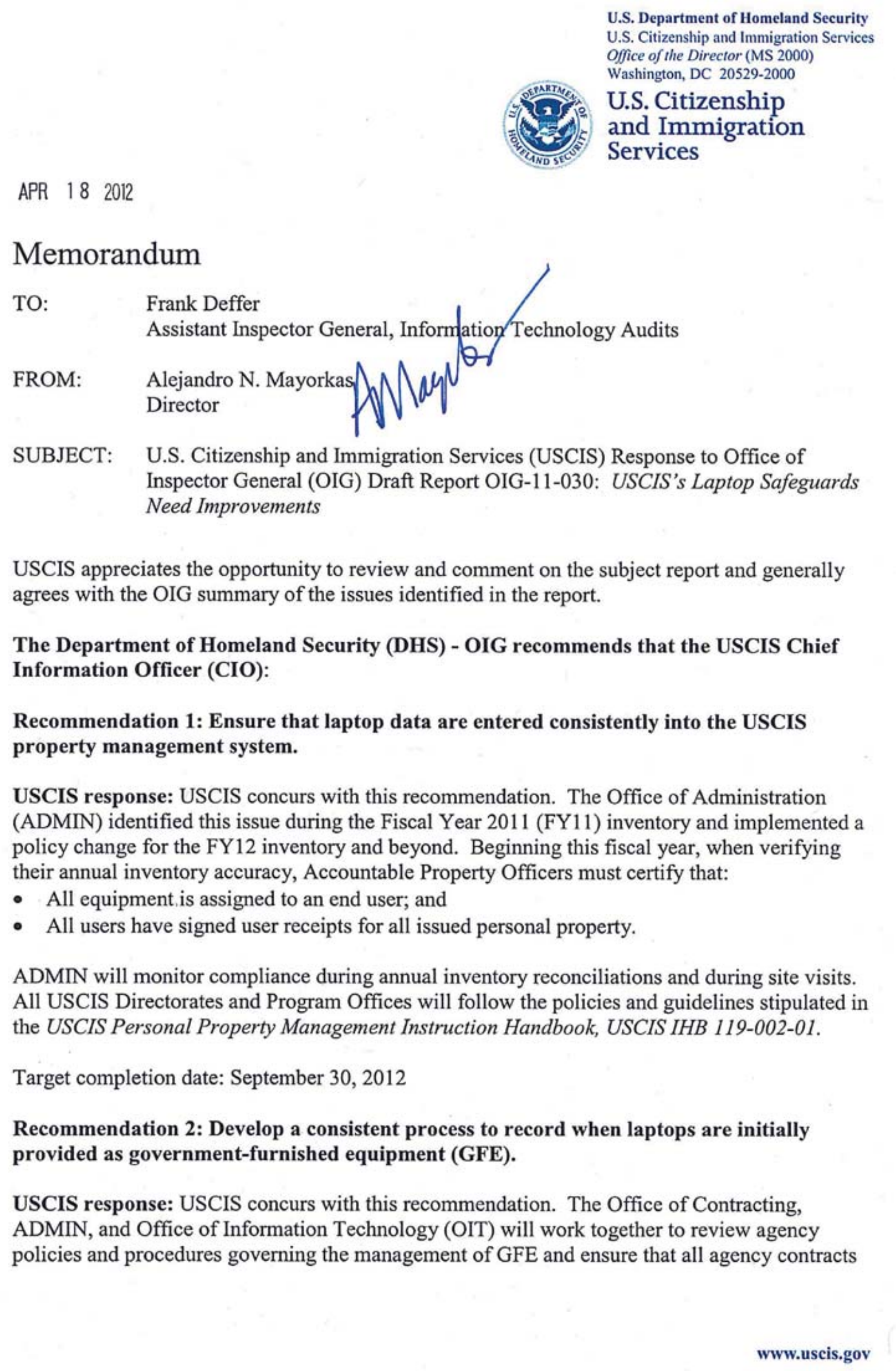
operating system information, computer name, and encryption software.

This methodology was intended to minimize the impact on users, but it had a greater impact on USCIS property custodians. For example, rather than focusing on the laptops in a few facilities, we requested information on laptops throughout USCIS' worldwide operations. This request required action from more property custodians. Additionally, several property custodians had to perform extra work, including tracking down the requested laptop and providing support to produce the screen prints. We are very appreciative of the work that USCIS staff performed to provide the requested information for this effort.

We conducted this audit between September 2011 and February 2012 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. We gave briefings and presentations to DHS staff concerning the results of our fieldwork and the information summarized in this report.

We appreciate the efforts of USCIS management and staff to provide the information and access necessary to accomplish this review. The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, (202) 254-4100, and Sharon Huiswoud, Director, Information Systems Division, (202) 254-5451. Major OIG contributors to the audit are identified in appendix D.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director (MS 2000)
Washington, DC 20529-2000

U.S. Citizenship
and Immigration
Services

APR 18 2012

Memorandum

TO: Frank Deffer
Assistant Inspector General, Information Technology Audits

FROM: Alejandro N. Mayorkas
Director

SUBJECT: U.S. Citizenship and Immigration Services (USCIS) Response to Office of Inspector General (OIG) Draft Report OIG-11-030: *USCIS's Laptop Safeguards Need Improvements*

USCIS appreciates the opportunity to review and comment on the subject report and generally agrees with the OIG summary of the issues identified in the report.

The Department of Homeland Security (DHS) - OIG recommends that the USCIS Chief Information Officer (CIO):

Recommendation 1: Ensure that laptop data are entered consistently into the USCIS property management system.

USCIS response: USCIS concurs with this recommendation. The Office of Administration (ADMIN) identified this issue during the Fiscal Year 2011 (FY11) inventory and implemented a policy change for the FY12 inventory and beyond. Beginning this fiscal year, when verifying their annual inventory accuracy, Accountable Property Officers must certify that:

- All equipment is assigned to an end user; and
- All users have signed user receipts for all issued personal property.

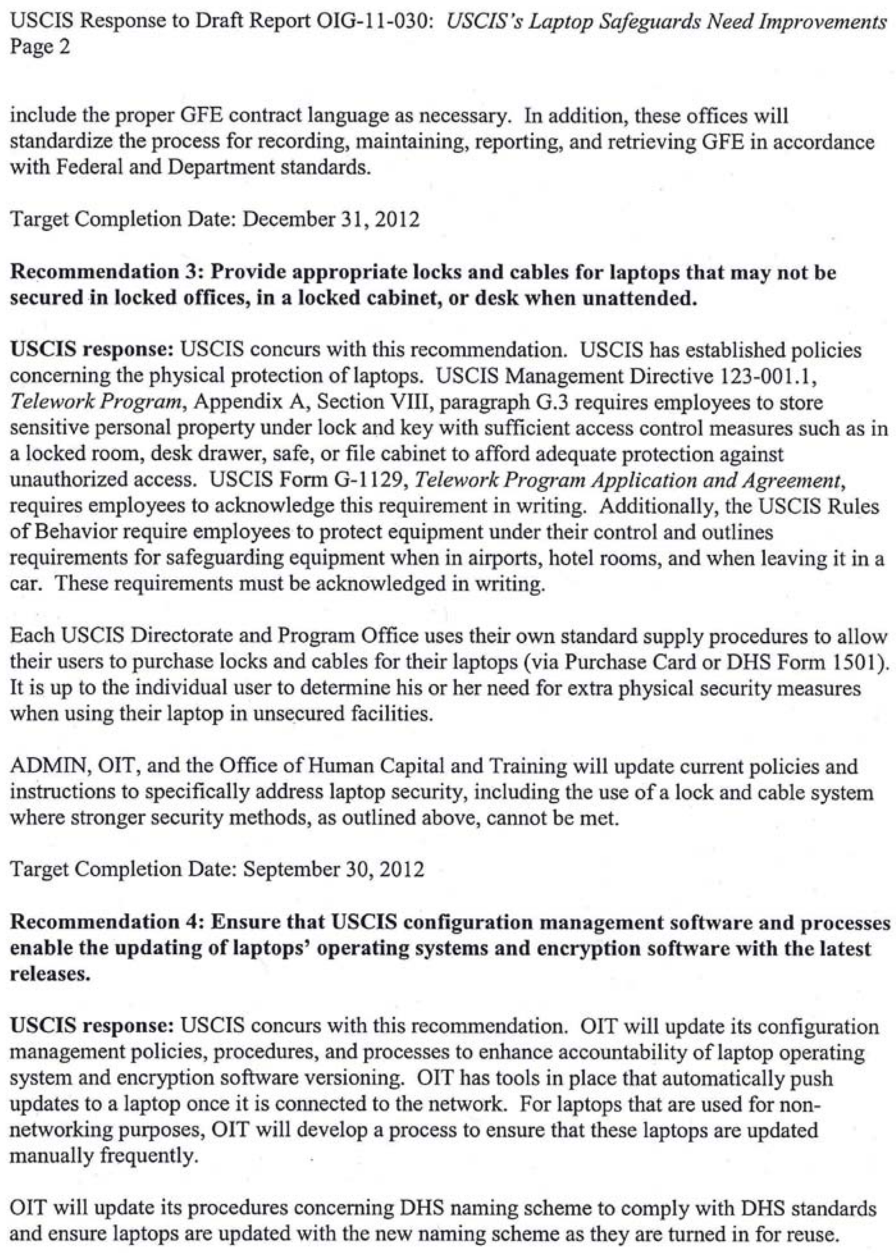
ADMIN will monitor compliance during annual inventory reconciliations and during site visits. All USCIS Directorates and Program Offices will follow the policies and guidelines stipulated in the *USCIS Personal Property Management Instruction Handbook, USCIS IHB 119-002-01.*

Target completion date: September 30, 2012

Recommendation 2: Develop a consistent process to record when laptops are initially provided as government-furnished equipment (GFE).

USCIS response: USCIS concurs with this recommendation. The Office of Contracting, ADMIN, and Office of Information Technology (OIT) will work together to review agency policies and procedures governing the management of GFE and ensure that all agency contracts

www.uscis.gov



include the proper GFE contract language as necessary. In addition, these offices will standardize the process for recording, maintaining, reporting, and retrieving GFE in accordance with Federal and Department standards.

Target Completion Date: December 31, 2012

Recommendation 3: Provide appropriate locks and cables for laptops that may not be secured in locked offices, in a locked cabinet, or desk when unattended.

USCIS response: USCIS concurs with this recommendation. USCIS has established policies concerning the physical protection of laptops. USCIS Management Directive 123-001.1, *Telework Program*, Appendix A, Section VIII, paragraph G.3 requires employees to store sensitive personal property under lock and key with sufficient access control measures such as in a locked room, desk drawer, safe, or file cabinet to afford adequate protection against unauthorized access. USCIS Form G-1129, *Telework Program Application and Agreement*, requires employees to acknowledge this requirement in writing. Additionally, the USCIS Rules of Behavior require employees to protect equipment under their control and outlines requirements for safeguarding equipment when in airports, hotel rooms, and when leaving it in a car. These requirements must be acknowledged in writing.

Each USCIS Directorate and Program Office uses their own standard supply procedures to allow their users to purchase locks and cables for their laptops (via Purchase Card or DHS Form 1501). It is up to the individual user to determine his or her need for extra physical security measures when using their laptop in unsecured facilities.

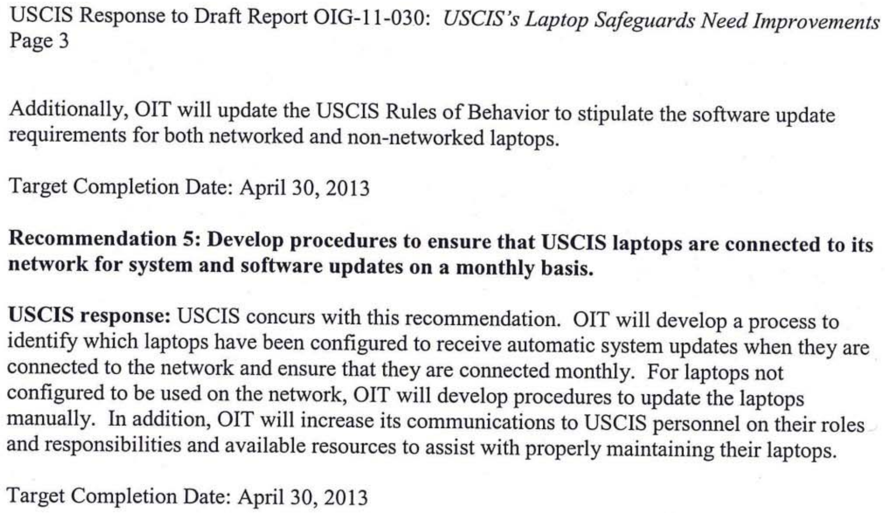
ADMIN, OIT, and the Office of Human Capital and Training will update current policies and instructions to specifically address laptop security, including the use of a lock and cable system where stronger security methods, as outlined above, cannot be met.

Target Completion Date: September 30, 2012

Recommendation 4: Ensure that USCIS configuration management software and processes enable the updating of laptops' operating systems and encryption software with the latest releases.

USCIS response: USCIS concurs with this recommendation. OIT will update its configuration management policies, procedures, and processes to enhance accountability of laptop operating system and encryption software versioning. OIT has tools in place that automatically push updates to a laptop once it is connected to the network. For laptops that are used for non-networking purposes, OIT will develop a process to ensure that these laptops are updated manually frequently.

OIT will update its procedures concerning DHS naming scheme to comply with DHS standards and ensure laptops are updated with the new naming scheme as they are turned in for reuse.



Additionally, OIT will update the USCIS Rules of Behavior to stipulate the software update requirements for both networked and non-networked laptops.

Target Completion Date: April 30, 2013

Recommendation 5: Develop procedures to ensure that USCIS laptops are connected to its network for system and software updates on a monthly basis.

USCIS response: USCIS concurs with this recommendation. OIT will develop a process to identify which laptops have been configured to receive automatic system updates when they are connected to the network and ensure that they are connected monthly. For laptops not configured to be used on the network, OIT will develop procedures to update the laptops manually. In addition, OIT will increase its communications to USCIS personnel on their roles and responsibilities and available resources to assist with properly maintaining their laptops.

Target Completion Date: April 30, 2013

Given a population size of 6,659 laptops, a 95 percent confidence interval, a 5 percent sampling error, and a 50 percent population proportion, a random selection sample would need to include 363 laptops. We used IDEA software to randomly select 363 laptops from USCIS' October 2011 inventory of 6,659 laptops. Laptops selected were in the United States as well as in other countries. Some laptops were classified, some were being used by contractors, some were used for training purposes, and some were unassigned. We received sample responses for 287 USCIS laptops. Although the response did not include all 363 requested laptops, the 287 responses exceeded a lower but still statistically valid sample size of 261 laptops.[3]

Based on these responses from our random sample, we are able to infer the following characteristics of the total USCIS laptop population (see table 3).

Table 3: Characteristics of the USCIS Laptop Population

Laptop	Random Sample Percentage	Percentage Applied to USCIS Population of 6,659 Laptops
WSUS computer name with wrong barcode	2.79%	185
Nonstandard WSUS computer name	6.27%	417
Wrong SAMS barcode	0.35%	23
Unassigned laptops	19.16%	1,276
Laptops with older versions of encryption software	8.01%	533
Encryption not active or not installed	4.53%	301
Older release of operating system or service pack	4.18%	278

[3] Given a population size of 6,659 laptops, a 90 percent confidence interval, a 5 percent sampling error, and a 50 percent population proportion, a random sample would total 261 laptops.

Appendix D
Major Contributors to this Report

Sharon Huiswoud, Director
Kevin Burke, Supervisory Auditor
Pamela Chambliss-Williams, Senior Program Analyst
Charles Twitty, Senior Auditor
Matthew Worner, Senior Auditor
M. Faizul Islam, Economist/Statistician
Robert Durst, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Director of USCIS
USCIS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603

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

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

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

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