DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Review of DHS Security Controls for Portable Storage Devices

OIG-08-95

September 2008

Office of Inspector General

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

Homeland Security

September 26, 2008

Preface

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

The report identifies measures that can be taken by the Department of Homeland Security to minimize the risk of theft, mishandling of the department's sensitive information, or unauthorized use of portable storage devices. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, discovery scans, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	Customs and Border Protection
CIS	Citizenship and Immigration Services
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FLETC	Federal Law Enforcement Training Center
I&A	Intelligence and Analysis
ICE	Immigration and Customs Enforcement
NPPD	National Protection and Programs Directorate
OMB	Office of Management and Budget
S&T	Science and Technology
TSA	Transportation Security Administration
USB	Universal Serial Bus
USCG	United States Coast Guard
USSS	United States Secret Service

Executive Summary

We evaluated the use of portable storage devices at the Department of Homeland Security (DHS). Our objective was to determine whether DHS has addressed the emerging security threat from the proliferation of portable storage devices. We also followed-up on the actions DHS has taken in response to Office of Management and Budget (OMB) Memorandum 06-16 (M-06-16), *Protection of Sensitive Agency Information*. The proliferation and uncontrolled use of portable storage devices (e.g., flash drives, external hard drives, and portable music players) increases the risk of theft and mishandling of sensitive information when users insert their personal or unauthorized devices into their agencies' computers' Universal Serial Bus (USB) or FireWire ports.

DHS has taken actions to address the threat of the unauthorized access to its sensitive information from the proliferation of portable storage devices. For example, DHS has established policies on the acceptable use of portable storage devices. In addition, DHS is evaluating a technical solution that will encrypt information stored on all recordable media.

We determined, however, that the policies developed have not been implemented by the components. Specifically, components do not have a centralized process to procure and distribute portable storage devices to ensure that only authorized devices that meet the technical requirements can connect to its systems. In addition, most components have not identified and do not maintain an inventory of authorized devices. Further, the devices sampled were not properly marked to protect the information stored on these devices from mishandling. Finally, DHS has not implemented all M-06-16 controls, despite the fact that it has been two years since OMB's milestone has elapsed.

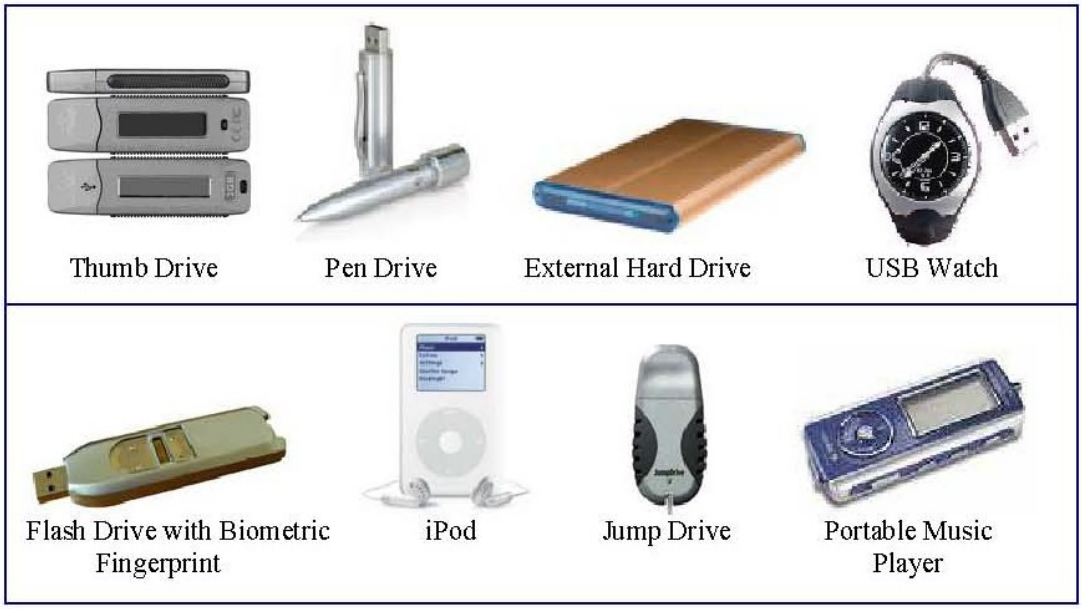
We recommend that components identify and establish an inventory of authorized devices; implement controls to ensure that only authorized devices can connect to DHS systems; and perform discovery scans, at least annually, to identify unauthorized devices. Finally, DHS should devote additional resources to implement OMB M-06-16 controls expeditiously. The department's response

is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The proliferation and uncontrolled use of portable storage devices increase the risk of theft and mishandling of sensitive information. This condition is most prevalent when users insert their personal or unauthorized devices into a computer's USB or FireWire ports. Examples of portable storage devices include flash drives, pen drives, external hard drives, and portable music and video players, such as iPods that can also be used to store data. These portable devices are small enough to fit into a shirt pocket, relatively inexpensive, and can be used to store a large amount of data. The features that make these devices popular can also introduce new security risks and amplify risks that already existed with floppy disks. Shown below are examples of various portable storage devices:

Portable Storage Devices



The risks of theft and mishandling of sensitive data stored on portable storage devices became more apparent when several incidents were reported in 2006. For example, local police in New Mexico seized three USB flash drives that contained classified government information from the Los Alamos National Laboratory at a contract employee's home. Additionally, stolen U.S. military flash drives that contained records about military operations and

individual soldiers were found being sold at a street market in Afghanistan.

In response to the above and a series of other incidents involving the compromise or loss of sensitive personal information, OMB issued M-06-16, *Protection of Sensitive Agency Information*. This memorandum recommends measures to compensate for the lack of physical security controls when sensitive information is removed or accessed from outside the agency location. Agencies were required to implement the following measures by August 7, 2006:

- Encrypt sensitive data stored on laptop computers and mobile computing devices
- Establish two-factor authentication for remote access connections
- Enable the timeout feature for remote access after 30 minutes of inactivity
- Log all data extracts from databases holding sensitive information, and ensure that copies of extracts made by users or administrators are erased within 90 days if they are no longer needed.

Fieldwork was performed at Citizenship and Immigration Services (CIS), Customs and Border Protection (CBP), Federal Emergency and Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and Customs Enforcement (ICE), Intelligence and Analysis (I&A), Management Directorate (Management), National Protection and Programs Directorate (NPPD), Science and Technology (S&T), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS). We performed discovery scans, using USBDetect software,[1] to identify whether unauthorized devices had been connected to DHS' unclassified systems at 11 components and five international airports located in California, Florida, Maryland, and Virginia.[2] In addition, we performed scans on selected classified systems at FEMA, I&A, and S&T.

[1] USBDetect is a software tool that was developed by the National Security Agency. The tool gathers data from the registry on Microsoft Windows machines and reports whether storage devices, such as portable music and video players, external hard drives, flash drives, jump drives, and thumb drives, etc., have been connected to the USB ports.

[2] We only evaluated the use of portable storage devices on selected classified systems at I&A.

Results of Audit

Unauthorized Devices Have Been Connected to DHS Systems

DHS has implemented an effective process to ensure that only authorized devices are connected to its classified systems. Specifically, system administrators have disabled the USB ports to restrict portable storage devices from connecting to DHS' classified systems. However, DHS has not implemented effective controls to restrict unauthorized devices from being connected to DHS' unclassified systems.

Based on our discovery scans, we identified instances where storage devices and portable music and video players were connected to selected unclassified servers and workstations at the 11 component offices included in our testing. Though we could not determine when these devices were connected or whether any sensitive information had been copied to these devices, DHS' controls did not restrict users from connecting unauthorized devices to the department's unclassified systems.

The discovery of unauthorized devices being connected to DHS' information systems is an indication that the controls implemented may not be effective in restricting DHS' sensitive data from authorized access or theft. Furthermore, while few components (CBP, Management, TSA, USCG, and USSS) performed discovery scans to determine whether unauthorized devices had been connected to their systems, there is no set schedule that outlines the frequency of the scans. Unless effective controls are implemented, increased risks exist for the potential mishandling or misuse of DHS' sensitive information stored on portable storage devices.

According to DHS officials, the department recognized the threats from the proliferation and uncontrolled use of portable storage devices. DHS has recently begun to evaluate a new technical solution, which will automatically encrypt any recordable media (such as USB flash drives, external hard drives, portable music and video players, and CDs/DVDs) that have been inserted into DHS systems. Once the encryption is applied, users can only access sensitive information stored on these devices when they are connected to DHS systems. With the new technical solution, the officials indicated that there would be no need to maintain an inventory of authorized devices or ensure that the devices being

used meet certain technical specifications. Furthermore, the officials said that deploying the new technical solution would be a cheaper alternative than purchasing portable storage devices with a biometric encryption feature.

DHS does not have a timeline in implementing the new solution. According to the officials, DHS plans to deploy the new solution department-wide once its technical evaluation is completed and the results are satisfactory. We believe that once the new technical solution is implemented, it can minimize the threats of the potential mishandling or misuse of DHS' sensitive information.

Recommendations

We recommend that the Chief Information Officer direct the components' Chief Information Officers to:

Recommendation #1: Establish a process to ensure that only authorized portable storage devices can connect to DHS systems. In addition, awareness training should be provided to users to educate them on the risks associated with the use of portable storage devices.

Recommendation #2: Implement stringent technical controls to ensure that unauthorized devices are not connected to DHS systems. Discovery scans should be performed, at least annually, to identify unauthorized devices.

Management Comments and OIG Analysis

DHS concurred with recommendation 1. DHS acknowledged the deficiency in its current hardware and network settings that may allow users to connect non-approved devices to DHS equipment and networks. Additionally, DHS restated its current policy that employees and contractors are prohibited from using any non-government issued removable media (e.g., USB flash drives) or connecting them to DHS equipment and networks or to store DHS sensitive information. All DHS-issued USB flash drives must be FIPS 197 compliant and have received FIPS 140-2 validation to protect the information stored on these devices. In addition, DHS plans to implement a technical solution with Windows Vista and Windows Server 2008. Finally, DHS stated that its users are already being educated on the risks associated with the use of portable storage devices, as part of the current security awareness training.

We agree that the steps DHS plans to take satisfy this recommendation. DHS did not provide an estimated timeframe to deploy Windows Vista and Windows Server 2008. DHS' sensitive data continues to be at risk until the department implements an effective process to ensure that only authorized portable storage devices can connect to its systems. Specifically, the results of discovery scans revealed that relying on policy alone does not restrict or deter users from connecting their personal music and video players (e.g., iPod) to DHS systems. While connecting an iPod to a DHS system is a violation of existing DHS policy, it is confirmation that a deficiency exists in the department's current hardware and network settings which allows users to connect non-approved devices to DHS equipment and networks. It may also be an indicator that the current security awareness training may not be effective in educating users on the risks associated with the use of portable storage devices.

DHS concurred with recommendation 2. DHS agreed that the use of portable storage devices (e.g., USB flash drives) should be controlled. Currently, DHS restricts the use of portable storage devices through policy, security awareness training, and disabling USB ports on workstations. DHS indicated that more stringent controls are available through Windows Vista and through Group Policy Objects in Microsoft Server 2008. Specifically, a deployment of Vista and Server 2008 has the capability to restrict USB device installation by Device ID and Device Class. The Device ID matches the exact make, model, and revision of the device, such as a particular USB drive model and manufacturer. Finally, DHS agreed that discovery scans should be performed annually to detect unauthorized devices.

We agree that the steps DHS plans to take satisfy this recommendation. DHS should deploy an interim solution to restrict the unauthorized use of portable storage devices until Windows Vista and Windows Server 2008 are implemented. During our review, we determined that USB ports were only disabled on some classified workstations.

Security Policies Should Be Implemented

DHS has developed policies to mitigate the risks associated with the use of portable storage devices on both classified and unclassified systems. For example, DHS requires that information stored on portable storage devices be encrypted in accordance with

FIPS 140-2 standards.[3] In addition, DHS prohibits the use of personal devices on DHS systems. Furthermore, DHS requires that all recordable media, including authorized portable storage devices, must be properly marked indicating the data's classification, such as "For Official Use Only (FOUO)," "Secret," or "Top Secret," etc.

Several major components (CBP, FLETC, ICE, NPPD, TSA, and USCG) have developed policies, which are aligned with DHS' guidance regarding the use of portable storage devices. However, neither DHS nor the components' policies have been implemented fully. Specifically, we identified:

- Portable storage devices are authorized for use at 11 of the 12 components visited.[4] However, none of these 11 components have established a centralized process to procure and distribute these devices. A centralized process is essential to ensure that only devices that meet DHS and components' technical requirements are used to process and store sensitive information.
- FEMA and I&A prohibit the use of portable storage devices on their classified systems.
- CBP, CIS, FEMA, FLETC, ICE, Management, NPPD, S&T, and USCG did not maintain inventories of authorized devices. CBP, CIS, ICE, and NPPD indicated that an inventory was not maintained because the monetary value for these portable devices was below the threshold. When an inventory is not maintained, DHS and its components cannot track the use of these devices or ensure that only authorized devices are connected to their networks.
- CIS, FEMA, FLETC, ICE, Management, NPPD, S&T, USCG, and USSS did not apply "marking" on the devices sampled to protect sensitive information stored on these devices from being mishandled. Applying proper marking can minimize the risks associated with the accidental disclosure of sensitive data stored on portable storage devices.

[3] This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunications systems. FIPS 140-2, *Security Requirements For Cryptographic Modules*, dated May 25, 2001.

[4] We did not evaluate the use of portable storage devices on I&A's unclassified systems. We only evaluated the use of these devices on classified systems located in an I&A sensitive compartmented information facility.

The implementation of specific policies is essential to ensure that sensitive information stored on portable storage devices is protected from unauthorized use, theft, or mishandling. To protect against threats involving potential misuse, it is imperative that DHS and its components establish a centralized process to procure and distribute portable storage devices, maintain an inventory of authorized devices, and apply proper marking to protect information stored on these devices from unauthorized disclosure.

Recommendation

We recommend that the Chief Information Officer direct the components' Chief Information Officers to:

Recommendation #3: Identify the manufacturers and models of authorized devices. Ensure that an inventory, which contains the names of manufacturers and serial numbers of devices, is maintained. The devices should be marked to indicate the data classification to protect sensitive information stored from unauthorized disclosure or mishandling.

Management Comments and OIG Analysis

DHS concurred with recommendation 3. DHS stated that an inventory of authorized portable storage devices can be established under the Windows Vista and Windows Server 2008 environment, as the Device ID for all authorized USB devices can be identified. However, this capability does not include the identification of serial numbers for USB devices. As this solution is not available until DHS is operating in a Vista and Server 2008 environment, DHS has identified standards for USB flash drives, which requires these devices be FIPS 140-2 and FIPS 197 compliant. Finally, DHS restated its policy requirement to have appropriate markings on storage media.

We agree that the steps DHS plans to take satisfy this recommendation. However, DHS does not plan to establish an inventory of its authorized portable storage devices until Windows Vista and Windows Server 2008 are implemented. In addition, DHS does not plan additional actions to enforce its current policy to ensure these devices are properly marked to indicate the data classification to protect sensitive information stored from unauthorized disclosure or mishandling.

Implementation of OMB-Required Controls Can Minimize Risk

In January 2007, we reported that DHS and its components were in the process of implementing OMB's recommended security controls for sensitive data and personally identifiable information (PII) as outlined in M-06-16.[5] During this evaluation, we followed-up on the actions taken to implement these controls at 11 components and determined that DHS has not completed the implementation of the required OMB controls to protect its sensitive data from unauthorized access.[6]

The purpose of OMB M-06-16 was to compensate for the lack of physical security controls when sensitive information is removed or accessed from outside the agency location. The implementation of these controls can also minimize the risks of unauthorized access to the sensitive data stored on portable storage devices.

Specifically, we identified:

- Ten of the 11 components have installed encryption software to protect sensitive information stored on their laptops
- Seven of the 11 components implemented the session time-out function which requires users to re-authenticate after 30 minutes of inactivity
- Only 5 of the 11 components have implemented two-factor authentication[7]
- None of the 11 components tested implemented effective controls or a reliable process to ensure that data extracts are erased within 90 days or when no longer needed.

Despite some progress in implementing OMB-required controls, more attention and resources may be needed to ensure that sensitive data stored on laptops and mobile computing devices is protected from unauthorized access. Further, DHS officials need to develop milestones for implementing OMB M-06-16. Until

[5] *DHS's' Implementation of Protective Measures for Personally Identifiable Information* (OIG-07-24, January 2007).

[6] We performed fieldwork at 12 components. However, the National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* controls outlined in OMB M-06-16 do not apply to I&A's classified systems.

[7] Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized.

these controls have been implemented, there is an increased risk that sensitive data may be compromised through the loss or theft of laptop computers and mobile computing devices.

Recommendation

We recommend that the Chief Information Officer direct the Chief Information Security Officer to:

Recommendation #4: Devote additional resources to ensure the controls outlined in OMB M-06-16 are implemented expeditiously.

Management Comments and OIG Analysis

DHS did not concur with recommendation 4. DHS did not agree that the OIG should direct the Chief Information Officer on allocating its resources. However, the Chief Information Officer acknowledged that resources must be identified to implement these controls. DHS indicated that implementation plans were being developed based on risks and cost analysis.

We maintain our position that it has been two years since OMB's mandated milestone has elapsed and that DHS should ensure controls outlined in OMB M-06-16 are implemented expeditiously.

We would note as well that we are not directing anything regarding the allocation of resources at DHS. Rather, we are recommending that the Chief Information Officer direct the Chief Information Security Officer to devote additional resources to implement OMB required security controls. It is well within our responsibility, when conducting audits, to identify areas where increased resources are needed to resolve the deficiency.

Also, in a final comment, the Chief Information Officer expressed concern that the title of the draft report, *DHS Must Address the Emerging Security Threat from the Proliferation of Portable Storage Devices,* predisposes readers to think that the department has not taken any action in that regard. We agree and have revised the title as requested.

Our objective was to determine whether DHS has addressed the emerging security threat from the proliferation of portable storage devices. We also followed-up on the actions DHS has taken in response to Office of Management and Budget (OMB) Memorandum 06-16 (M-06-16), *Protection of Sensitive Agency Information*.

To accomplish our audit, we interviewed selected personnel at CBP, CIS, FEMA, FLETC, ICE, Management, NPPD, I&A, S&T, TSA, USCG, and USSS. In addition, we reviewed and evaluated DHS' and components' security policies and procedures regarding the use of portable storage devices. We performed discovery scans, using USBDetect software, to identify whether unauthorized devices had been connected to DHS' unclassified systems at 11 components (CBP, CIS, FEMA, FLETC, ICE, Management, NPPD, S&T, TSA, USCG, and USSS) and five international airports located in California, Florida, Maryland, and Virginia. In addition, we performed scans on selected classified systems at FEMA, I&A, and S&T.

We conducted our evaluation between February and May 2008, under the authority of the Inspector General Act of 1978, as amended, and according to the Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency (PCIE). Major OIG contributors to the audit are identified in Appendix C.

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

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

Homeland Security

AUG 22 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technqlogy Audits

FROM: Richard Mangogna
Chief Information Officer

SUBJECT: Response to Draft Audit Report – *DHS Must Address the Emerging Security Threat from Proliferation of Portable Storage Devices*

Thank you for this opportunity to review and comment on the Office of Inspector General draft report entitled, *DHS Must Address the Emerging Security Threat from Proliferation of Portable Storage Devices,* dated July 25, 2008. The attached document provides comments and/or corrective actions to the four recommendations identified in the report. As requested, we will be advising you under separate cover of any concerns we may have with respect to release of the information contained in the report. If you have any questions, please contact me at (202) 447-3736 or have your staff contact Mr. Robert West, Chief Information Security Officer, at (202) 202-282-9251.

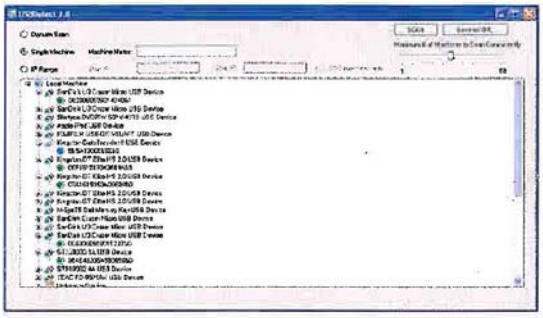
Attachment

cc: Under Secretary for Management

Response to OIG Draft Report - – *DHS Must Address the Emerging Security Threat from Proliferation of Portable Storage Devices*

Methodology: The scanning methodology used by the Office of the Inspector General (OIG) involved querying the windows registry for unauthorized Universal Serial Bus (USB) devices, using the National Security Agency tool *USBDetect*. This methodology will reveal if a USB device has been installed at any point since the DHS machine was first imaged. See the image below.

Sample Screen Shot of USBDetect



As noted in the OIG report, this methodology does not identify if USB devices are currently connected, nor if any sensitive information was copied. However, this methodology has additional weaknesses that were not addressed. The methodology does not take into account that administrators may have been granted waivers to use USB devices for authorized functions. In addition, the methodology does not take into account government-purchased USB devices that were issued prior to the Office of Management and Budget (OMB) 06-16 memorandum requiring Federal Information Processing Standards (FIPS) 140-2 encryption. Both of these usage scenarios may result in a false positive following the OIG methodology.

According to Department of Homeland Security (DHS) policy, an acceptable work solution is to use government-purchased USB drives and encrypt sensitive data to FIPS 140-2 and FIPS 197 requirements using currently available and approved software, such as WinZip.

Recommendation #1: The draft OIG report recommends that the Chief Information Officer direct the Component's Chief Information Officers to establish a process to ensure that only authorized portable storage devices can connect to DHS systems. In addition, awareness training should be provided to users to educate them on the risks associated with the use of portable storage devices.

Concur. DHS currently has a policy in place, as documented in DHS Sensitive Systems Policy Directive 4300A, Section 4.3.1, Media Protection (excerpted below). Current hardware/network settings allow non-approved devices to be connected; however, the DHS Chief Information Officer (CIO) has plans for a technical solution with Microsoft Vista and Windows Server 2008,

Corrective Action Plan for OIG Draft Report - – *DHS Must Address the Emerging Security Threat from Proliferation of Portable Storage Devices*

as addressed in Recommendation #2. Current security awareness training addresses risks from unauthorized USB use, so this portion of the recommendation has been completed.

DHS Sensitive Systems Policy Directive 4300A Section 4.3.1, Media Protection

DHS Policy
c. DHS personnel and contractors are prohibited from using any non government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information.
d. All DHS USB drives shall use encryption that is FIPS 197 compliant and has received FIPS 140-2 validation.

Recommendation #2: The draft OIG report recommends that the Chief Information Officer direct the Component's Chief Information Officers to implement stringent technical controls to ensure that unauthorized devices are not connected to DHS systems. Discovery scans should be performed, at least annually, to identify unauthorized devices.

Concur. USB drives and their use should be controlled, and the current control is through policy, awareness, and disabling USB drives on workstations. More stringent controls are available through Microsoft Vista and through Group Policy Objects in Microsoft Server 2008. Specifically, a deployment of Vista and Server 2008 has the capability to restrict USB device installation by Device ID and Device Class. The Device ID matches the exact make, model, and revision of the device, such as a particular USB drive model and manufacturer. The Device Class matches a broader device category, where all CDROM drives belong to the same Device Class.[1]

The DHS Chief Information Security Officer (CISO) does not currently have the capability to deploy this technical control. Technology deployment is the responsibility of enterprise IT operations and component IT offices. It is important to remember the objective is to protect mobile data, such as USB drives, which can be performed appropriately with a number of operational and technical solutions. These include file encryption; drive encryption, increased use of network shares and collaboration portals, and data exchange through encrypted email.

It should be noted that at this time, Vista and Server 2008 environment does not have the ability to query and inventory USB devices throughout the enterprise. Annual discovery scans would need to be conducted through a separate process, and should be required annually. Annual device scanning is one option to detect unauthorized devices, but current tools such as USBDetect are cumbersome and generate a large number of false positive findings. The Microsoft solution will provide more accurate information and more stringent technical control.

[1] Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy. Retrieved from http://www.microsoft.com/downloads/details.aspx?FamilyID=311f4ba8-9983-4ab0-9685-f1bfec1e7d62&DisplayLang=en#filelist ,August 5, 2008.

Corrective Action Plan for OIG Draft Report - – *DHS Must Address the Emerging Security Threat from Proliferation of Portable Storage Devices*

Recommendation #3: The draft OIG report recommends that the Chief Information Officer direct the Component's Chief Information Officers to identify the manufacturers and models of authorized devices. Ensure that an inventory, which contains the names of manufactures and serial numbers of devices, is maintained. The devices should be marked to indicate the data classification to protect sensitive information stored from unauthorized disclosure or mishandling.

Concur. To accurately implement a Vista and Server 2008 environment, the Device ID for all authorized USB devices must be identified. Either the identification of all disapproved USB Devices or the creation of an approved USB Device ID white list is a recommended solution from Microsoft. However, this does not include identifying USB device serial numbers.

As this solution is not available until DHS is operating in a Vista and Server 2008 environment, the DHS CISO has identified standards for USB drives, requiring they meet FIPS 140-2 and FIPS 197 encryption requirements. This mitigating control protects mobile data on USB drives.

Finally, DHS policy currently requires all For Official Use Only (FOUO) and classified media to have appropriate markings.

DHS Sensitive Systems Policy Directive 4300A Section 4.3.2, Media Marking

DHS Policy
Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1: *Safeguarding Sensitive but Unclassified (For Official Use Only) Information.*

Recommendation #4: The draft OIG report recommends the Chief Information Officer direct the Chief Information Security Officer to devote additional resources to ensure that the controls outlined in OMB-06-16 are implemented expeditiously.

Non-Concur: It is not the responsibility of the DHS OIG to direct the DHS Chief Information Officer resource allocation process. The Chief Information Officer acknowledges that resources must be identified to implement these controls; however, in addition to security posture, consideration is given to evaluation of risk versus cost as implementation plans are developed.

Component Feedback: The Transportation Security Administration (TSA) Chief Information Officer does not concur with the following statements on Page #6, Paragraph #3 of the OIG DRAFT REPORT "DHS Must Address the Emerging Security Threat from the Proliferation of Portable Storage Devices": *"Portable storage devices are authorized for use at 11 of the 12 components visited. However, none of these 11 components have established a centralized process to procure and distribute these devices. A centralized process is essential to ensure that only devices that meet DHS and components' technical requirements are used to process and store sensitive information."*

Corrective Action Plan for OIG Draft Report - – *DHS Must Address the Emerging Security Threat from Proliferation of Portable Storage Devices*

TSA's Information Technology Division (ITD) developed an approach designed to increase the security of information stored on portable devices. TSA provided instructions for obtaining approved centrally-issued encrypted thumb drives. Employees and contractors were reminded that TSA policy prohibits the use of personal thumb drives, and as of June 2007, TSA data may not be stored on any portable device other than an ITD-issued encrypted thumb drive (ITD, *Information Technology Security Policy Handbook*, Chapter 3, Section 12d). Supervisors were instructed to collect, store, and manage the encrypted thumb drive passwords of all employees under their respective supervision. The accountability of these passwords will comply with TSA *Password and Personal Identification Number (PIN)* policy. Compliance with this requirement will be an auditable item for which supervisors are held accountable.

Thumb drive requests are only processed if submitted by the Accountable Property Officer (APO). The drives are issued as sensitive accountable government property in accordance with Management Directive No. 200.57, *Personal Property Management,* and audited during the annual equipment inventories.

TSA centralized flash drive process provides encrypted flash drives that comply with the following password composition criteria.

- Minimum password length of eight characters
- Passwords must contain at least one of each of the following:
  - One alphabetic uppercase
  - One alphabetic lowercase
  - One numeric
  - One special character
- Drives are encrypted with a 256bit AES Hardware-Based Encryption.

In addition, TSA's process ensures end to end management and control of all encrypted flash drives and services associated with this effort. In accordance with TSA Management Directive 200.57, *Personal Property Management*, TSA's Office of Property Management has overall responsibility for compliance and management of TSA's personal property; APOs are responsible for establishing and maintaining records in TSA's Sunflower asset management system.

Final Comment: The title of the draft report, *DHS Must Address the Emerging Security Threat from the Proliferation of Portable Storage* Devices, predisposes readers to think that the Department has not taken any action in this regard. Measures have been taken and plans are developed for further implementation. The Chief Information Officer suggests that the report title be changed to: *Assessment of DHS Security Controls for Portable Storage Devices.*

Information Security Audit Division

Edward Coleman, Director
Chiu-Tong Tsang, Audit Manager
Mike Horton, Information Technology Officer
Barbara Bartuska, Audit Manager
Charles Twitty, Audit Team Leader
Nazia Khan, IT Specialist
Thomas Rohrback, IT Specialist

Melissa Keaster, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight
Director, GAO/OIG Liaison Office
Chief Information Officer Audit Liaison
Chief Information Security Officer Audit Manager

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

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

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528.

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