Department of Homeland Security

Office of Inspector General

DHS Needs To Address Portable Device Security Risks

OIG-12-88

June 2012

Table of Contents/Abbreviations

Appendices

Abbreviations

AES	Advanced Encryption Standard
CIO	Chief Information Officer
CBP	Customs and Border Protection
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
GPS	global positioning system
HSDN	Homeland Secure Data Network
ICE	Immigration and Customs Enforcement
IT	information technology
iOS	iPhone Operating System
MGMT	Management Directorate
MDM	mobile device management
NIST	National Institute of Standards and Technology
ROB	rules of behavior
SMS	short message service
TSA	Transportation Security Administration
USB	Universal Serial Bus
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
Wi-Fi	Wireless Fidelity

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We reviewed the effectiveness of the Department of Homeland Security's (DHS) efforts to secure and deploy portable devices on DHS networks and to maintain and dispose of these devices. Portable devices included tablet computers and smartphones that are based on Android, iPhone Operating System, Web Operating System, and Windows Operating Systems, as well as Universal Serial Bus thumb drives. Specifically, we evaluated whether (1) adequate policies and procedures have been implemented, (2) DHS maintains an accurate inventory of its portable devices, and (3) effective controls have been implemented to protect the information stored or processed on portable devices. Additionally, we reviewed security authorization packages of systems using portable devices for compliance with applicable policies.

DHS has taken actions to govern, track, categorize, and secure portable devices. Specifically, DHS and its components have developed policies, procedures, and training regarding the use of portable devices. Additionally, some components include portable devices as part of their accountable personal property inventory.

However, DHS still faces challenges in using these devices to carry out its mission and increase the productivity of its employees. For example, components must develop policies and procedures to govern the use and accountability of portable devices. Further, we determined that unauthorized Universal Serial Bus devices had been connected to the workstations at selected components. Finally, DHS must implement controls to mitigate the risks associated with the use of portable devices and to protect the sensitive information that these devices store and process.

We are making three recommendations to the Chief Information Officer. The Chief Information Officer concurred with all recommendations and has begun to take actions to implement them. The Department's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

Portable devices, such as Universal Serial Bus (USB) thumb drives, Apple iPhone Operating System (iOS) and Google Android-based smartphones and tablet computers with wireless Internet access and touch screen features have become increasingly popular with today's highly mobile workforce. These devices allow employees to perform their tasks at any time and from any place, as well as transport large volumes of data efficiently. Additionally, employees use these portable devices to send and receive electronic mail, browse the Internet, edit documents, deliver presentations, and access data remotely. Figure 1 depicts examples of various portable devices.

Figure 1: Examples of portable devices.

Although portable devices may improve productivity, they also expose the Department to new security risks, such as downloading viruses or inadvertently exposing sensitive information or personally identifiable information. In addition, portable devices typically lack a number of security features that can be found on desktop computers. Security threats to portable devices include

loss or theft, unauthorized access to networks or data, electronic eavesdropping, and electronic tracking of users.

Additionally, Android- and iOS-based smartphones and tablet computers were designed primarily for consumers; they lack the functionality and security features needed to be centrally managed in an enterprise or government environment. Unlike Blackberry smartphones, these devices cannot be managed easily without a third-party application. Further, the Android- and iOS-based tablet computers are not designed to use the Federal Information Processing Standard (FIPS) 201-compliant Personal Identity Verification card to establish two-factor authentication for accessing Federal information systems without an accessory or attachment.[1]

To improve the mobility of its workforce, DHS and its components are evaluating the feasibility of integrating these consumer-oriented portable devices into their networks. For example, the Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement (ICE), and Transportation Security Administration (TSA) are currently pilot testing Android- and iOS-based devices to determine whether they can be used to meet the needs of the mobile workforce without compromising security. The United States Coast Guard (USCG) has begun to deploy Android- and iOS-based smartphones to its workforce. Finally, the United States Citizenship and Immigration Service (USCIS) is exploring iPads and Blackberry Playbooks as potential platforms for its senior officials. Since each component has a different mission, their needs and requirements for using and securing the devices vary. During our fieldwork, we did not identify any components considering or implementing the WebOS-based devices. Figure 2 lists the portable devices that the components are using.

[1] OMB Memorandum 05-24, "Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors.

COMPONENT	SMARTPHONES AND TABLETS	THUMB DRIVES
CBP	Fujitsu Lifebook, Panasonic Toughbook Tablet, Blackberry Playbook, Hewlett-Packard Slate 500, iPad, Stylist Q550 Tablet, and CL900 Motion Tablet	Ironkey, Acomdata, Aegis, Apricon, Axiom, Cruzer, Edge, Flash Drive 2G, Kanguru, SanDisk, SanDisk Cruzer, Stealth MXP, Verbatim, and Western Digital
FEMA	iPads and iPhones	Ironkey
ICE	Androids, iPads and iPhones	McAfee Encrypted, Ironkey, and Stealth MXP
TSA	iPhones, Samsung Focus, iPads, Motorola Atrix, Motorola Droid, LG Fathom, Companion ePad, Motorola Xoom, Blackberry Torch, Hewlett-Packard Slate 500, Blackberry Playbook, MacBook AIR and Pro, and Mi-Fi Verizon	Kingston Data Traveler 5000
USCIS	iPads, Blackberry Playbooks, and Samsung Tablets	Ironkey, Kingston, and Integral
USCG	iPhones, Androids, HTC Evo View Tablet, Samsung Galaxy Tablet, and Motorola Xoom	USCG does not allow thumb drives unless waiver is approved.

Figure 2: Portable devices used

Through these pilot programs, DHS and its components are evaluating technical solutions, such as a virtual private network or a mobile device management (MDM) solution, to secure and manage these devices in an enterprise environment.[2] For example, FEMA, ICE, TSA, and USCG are using the Good Technology MDM solution to provide configuration management and encryption to these emerging portable devices.[3] Although Customs and Border Protection (CBP) had tested the MDM solution to manage its Android- and iOS-based smartphones and tablet computers, it is now testing the use of Microsoft Active Directory to manage these devices through its group policy. Figure 3 depicts connectivity avenues and encryption methods for portable devices.[4]

[2] An MDM solution secures, monitors, and manages mobile devices deployed across the enterprises. MDM functionality typically includes over-the-air distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers.

[3] The Good Technology MDM solution offers a securely contained "sandbox" environment through the use of FIPS 140-2 certified encryption using the Advanced Encryption Standard (AES) algorithm. This secure container uses a 192-bit encryption key to help protect data transmitted over the air and stored on the devices.

[4] A sandbox architecture provides an isolated portion of the portable device resources for applications to run. Most access to the device's resources is usually disallowed. Also, the architecture restricts the device's ability to alter or read data outside its specific self-contained environment.

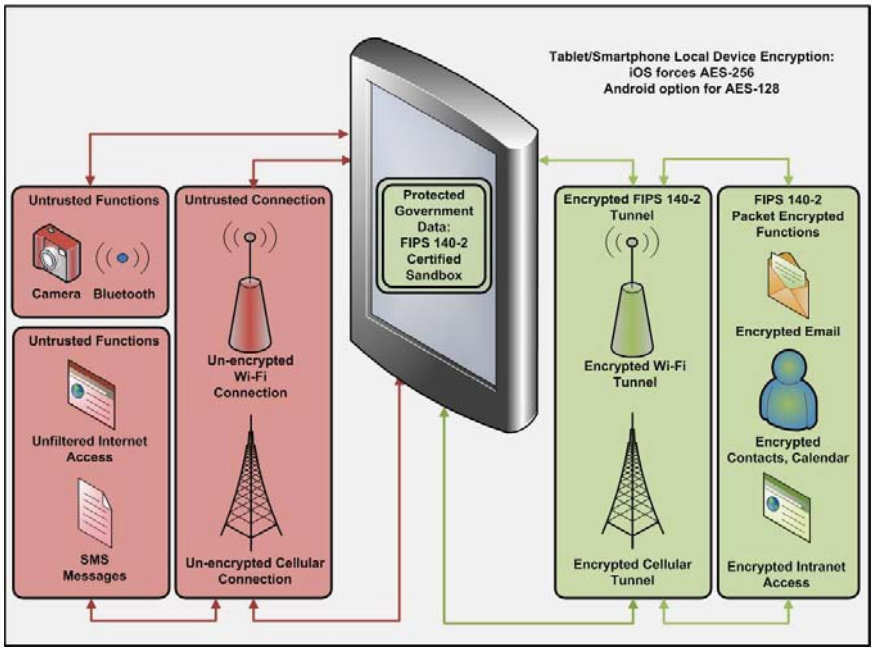

Figure 3: Connectivity avenues and encryption methods for devices

The MDM solution provides the capability to centrally manage configuration settings and allows administrators to restrict access to integrated capabilities of the portable devices, such as the camera and Bluetooth. Additionally, data stored in the secure environment do not mix with data outside of the sandbox container, which minimizes potential data loss or leakage.

As the popularity of portable devices grows, new security threats are introduced constantly and portable device architectures pose new technical and policy issues that must be addressed. For example, a 400 percent increase in Android malware has been identified since the summer of 2010. Further, increasing security vulnerabilities have been identified in Android-based products, which may allow unauthorized access to sensitive information.

Results of Audit

Actions Taken To Address the Use and Safeguarding of Portable Devices

DHS and its components have taken actions to track and promote the use of portable devices in support of their missions. Specifically, they have

undertaken a number of efforts to mitigate security risks posed by portable devices:

- FEMA, TSA, and USCG have developed specific portable device policies and procedures and aligned them with DHS guidance. For example, they have developed specific rules of behavior (ROB) for portable devices. TSA has developed a Mobile Computing Test Devices ROB specific for testing portable devices.

- CBP, FEMA, ICE, TSA, and USCIS use an asset management system to record and track inventory of sensitive items, such as smartphones, tablet computers, and thumb drives.

- CBP, FEMA, TSA, and USCG provide specific training on the acceptable use of portable devices to their users, in addition to general information technology (IT) security awareness. This ensures that users have a full understanding of use, management, accountability, and incident response in the event that a device is lost or stolen.

Although DHS and its components have taken actions to mitigate the risks associated with using portable devices, the Department still faces challenges in deploying these devices to carry out its mission as well as to improve the productivity and mobility of its employees. Additionally, components must develop policies and procedures to govern the use and improve the accountability of portable devices. Finally, DHS must implement security controls to safeguard the portable devices and the sensitive information stored on and processed by these devices.

Adherence to Policies and Procedures Is Needed To Account for Thumb Drives and Ensure Proper Usage of Portable Devices

Components are not adhering to DHS policies and procedures regarding the inventory of USB thumb drives, nor are they consistently signing ROB prior to issuing equipment. Specifically, CBP, TSA, and USCIS do not categorize USB thumb drives as a sensitive asset. Additionally, some components have issued portable devices to their users without signed ROB. Further, some components have not developed policies specific to portable devices, such as thumb drives, and protecting the data that they process and store. As a result, USB thumb drives are inconsistently accounted for in the components' asset management systems.

Sensitive Assets Are Not Accurately Categorized

Three components do not track their USB thumb drives as sensitive assets as required by DHS guidance. DHS requires sensitive assets, such as personal computing devices and USB thumb drives, to be recorded in a personal property system. DHS guidance defines sensitive personal property, regardless of dollar value, as devices that have data storage capability, are inherently portable, can easily be converted to private use, or have a high potential for theft. Specifically, CBP, TSA, and USCIS do not include USB thumb drives in their asset management systems. As a result, these components do not accurately categorize USB thumb drives, which may put their sensitive data at risk.

According to component officials, they did not define and categorize USB thumb drives as sensitive property assets because of the cost and size of these devices. Since USB thumb drives usually cost less than the $5,000 personal property threshold, they do not meet the requirements to qualify as accountable property. Additionally, according to CBP and USCIS officials, since their USB thumb drives are encrypted and inexpensive, they did not think that it would be necessary to inventory these devices. USCIS officials added that they believed it was not logistically efficient to record them in their asset management system. If USB thumb drives are lost or stolen, according to USCIS officials, the property custodians would have to prepare paperwork, get it signed, and add it to the asset management system to fully record the loss. USCIS property custodians and IT staff are currently considering whether to track USB thumb drives as accountable property.

Component asset management systems use serial numbers to inventory and track sensitive items such as smartphones, tablet computers, and USB thumb drives. However, only FEMA and ICE record all USB thumb drives in their asset management systems.

Policies establish internal controls to ensure accountability and protect against fraud, waste, and abuse of government data and property. Further, proper accounting of USB thumb drives enables DHS and its components to effectively use, maintain, protect, transfer, and dispose of their property.

Rules of Behavior Are Not Consistently Signed Prior to Issuing Portable Devices at Components

DHS and its components are not consistently using ROB to remind users to safeguard portable devices and data. Specifically, ROB inform users of their responsibilities and acceptable behaviors while accessing DHS data on portable devices. Since ROB are not reviewed annually, users may not exercise due care and accountability in using, handling, transporting, and storing government data and property. For example, FEMA and TSA rely heavily on the use of ROB to inform users of their responsibilities and the prohibited activities when using portable devices. We determined that 9 of 10 FEMA and 7 of 7 TSA selected users signed the required ROB. However, 9 of the 10 ICE users selected did not sign a separate ROB upon receipt of their portable device. Although users signed an ROB when they first accessed the system, they did not recertify when they received additional equipment.

DHS requires that users be trained regarding acceptable behaviors and that each user sign an ROB prior to being granted user accounts or access to information systems or data. Additionally, the ROB applies to employees using DHS systems and IT resources, such as portable devices, to access, store, receive, or transmit sensitive information.

Policies and procedures, such as ROB, specific to portable devices would strengthen employee awareness of appropriate and effective device usage. Additionally, recertifying employees' ROB annually would remind employees of their responsibilities. Further, the ROB can serve as an additional training mechanism to protect the portable device and its sensitive data.

Recommendations

We recommend that the Chief Information Officer (CIO):

Recommendation #1: Coordinate with the Chief Administrative Officer and component CIOs to update their asset management policies to ensure that USB thumb drives are recorded as sensitive personal property. In addition, components should record USB thumb drives as sensitive personal property in their asset management systems.

Recommendation #2: Enhance the Department's annual IT security awareness training to remind users of their responsibilities, acceptable behaviors, and associated risks when using government-issued portable devices.

Management Comments and OIG Analysis

DHS concurred with recommendation 1. The CIO will coordinate with the Office of the Chief Administrative Officer and the component CIOs to ensure that their asset management policies are updated to require that USB thumb drives are recorded as sensitive personal property as required by DHS *Personal Property Management Directive*. In addition, component CIOs will implement a process to record USB thumb drives as sensitive personal property in their asset management systems.

We agree that the steps DHS has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 2. The CIO will ensure that the Department's annual IT security awareness training is enhanced to remind users of their responsibilities, acceptable behaviors, and associated risks when using government-issued portable devices.

We agree that the steps DHS has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Security Risks of Portable Devices Must Be Addressed To Safeguard DHS Data

The growing popularity and use of portable devices have introduced new security concerns for DHS and its components. For example, DHS has not developed detailed configuration settings for Android- and iOS-based portable devices. Also, components are not consistently applying the required encryption on portable devices. In addition, components have not fully implemented the required DHS security settings. Further, components

are using potentially insecure integrated functions that are required for their mission. Unless these issues are addressed, they may pose a security risk to the Department's data if security controls are inadequate.

Consumer Devices Pose Security Challenges

Although Android- and iOS-based devices offer many sought-after features in the consumer market, these devices can create unique security concerns for DHS and its components due to their consumer-oriented nature. For example, integrated features, such as Bluetooth, global positioning system (GPS), camera, Internet access, and text messaging, are consumer-demanded functions that can become avenues of attack to gain unauthorized access to DHS data. Currently, a third-party MDM application is needed to provide the required FIPS 140-2 encryption for data transmission. However, the MDM application has limited capability to fully implement DHS required security controls.

DHS has developed guidance for configuring portable devices (i.e., user authentication, encryption, antivirus software, remote wipe capability, disabling unneeded integrated functions). However, the Department lacks specific detailed configuration settings needed to mitigate the unique security risks associated with the Android- and iOS-based architectures.

Encryption of Portable Devices

Android- and iOS-based devices are not currently FIPS 140-2 certified to transmit data as required by DHS. The use of these devices, which do not meet the required government encryption standards, poses security risks on DHS networks. For example, the MDM solution encrypts data stored on the device as long as the data are within the container, and implements this same encryption on data transmitted from the container. A limitation of the current MDM solution is that it is not possible to centrally enforce local encryption on Android- or iOS-based devices.[5]

The DHS components we reviewed are not consistently using encryption to protect sensitive data stored on and processed by

[5] Apple iOS devices provide encryption of local data with AES-256 bit encryption on the iPhone 3GS model or higher, and all iPad models as long as the user authenticates to the device. Google Android devices with operating system version 3.0 or higher have the manual option of turning on encryption that uses AES 128-bit encryption. The use of higher bit encryption increases computational time and effort needed by the device, but helps protect the data for a longer period.

portable devices. For example, ICE and USCG have not enabled local encryption on their Android devices. As a mitigating control, USCG user policy requires that all data processed by a portable device must be kept in the MDM container. To enable local encryption on Android devices is a time-consuming process, as it requires USCG and ICE to configure each device manually. In addition, ICE does not enforce user authentication on iOS devices, which disable forced encryption by the operating system. Also, ICE has yet to develop a user policy that requires all data to be kept within the MDM container solution. Any sensitive data stored outside the MDM solution could be in an unencrypted space and might be vulnerable to unauthorized access. To protect their sensitive data, FEMA and TSA have implemented the iOS devices through the use of the MDM solution to meet DHS encryption requirements.

CBP is testing a tablet form-factor with Windows 7 installed, through the use of Microsoft BitLocker technology. CBP has encrypted data on the device, and has secured data in transmission through a virtual private network connection.[6] This virtual private network connection requires two-factor authentication and integrates with Active Directory for user validation while establishing a Wireless Fidelity (Wi-Fi) or cellular connection.

Data stored on wireless portable devices must be encrypted by securing either the individual files or the file system using the National Institute of Standards and Technology (NIST) validated encryption scheme (i.e., FIPS-197 AES algorithm). Additionally, wireless portable devices must utilize products or modules with NIST FIPS 140-2 compliant encryption when synchronizing wirelessly.

Configuration Management of Portable Devices

Components have not fully implemented DHS configuration management guidance on portable devices. Instead, they have implemented component-specific settings on their devices. Discrepancies occur in the authentication controls and complexity of passwords, location for first authentication on either the local device or secure container, and the idle-timeout period for inactivity. Without fully implementing DHS configuration

[6] BitLocker is an encryption function of Microsoft Windows operating systems that, once enabled, allows full disk encryption. This includes the operating system itself, the Windows registry, temporary files, and hibernation file. In addition, a BitLocker add-on can encrypt removable media such as USB thumb drives.

guidance, components cannot ensure that their devices are protected from potential exploits.

Since the MDM solution does not fully address all DHS configuration management guidance requirements, components are unable to fully implement DHS security settings. For example, the MDM application cannot enforce the use of special characters to access the local Android-based device. Across the components we reviewed, there is no standard implementation of special character use for complex passwords. USCG has not enforced special character use for complex passwords for any user authentication, including both local and sandbox locations on Android and iOS devices. CBP, FEMA, and ICE have implemented special characters when users authenticate, but TSA has not implemented special characters on its iOS devices.

Without the detailed DHS configuration settings, components are authenticating users at different levels of the devices at either the local or sandbox level. We identified the following discrepancies:

- TSA and USCG require authentication locally to the device and at the secure container level. DHS requires that users authenticate when the device is powered on to be granted access.

- FEMA requires users to authenticate to the local device but does not require users to authenticate a second time to the secure container on its iOS devices.

- ICE enforces strong passwords at the sandbox, but there is no authentication to access the local Android and iOS devices. The lack of authentication and password enforcement may allow unauthorized individuals to gain access to DHS data stored on the local device.

DHS requires a 10-minute idle-timeout for portable devices, after which users must re-authenticate to revalidate their identity. While ICE has implemented an idle-timeout of 20 minutes on its MDM solution, the component has not implemented the timeout feature on its Android- and iOS-based devices. FEMA and TSA have implemented a less stringent 15-minute idle-timeout limit. According to CBP personnel, it is in the process of submitting a waiver to account for its 15-minute idle-timeout, which currently is in place for network timing alignment. USCG, with its Android

and iOS device policies, has enforced a more stringent 5-minute idle-timeout.

DHS requires that wireless portable devices, such as smartphones and tablets, be distributed and configured with an approved baseline configuration. The baseline configuration guidance includes authenticating before access is granted to the device. In addition, passwords protecting the devices must have a minimum of eight characters and a combination of both alphanumeric and special characters.

The ability to centrally manage and enforce a standard configuration setting is vital to assure components of a standard baseline for security. The lack of a standard configuration for its portable devices could expose DHS sensitive data to potential attacks. Not authenticating at the local device could allow unauthorized users to gain access to DHS data stored on the local device.

Remote Wipe of Data Capability Is Vital To Protect Data

The lack of centrally executable built-in remote wipe capability may put DHS data at risk if a portable device is lost or stolen. Currently, a third-party MDM solution is needed to invoke a remote wipe command to erase data stored on the devices. This function can wipe the device, including storage cards or sandbox data, to prevent unauthorized disclosure. In addition, the MDM solution offers the capability to enforce compliance rules and restricts users from installing applications on the devices. Compliance rules verify that the device operating system version, device model, account inactivity, and MDM client are within the component-selected parameters. If a device is found to be "jail-broken," or in violation of a compliance rule, it will automatically be wiped either at the sandbox or the local device.[7] Compliance rules and jail-break detection function can be checked at specified intervals.

The components we visited that use the MDM solution have implemented remote wipe, compliance rules, and the jail-break detection function to ensure that the standard configuration does not change. Without these capabilities, managers cannot be assured that the devices have not been altered without their

[7] Jail-breaking is the act of installing a file to open the operating system so unauthorized third-party applications can be installed. It also allows the user to customize the device.

knowledge or consent, or help protect DHS data from unauthorized access.

Integrated Functions Cause Security Concerns

Components are using potentially insecure integrated functions in using portable devices to support their missions. While integrated functions (e.g., camera, GPS, Bluetooth) on mobile devices can improve mobility and add functions, they can also expose DHS sensitive data to potential exploits and pose privacy concerns. For example, components are using integrated, potentially unencrypted features, such as Bluetooth, camera, and GPS. Other features that can be used for limited personal use include unfiltered Internet access and short message service (SMS) (i.e., text messaging). These integrated functions are potentially insecure and can put DHS data confidentiality and integrity at risk. Figure 4 lists the integrated built-in functions used at the components:

Component	Devices	Bluetooth	Camera[8]	Wi-Fi
CBP	Windows 7	X	X	X
FEMA	iOS	X	X	X
ICE	Android, iOS	X	X	X
TSA	iOS			
USCG	Android, iOS		X	
Legend: "X" denotes functions that are enabled.				

Figure 4: Enabled integrated functions

Component officials said that some integrated functions, such as Bluetooth, are required to allow mobile hands-free calling to reduce the dangers of text messaging while driving.[9] In addition, they said that the use of a built-in camera can reduce the amount of equipment that inspectors and investigators have to carry when conducting official business, as well as cut costs. Lastly, component officials said that Wi-Fi connectivity is needed to reduce the cost of cellular use to transmit data.

DHS requires that functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information. In addition, SMS shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible. Integrated capabilities, such as cameras and recording mechanisms, pose significant levels of

[8] The MDM solution does not have the capability to enable or disable the camera on Android devices.
[9] A result of Executive Order 13513, signed in October 2009.

risk and should be disabled, unless specifically required, in order to mitigate the risk of exposing sensitive information.

These integrated functions are consumer-oriented and are not located within the secure MDM solution. Using potentially insecure functions may expose sensitive data to unauthorized access.

Consideration of security in the system development life cycle is essential as DHS and its components are evaluating the feasibility of integrating these consumer-oriented portable devices into their networks. To accomplish this, security must be made an integral part of the testing performed as new features and functionality are introduced into a system. As stated in applicable guidance, to be most effective, security controls must be integrated into the information system from its inception. Including security controls early in the information system development life cycle will result in less expensive and more effective security than adding it to an operational system.

USB Protective Measures

DHS and its components have not implemented effective controls to restrict unauthorized devices from being connected to DHS' unclassified systems. However, the Department has implemented an effective technical solution to ensure that only authorized personnel can use USB devices on its enterprise-wide "Secret" classified network.

Unauthorized USB Connected to Unclassified Networks

Unauthorized USB devices have been connected to DHS networks. We conducted technical scans to determine whether unauthorized USB storage devices have been connected to DHS computers at ICE, Management Directorate (MGMT), TSA, and USCG.[10] Our scans identified unauthorized devices in all components reviewed. Most devices identified were connected between 2010 and early 2012. The use of unauthorized devices to store sensitive data can lead to unauthorized access when the devices are not encrypted. Figure 5 lists examples of unauthorized devices identified.

[10] We used the National Security Agency's developed USB Detect software to determine if unauthorized devices have been connected to DHS and its components' networks. This tool queries registry keys within the Windows operating system and records mass storage devices that have been inserted in the targeted computers. The tool gives a historical view from the time the operating system image was installed to the present, and can identify if devices were properly installed by the operating system, or denied.

Component	Authorized Devices	Examples of Unauthorized Devices Identified
ICE	McAfee Encrypted Drive IronKey S200 & D200 Stealth MXP	Amazon Kindle E-Book Reader Apple iPod Nike Sportwatch GPS Unit Digital Picture Frame Best Buy Geek Squad U3 USB Drive SanDisk Cruzer USB Drive Sony Storage Mass Media
MGMT	Outbacker MXP Stealth MXP McAfee Encrypted Drive IronKey S200 & D200 Kingston DataTraveler 5000	Apple iPod Imation USB Flash Drive Corsair Voyager USB Flash Drive SanDisk Cruzer Micro SD card Sony Storage Mass Media Western Digital External Hard Drive LaCie ED Mini External Hard Drive
TSA	Kingston DataTraveler 5000	Garmin Nuvi GPS Unit Apple iPod SanDisk Cruzer Seagate FreeAgent Go Hard Drive Best Buy Geek Squad U3 USB Drive
USCG	No Flash Media unless waiver approved	Apple iPod Garmin Nuvi GPS Unit Digital Picture Frame HTC Android Phone USB Device

Figure 5: Unauthorized devices identified

ICE, MGMT, TSA, USCIS, and USCG officials said that currently they cannot prevent unauthorized devices from being connected to their workstations.[11] Instead, components rely on a multitier process that includes authorizing, procuring, and distributing only specific encrypted USB drives, and educating users, through awareness training, not to connect unauthorized devices to government computers.

DHS prohibits the use of nongovernment-issued removable media, such as USB drives, to store DHS sensitive information. In addition, DHS requires that all USB drives be encrypted to protect sensitive data stored on these devices.

[11] We did not conduct scans at USCIS to determine use of unauthorized devices.

Recognizing the risks of using USB thumb drives, ICE, MGMT, and USCG have begun to deploy a technical solution to prevent the use of unauthorized devices that may put DHS data at risk. For example, a technical solution can be configured to restrict certain USB and other devices from connecting to DHS computers based on vendor and product identification number, as well as other attributes. ICE, MGMT, and USCG have started a three-phase approach to implement this technical solution:

- Phase 1: Monitoring network to identify the devices;
- Phase 2: Constructing the authorized and unauthorized device lists based on the information that is collected during Phase 1;
- Phase 3: Implementing prevention of unauthorized devices.

Currently, ICE, MGMT, and USCG are in Phase 1, and are about to begin Phase 2. TSA officials indicated that they had developed a written policy but did not have any technical means to prevent this type of unauthorized device use.

Protective Measures Taken on Classified Network

The Department has taken protective measures on the classified network to allow only authorized personnel to use USB devices. We conducted a review of the DHS enterprise-wide "Secret" classified network, Homeland Secure Data Network (HSDN). We determined that DHS has implemented a technical solution, a type of continuous monitoring, that restricts the use of USB devices based on authorized user accounts and is integrated with Active Directory. If a user not authorized to use USB thumb drives inserts a USB device into the network, the technical solution denies use, logs the event, and sends a notification to the HSDN Security Operations Center. HSDN relies on the same multi-tier process that the components use for USB devices to ensure that they are encrypted and authorized. For logging purposes, the technical solution records the file path and file name of data moved to USB devices.

The continuous monitoring solution implemented on HSDN can prevent the use of unauthorized devices, including USB devices, writing to discs, Bluetooth connections, and others from

connecting and being used. The solution can be configured to allow only certain approved USB and other devices to be installed, based on vendor and product identification number and other attributes, or to allow only certain approved users to install devices. In addition, this solution can tag data and can then restrict data movement based on these tags.

A continuous monitoring program for enforcement of USB device use can help prevent data loss and unauthorized disclosure. It will also allow DHS to be more cognizant of threats and weaknesses in its network and help gain a more secure infrastructure.

Recommendation

We recommend that the CIO:

Recommendation #3: Work with the ICE CIO to ensure compliance with DHS guidance on authentication requirements for Android and iOS devices.

Management Comments and OIG Analysis

DHS concurred with recommendation 3. The CIO will work with the ICE CIO to ensure compliance with DHS guidance on authentication requirements for Android- and iOS-based devices. Currently, Android- and iOS-based devices are being piloted for possible formal implementation. If ICE decides to formally implement either device, it will be required to comply with the appropriate DHS guidance on authentication requirements for the device selected.

We agree that the steps DHS has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Appendix A
Purpose, Scope, and Methodology

The objective of our audit was to determine the effectiveness of DHS' efforts to secure and deploy portable devices on DHS networks and to maintain and dispose of these devices. Specifically, we evaluated whether (1) adequate policies and procedures have been developed, (2) DHS maintains an accurate inventory of its portable devices, and (3) effective controls have been implemented to protect the information stored or processed on portable devices. Additionally, we reviewed security authorization packages of systems using portable devices for compliance with applicable DHS, Office of Management and Budget, and NIST requirements.

Our review focused on portable devices such as tablet computers and smartphones that are based on Apple iOS, Google Android, and Windows operating systems, as well as USB thumb drives. We excluded laptop computers and Blackberry smartphones from this audit. Our review was based on the requirements outlined in *The Homeland Security Act* (2002), the DHS 4300A Sensitive Systems Handbook, NIST Special Publications, and FIPS guidance. We reviewed DHS as well as component policies and procedures and inventory records and practices. We interviewed selected DHS officials from CBP, DHS MGMT, FEMA, ICE, TSA, USCG Headquarters – CG6, and USCIS. We performed technical reviews of USB detection capabilities at DHS Management, ICE, TSA, and USCG. We performed technical reviews of portable device management controls at CBP, FEMA, ICE, TSA, and USCG Headquarters – CG6. Additionally, we interviewed officials from the Department of Veterans Affairs, and private sector portable device security experts.

We conducted this performance audit between September 2011 and March 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.

The principal OIG point of contact for the audit is Frank W. Deffer, Assistant Inspector General, Information Technology Audits, at (202) 254-4041.

Office of the Chief Information Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

JUN 0 1 2012

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Richard A. Spires
DHS Chief Information Officer

SUBJECT: *DHS Needs to Address Portable Device Security Risks – For Official Use Only (OIG Project No. 11-148-ITA-DHS)*

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has reviewed the findings of the Office of the Inspector General (OIG) draft report 11-148-ITA-DHS, *DHS Needs to Address Portable Device Security Risks,* released March 21, 2012. OCIO's response to the OIG's draft report is as follows:

Recommendation #1: We recommend that the Chief Information Officer coordinate with the Chief Administrative Officer and component CIOs to update their asset management policies to ensure that USB thumb drives are recorded as sensitive personal property. In addition, components should record USB thumb drives as sensitive personal property in their asset management systems.

OCIO Response: Concur. The OCIO will coordinate with the OCAO and Component CIOs to ensure that their asset management policies are updated to require that USB thumb drives are recorded as sensitive personal property as required by DHS *Personal Property Management Directive* (MD #0565). In addition, Component CIOs will implement a process to record USB thumb drives as sensitive personal property in their asset management systems.

Recommendation #2: We recommend that the Chief Information Officer (CIO) enhance the department's annual IT security awareness training to remind users of their responsibilities, acceptable behaviors, and associated risks when using government issued portable devices.

OCIO Response: Concur. The CIO will ensure that the department's annual IT security awareness training is enhanced to remind users of their responsibilities, acceptable behaviors, and associated risks when using government issued portable devices.

Recommendation #3: We recommend that the Chief Information Officer work with the ICE CIO to ensure compliance with DHS guidance on authentication requirements for Android and iOS devices.

OCIO Response: Concur. The Chief Information Officer will work with the ICE CIO to ensure compliance with DHS guidance on authentication requirements for Android and iOS devices. Currently, Android and iOS devices are being piloted for possible formal implementation. If ICE decides to formally implement either device, it will be required to comply with the appropriate DHS guidance on authentication requirements for the device selected.

Appendix C
Major Contributors to this Report

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Shannon Frenyea, Team Lead
Thomas Rohrback, IT Specialist
Megan Ryno, Program Analyst
Angela Maxwell, IT Auditor
Gregory Wilson, II, Management/Program Assistant
Charles Twitty, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Chief Information Officer
Deputy Chief Information Officer
Acting Chief Information Security Officer
Director, GAO/OIG Liaison Office
Director, Compliance and Technology, DHS, Office of Chief Information Security Officer
Branch Chief, Office of Chief Information Security Officer
Audit Liaison, DHS/CIO
Audit Liaison, DHS/CBP
Audit Liaison, DHS/FEMA
Audit Liaison, DHS/ICE
Audit Liaison, DHS/TSA
Audit Liaison, DHS/USCIS
Audit Liaison, DHS/USCG

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.