OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-IT-17-61 | Office of Audits | September 2017

Audit of the Department of State's Efforts to Detect and Address the Use of Unapproved Portable Devices

INFORMATION TECHNOLOGY DIVISION

OIG HIGHLIGHTS

AUD-IT-17-61

September 2017
OFFICE OF AUDITS
Information Technology Division

Audit of the Department of State's Efforts to Detect and Address the Use of Unapproved Portable Devices

What OIG Audited

Protecting sensitive information is one of the Department of State's (Department) greatest responsibilities and challenges. Portable devices, such as miniature or external hard drives and thumb drives, provide users the capability to easily transport business and personal information, as well as other data. As their use increases, however, so do the associated risks because the properties that make these devices portable and enable their convenient connections also increase the risk of data loss and the introduction of malware.

The Office of Inspector General (OIG) conducted this audit to determine whether the Department has implemented a process to detect the use of unapproved portable devices, as required by Federal and Department requirements, and has taken action to address instances in which unapproved portable devices have been used.

What OIG Recommends

OIG made seven recommendations to the Bureau of Information Resource Management (IRM), one of which is in coordination with the Bureau of Diplomatic Security (DS), to enhance controls over the identification of unapproved portable devices and to prompt action when unapproved devices are detected. On the basis of IRM's response to a draft of this report, OIG considers five recommendations resolved, pending further action, and two recommendations unresolved. A synopsis of IRM's comments regarding the recommendations offered and OIG's reply follow each recommendation in the Results section of this report. IRM's response to a draft of this report is reprinted in its entirety in Appendix B.

What OIG Found

Department policy prohibits the use of non-Department owned portable devices on the Department's systems. OIG found that the Department has implemented methods to detect the use of unapproved portable devices. For example, IRM's Office of Operations, Information Technology Infrastructure Office, Systems Integrity Division uses software to detect when unapproved portable devices are connected to Department systems based on the Enterprise Master List, which is a list that contains both authorized and excluded devices. DS also identifies the use of unapproved devices through its requirement that employees report cybersecurity incidents. These approaches can nonetheless be improved. Specifically, the Systems Integrity Division should keep current its list of approved and excluded portable devices to further protect the network from unapproved portable devices. Moreover, the Systems Integrity Division has not implemented an effective method to verify the approval of authorized portable devices that have been added to the Enterprise Master List. Inadequate controls with respect to these issues increases the risk of data loss and the introduction of malware.

OIG also found that the Department has taken action to address instances in which unapproved portable devices have been used. In addition to automatically blocking unapproved portable devices from connecting, the Systems Integrity Division informally follows up on some reported incidents. DS also follows up on unauthorized portable devices reported by Department employees. Again, these processes can be enhanced. For example, the Systems Integrity Division needs to formalize its processes for following up on incidents and documenting the remediation of the incident. In addition, the Systems Integrity Division and DS should collaborate to clarify their respective roles and responsibilities to maximize effectiveness.

CONTENTS

OBJECTIVE

The Office of Inspector General (OIG) conducted this audit to determine whether the Department of State (Department) has implemented a process to detect the use of unapproved portable devices, as required by Federal and Department requirements, and has taken action to address instances in which unapproved portable devices have been used.

BACKGROUND

Protecting sensitive information is one of the Department's greatest responsibilities and challenges. Portable devices—such as miniature or external hard drives, Universal Serial Bus (USB) keys (also known as flash drives or thumb drives), personal audio players, and tablets—provide users the capability to easily transport business and personal information, as well as other data. These portable devices can be small enough to fit into a shirt pocket, relatively inexpensive, and used to store a large amount of information (digital data). As their use increases, however, so do the associated risks. The properties that make these devices portable and enable them to have convenient connections increases the risk of data loss as well as the risk of mishandling sensitive information[1] and personally identifiable information (PII).[2] Moreover, the uncontrolled proliferation of portable devices increases the risk of network-based attacks.[3]

In numerous instances, the Government has been harmed by employees and contractors who have removed sensitive or PII data using portable devices. In one example, which occurred in April 2016, PII and other sensitive information for approximately 44,000 Federal Deposit Insurance Corporation customers was taken by a departing employee. According to an agency memorandum, the employee "downloaded the information to a personal storage device" inadvertently and without malicious intent. This example demonstrates how easily Government data can be taken from a Government facility on unapproved portable devices and how tenuous Federal cyber defenses are.[4] Furthermore, the use of unapproved portable devices can lead to

[1] National Institute of Standards and Technology (NIST), Internal/Interagency Reports 7298 (rev. 2), "Glossary of Key Information Security Terms," defines sensitive information as "information that the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled…but that has not been specifically authorized…to be kept classified in the interest of national defense or foreign policy."

[2] According to NIST Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

[3] *The Risks of Using Portable Devices*, by Pennie Walters, Carnegie Mellon University, 2012. This report was prepared for the United States Computer Emergency Readiness Team, a Government organization.

[4] The employee reportedly downloaded information to a personal storage device "inadvertently and without malicious intent," http://thehill.com/policy/cybersecurity/275814-fdic-suffers-inadvertent-data-breach, accessed on October 25, 2016.

malware being uploaded onto an organization's network. For example, in 2008, Government analysts discovered malware on the Secret Internet Protocol Router Network, which the Defense and State Departments use to transmit classified material. The malware also infected the Joint Worldwide Intelligence Communication System, which carries top-secret information to U.S. officials throughout the world. One "likely scenario", supported by a former Government official, is that an American soldier, official, or contractor in Afghanistan—"where the largest number of infections occurred"— used a thumb drive in an infected computer at an Internet cafe, and later inserted the drive in a classified machine. "Once a computer became infected, any thumb drive used on the machine acquired a copy of the malware," and the malware was then transferred to other computers.[5]

The Department prohibits the connection of unauthorized hardware or electronic devices to Department networks. This action is identified as a cybersecurity violation. The Department defines, unauthorized hardware or electronic devices as: (1) Department-owned hardware or electronic devices not authorized by one of the Department's Information Technology Configuration Control Board (IT CCB) or Local Configuration Control Board (CCB), as appropriate for the specific system; (2) Department-owned hardware or electronic devices authorized by one of the IT CCB or CCBs but not authorized for connection by the affected system owner or their representative; and (3) hardware or electronic devices not owned by the Department (that is, personally owned or contractor owned).[6]

Roles and Responsibilities

Many bureaus and organizations within the Department have a responsibility to maintain a strong IT security posture. The Bureau of Information Resource Management (IRM) manages and coordinates the Department's information resources and technology infrastructure and provides core services. To conform with national and Department policies and regulations, IRM's Systems Integrity Division administers key management infrastructure policy, standards, and procedures regarding information assurance and systems integrity. The Systems Integrity Division also provides technical security oversight and management for mainframe security, cryptographic services, and information integrity.

The Bureau of Diplomatic Security (DS) develops and implements computer and information security. Specifically, the Office of Information Security which reports to the Senior Coordinator for Security Infrastructure within DS, is responsible for the Department's information protection programs. Posts also have an important role in IT security. Post information systems security officers monitor the use of local post networks to ensure compliance with the Department's information security policies.[7]

[5] https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html?utm_term=.ed8c6e99b41b, accessed on July 29, 2017.

[6] According to the Foreign Affairs Manual (FAM), 12 FAM 592.2, "Cyber Security Violations." (B)(9)(b)

[7] 12 FAH-10 H-262.6-2, "Media Use – System Administrator Responsibilities."

The IT CCB, which is led by the Enterprise Network Management Office in IRM, manages changes to the Department's IT infrastructure. The IT CCB is concerned with the availability, reliability, integrity, security, interoperability, and performance of the IT infrastructure and is charged with ensuring that it does not degrade any IT performance. The IT CCB is a central point for evaluating change. When a change affects the Department's IT infrastructure or has the potential for affecting the infrastructure, that change must be assessed and the IT CCB advises on the change. The Department allows bureaus and posts to have their own local CCBs. Local CCBs are involved in the process to acquire IT projects at the bureau or post. The local CCB will assess whether the IT asset will migrate outside the local IT domain. If the IT asset is going to be connected to OpenNet,[8] then it must be presented to the Department's IT CCB for evaluation to ensure that it does not adversely affect the network.

AUDIT RESULTS

Finding A: The Department Has Implemented a Process to Detect the Use of Unapproved Portable Devices but the Process Can Be Improved

Department policies provided that portable devices not owned by the Department may not be connected to the Department's systems. OIG found that the Department has implemented methods to detect the use of unapproved portable devices. For example, the Systems Integrity Division uses software to detect the use of unapproved[9] portable devices based on a list it maintains of both authorized[10] and excluded[11] devices. DS also identifies the use of unapproved devices through its requirement for employees to report cybersecurity incidents affecting the Department's networks. These approaches, however, can be improved. Specifically, the list of authorized and excluded devices that the Systems Integrity Division maintains should be continuously updated to further protect the network from unapproved portable devices. In addition, the Systems Integrity Division has not implemented an effective method to verify approved portable devices that have been authorized and added to the Enterprise Master List. The Systems Integrity Division could address this issue by establishing a process to verify approved devices that the bureaus and posts have proposed for use. The Department could also improve its process by clarifying the roles, responsibilities, and authorities of the Systems Integrity Division and DS in detecting devices, enforcing Department policy, and generally safeguarding the network against the use of unapproved portable devices. Inadequate controls in these areas increases the risk of data loss and the introduction of malware.

[8] OpenNet is a Sensitive But Unclassified network that supports Department email services and data applications.

[9] For the purpose of this audit, an unapproved device is any device not approved by the Department for use or that is personally owned.

[10] For the purpose of this audit, an authorized device is any device approved by a post or bureau for use that has been added by IRM to the Enterprise Master List.

[11] For the purpose of this audit, an excluded device is any device requested by a post or bureau that is denied use on the network and added to the Enterprise Master List.

Department Efforts to Detect Unapproved Portable Devices

The Department requires[12] that only Federal Information Processing Standard (FIPS) 140-2[13] compliant portable devices approved by the Department's IT CCB be used on the Department's networks. Furthermore, Department policy states that "users must not physically or wirelessly connect any portable device not owned by the Department to any Department system or network unless the person uses a remote access program for the connection (that is, a wireless connection not a physical connection.)"[14,15]

OIG found that the Department has implemented several methods to detect the use of unapproved portable devices. For example, the Systems Integrity Division uses Symantec Endpoint Protection Application and Device Control (ADC) software[16] to monitor and detect the use of unapproved portable devices on the Department's OpenNet. Symantec is enterprise-wide software that is deployed to all of the Department's desktop computers as part of the standard desktop computer configuration. Symantec can identify and take action on "rules" that are violated. For example, the Department has set up a rule to identify and block the use of any portable device on the network that is not allowed according to the Department's "Enterprise Master List."

To facilitate using the ADC software, the Systems Integrity Division has created an "Enterprise Master List," which has two parts. One part is a list of excluded devices (such as devices that use Bluetooth technology) that the ADC software will identify and block. The other part of the Enterprise Master List is a list of authorized devices, which includes a description of allowed devices, such as the brand name (for example, IronKey) and type of device (for example, USB).[17] In addition, each post and bureau has autonomy to determine the types of portable devices that users are permitted to connect to the local network, which means that one post might allow a type of portable device that another post does not permit. Therefore, the devices authorized or excluded on the Enterprise Master List for one post or bureau could deviate from devices authorized or excluded by another post or bureau. Any item included on the Authorized Devices List is permitted on OpenNet, and the ADC software will not identify its use as an exception.

---

[12] According to 5 FAM 469.4, "Avoiding Technical Threats to Personally Identifiable Information (PII)," unclassified media "must be encrypted to the Federal Information Processing Standards (FIPS) 140-2, or later National Institute of Standards and Technology (NIST) standard. The Information Technology Configuration Control Board (IT CCB) must also approve the encryption product."

[13] FIPS 140-2, "Security Requirements for Cryptographic Modules," issued by NIST, coordinates the requirements and standards for cryptography modules that include both hardware and software components.

[14] Foreign Affairs Handbook, 12 FAH-10 H-165.1, "Access Control for Non-Department-Owned Mobile Devices – Management Responsibilities."

[15] In essence, this provision addresses a situation in which someone obtains access to OpenNet remotely, through the Department's Global OpenNet, by using a non-Department computer.

[16] According to the Symantec website (symantec.com), Symantec ADC software enables extra security protection for client systems. Simple rules can enforce security procedures and stop unknown malware.

[17] The Authorized Device List does not describe devices by a specific identification number (such as a serial number).

While the Department has implemented technical solutions on desktops connected to OpenNet, enterprise-wide efforts alone cannot achieve the Department's goal of protecting sensitive information and preventing network-based attacks, which is why posts and bureaus also need to be involved in the process. Therefore, in addition to the enterprise-wide use of ADC software, the Systems Integrity Division allows bureaus and posts to use a locally-administered copy of the ADC software to detect the use of unapproved or excluded portable devices at the bureau or post level. This provides an additional layer of oversight on the use of portable devices. According to Department officials, 80 bureaus and posts[18] have implemented post-specific ADC software.

Although DS does not scan the network for unapproved or excluded devices, it assists with identifying these devices. Specifically, DS is responsible for the Department's Cyber Incident Response Team (CIRT), which serves as the Department's focal point for reporting cybersecurity incidents affecting the Department's networks.[19] Bureau or post employees will notify CIRT when they determine that unapproved or unauthorized devices were used on the bureau or post network, and CIRT maintains a record of that information. From October 1, 2015, to January 1, 2017, CIRT received and documented a total of 48 reports of unapproved devices connected to the Department's network.

Notwithstanding these efforts to detect the use of unapproved portable devices on OpenNet, the Department's overall approach can be improved. The National Institute of Standards and Technology (NIST) Special Publication 800-53[20] states that organizations should develop and document an inventory of information system components that meets the level of granularity needed for tracking and reporting. The United States Computer Emergency Readiness Team (US-CERT)[21] also suggests creating an inventory of mobile devices permitted to carry sensitive company information and auditing this inventory on a regular basis.[22] As noted previously, the Systems Integrity Division created the Enterprise Master List to maintain a list of authorized portable devices. To update the Enterprise Master List, bureaus and posts submit requests to the Systems Integrity Division to add portable devices to the list.

OIG found that the Systems Integrity Division relies on bureaus and posts to keep the information on the Enterprise Master List updated. A Systems Integrity Division official stated that once a device is added to the Enterprise Master List, it stays on the list until a bureau or post requests that the item be removed. The official also stated that a review of the Enterprise

[18] Some bureaus and posts chose not to participate in this IRM initiative.

[19] 1 FAM 262.7-2(A), "Monitoring and Incident Response Division."

[20] NIST Special Publication 800-53 (rev. 4), "Security and Privacy Controls for Federal Information Systems and Organizations," CM-8, Information System Component Inventory.

[21] US-CERT is part of the Department of Homeland Security and its mission includes providing boundary protection for the Federal civilian executive domain and cybersecurity leadership.

[22] *The Risks of Using Portable Devices*, by Pennie Walters, Carnegie Mellon University, 2012.

Master List only occurs when a bureau or post requests that the Systems Integrity Division remove a device from the list. As previously explained, the ADC software uses the information from the Enterprise Master List to identify excluded devices and, if the information is not kept current, the list itself could include items that are no longer approved by the post. Consequently, the scanning software may not identify devices that should no longer be used on OpenNet. Moreover, the Systems Integrity Division does not verify the accuracy of the information input by bureaus and posts, so devices that were not approved by the local CCBs could also be added to the Enterprise Master List. Without a current, complete, and verified list of authorized devices, the scans will not be as effective as they could be, which increases the risk that an undetected device could be connected to the network and introduce malware.

US-CERT also suggests limiting the number of portable devices that are supported by a system, to make it easier to identify unapproved devices.[23] Currently, the IT CCB only authorizes the use of IronKey brand USB devices. In fact, the Systems Integrity Division has a Blanket Purchase Agreement with Kingston Digital for IronKey USB devices.[24] However, local CCBs are permitted to approve the use of other types of portable devices at their bureau or post as long as the devices are generally consistent with what the enterprise-wide IT CCB allows (that is, FIPS 140-2 compliant). If the Department committed to limiting the types of permitted portable devices, it would improve the efficiency of the oversight. According to the Chief Information Officer, IRM would not be able to limit the number of different brands of portable devices that can be connected to OpenNet because it would not comply with Federal Acquisition Regulation requirements for full and open competition. IRM officials' comments are inaccurate because, as noted above, IRM has already established a Blanket Purchase Agreement for IronKey devices that bureaus and posts can use. Limiting the brands of portable devices that can be used on the system to items acquired using the Blanket Purchase Agreement would not violate acquisition requirements for full and open competition.

Process Could Be Improved by Validating Information and Clarifying Roles and Responsibilities

The Systems Integrity Division could improve the process by which it identifies unapproved or excluded devices by establishing a process to validate the information submitted by bureaus and posts to the Enterprise Master List. Currently, the Systems Integrity Division does not perform any steps to validate the completeness or accuracy of the information entered into the Enterprise Master List by bureaus and posts. For example, the Systems Integrity Division does not have a process in place to periodically validate that the information on the Enterprise Master List is current and consistent with Department policy. Furthermore, the Systems Integrity Division does not have a process in place to verify that the portable device types entered into the Enterprise Master List by bureaus and posts have been approved by the local CCBs and comply with Department requirements for portable devices.

[23] Ibid.

[24] IronKey encrypted USB devices comply with the FIPS standards.

Another potential improvement would be to clarify the roles and responsibilities of the Systems Integrity Division for the program. Although the Systems Integrity Division is responsible for administering key management IT infrastructure policies, standards, and procedures related to information assurance and systems integrity, the office sees its role as a facilitator rather than a program manager. For example, as described previously, although the Systems Integrity Division has suggested the use of one USB brand—IronKey—in cables to all posts; it has not required use of this brand, even though it would improve the efficiency of identifying unapproved or excluded devices when they are connected to the Department's network. A Systems Integrity Division official stated that the Systems Integrity Division has no authority to approve or exclude devices used on local bureau and post networks. This is an overly narrow view of the role and responsibilities of the System Integrity Division. Pursuant to the FAM, IRM exercises designated approving authority for developing and administering the Department's computer and information security programs and policies.[25] If the Systems Integrity Division clarified its role in identifying unapproved or excluded portable devices used on the Department's OpenNet, it would improve controls over the use of portable devices. Furthermore, the Systems Integrity Division should determine the advantages and disadvantages of limiting the number of brands of portable devices allowed on the Department's OpenNet and develop a Department policy based on that analysis. Since the Systems Integrity Division is responsible for administering IT infrastructure policies for the Department, this Office should create guidelines to control the use of portable devices.

Inadequate Controls Over Portable Devices Could Increase the Risk of Data Loss

According to US-CERT, "TechAdvisory.org reports that 25 percent of malware (malicious programs) is spread today through USB devices." These devices may contain malware that can be copied to the computer unknowingly. Once the malware infects a computer, it can spread to other computers on the network. According to US-CERT, storage devices can also "give malicious insiders the opportunity to steal data easily and inconspicuously because the devices are easy to hide and their use is hard to track." Moreover, due to the "small size and portability" of the devices, the risk of loss is increased, which increases the potential for irreparable data exposure or loss. If the lost device contains sensitive or proprietary Department information, it could jeopardize the reputation of the organization or the security of employees.

Recommendation 1: OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically verify that the Enterprise Master List is kept current and complete.

Management Response: IRM concurred with the recommendation stating that it had "established procedures to ensure only accurate information is populated in the Enterprise Master List." IRM also stated that it will "expand procedures to ensure the list is validated quarterly and is as accurate as possible."

[25] 1 FAM 270, "Bureau of Information Resource Management"

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has developed and implemented a process to periodically verify that the Enterprise Master List is kept current and complete.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management (IRM) develop and implement a process to verify that a Local Configuration Control Board has authorized the type of portable device requested each time a bureau or post requests that IRM add a type of portable device to the Enterprise Master List.

Management Response: IRM concurred with the recommendation stating that it is "reviewing and analyzing all process and policies related to Local Configuration Control Boards."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has developed and implemented a process to verify that a Local Configuration Control Board has authorized the type of portable devices requested each time a bureau or post requests that IRM add a type of portable device to the Enterprise Master List.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management enforce its authority to administer the use of portable devices in the Department of State, as well as the policies, standards, and procedures related to portable devices.

Management Response: IRM concurred with the recommendation stating that it is "reviewing and analyzing all process and policies related to Local Configuration Control Boards."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers this recommendation resolved pending further action. The response to Recommendation 3, taking into consideration the concurrence and proposed actions for Recommendations 1 and 2, which will require IRM to not only review but also enforce its authority over the usage of USB devices, addresses the recommendation.as required by Recommendation 3. Specifically, by establishing policies and procedures to ensure the Enterprise Master List is accurate and reviewing and analyzing processes and procedures related to the Local CCBs, IRM is demonstrating a plan to take a more active, authoritative, role in the administration of portable devices. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM enforced its authority to

administer the use of portable devices in the Department, as well as the policies, standards, and procedures related to portable devices.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management (IRM) perform and document an analysis of the advantages and disadvantages to limiting the brands of portable devices that are allowed to be connected to OpenNet, including connection though local networks. From the completed analysis, IRM should determine whether to limit or not limit the brands of portable devices.

Management Response: IRM did not concur with the recommendation, stating that each device is submitted to the Enterprise Configuration Control Board and is examined prior to allowing it to be added to the network. This board ensures all applicable safeguards and requirements are incorporated into the devices. Because of this, restricting devices based on brand name will not increase the security of the network and would remove vendor competition. This would result in increased costs to the Department.

OIG Reply: On the basis of IRM's non-concurrence with the recommendation, OIG considers this recommendation unresolved. As presented in this report, the primary reason to of limit the brands of portable devices used in an organization is to make it easier to identify unapproved devices and improve oversight of the devices connected to the network. Further, as presented in this report, IRM did not, in fact, determine if authorized devices had been approved by the Local CCB before being added to the Enterprise Master List.

In August 2016, IRM attempted to restrict the use of USB devices. In a cable to all posts dated August 1, 2016, IRM announced that it had established a new blanket purchase agreement for the procurement of encrypted/secure USB devices. The cable specifically stated, "Only IronKey Enterprise devices are to be used on the Department's OpenNet network. For this reason, the purchase and use of IronKey Basic devices is not authorized." IRM did not enforce this directive, and the local CCBs are currently permitted to approve the use of other types of portable devices at their bureau or post. To suggest that this approach is somehow inconsistent with "vendor competition" is both inaccurate and inconsistent with IRM's own prior practice. Therefore, OIG maintains that, as recommended, IRM should give careful consideration to limiting the brands of portable devices used on OpenNet, as advised by US-CERT. IRM's attention to this detail is necessary and warranted because, according to US-CERT, 25 percent of malware (malicious programs) is spread today through USB devices.

This recommendation will be considered resolved when IRM agrees to fully consider limiting the brands of portable devices that can be connected to the network, or provides an acceptable alternative that meets the intent of the recommendation, which is to improve oversight of the devices connected to OpenNet and facilitate the discovery and removal of unapproved devices. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has fully considered limiting the brands of portable devices that are allowed to be connected to OpenNet, including connection though local networks.

Recommendation 5: If the Bureau of Information Resource Management (IRM) determines that it should limit the brands of portable devices that are allowed to be connected to OpenNet (Recommendation 4), OIG recommends that IRM develop and issue a policy that implements this determination.

Management Response: IRM did not concur with the recommendation based on explanations cited in responses to Recommendations 3 and 4.

OIG Reply: On the basis of IRM's non-concurrence with the recommendation, OIG considers this recommendation unresolved. Because this recommendation is dependent on the implementation of Recommendation 4, OIG will consider this recommendation resolved when IRM has fully considered limiting the brands of portable devices that are allowed to be connected to OpenNet and determines if a policy directive is warranted. This recommendation will be closed when IRM has determined the extent to which portable devices are allowed to connect to OpenNet and has developed and issued a corresponding policy directive to implement that determination.

Finding B: The Department Has Taken Action to Address Potentially Unapproved Portable Devices but the Process Can Be Enhanced

OIG found that the Department has taken action to address instances in which unapproved or excluded portable devices have been used. For example, the Systems Integrity Division uses Symantec ADC software to automatically block unapproved or excluded portable devices on the Department's OpenNet. In addition, the Systems Integrity Division analyzes reports generated from the ADC software and informally follows up on some incidents. Furthermore, DS officials stated that DS follows up on unauthorized portable devices reported by a Department employee to CIRT. Although the Department has processes in place to take action when unapproved portable devices are identified, these processes could be enhanced. For example, the Systems Integrity Division should formalize its processes for analyzing the ADC reports, following up on incidents included in the ADC reports, and documenting the remediation of incidents. In addition, the Systems Integrity Division and DS should collaborate to clarify each group's respective roles, responsibilities, and authorities to maximize effectiveness. Unless controls are improved, there is increased risk that cybersecurity violations may not be promptly detected and malware could be spread.

Department Efforts to Take Action When Unapproved Devices Are Identified

As reported in Finding A of this report, Department policy states that "users must not physically or wirelessly connect any portable device not owned by the Department to any Department system or network unless the person uses a remote access program for the connection (which would be a wireless connection, not a physical connection)."[26] After identifying instances of potential noncompliance with the Department's policies on the use of portable devices, the next

[26] 12 FAH-10 H-165.1, "Access Control for Non-Department-Owned Mobile Devices – Management Responsibilities."

step is for the Department to address the noncompliance. OIG found that the Department has taken action to address instances in which unapproved devices have been used in the Department's OpenNet system; however, the methods employed can be enhanced.

The Department addresses the use of unapproved devices is primarily by blocking the devices. The Systems Integrity Division uses Symantec ADC software to automatically block unapproved or excluded portable devices on the Department's OpenNet. Using technology to enforce important IT policies is key to efficiently and effectively preventing data loss. Blocking the use of unapproved portable devices on OpenNet is an important step in safeguarding against potential data loss.

In addition to blocking unapproved or excluded portable devices, the ADC software generates daily reports of attempts to use an unapproved or excluded device on OpenNet. This report includes information on the location the attempt was made, the device name, the device type, and a vendor identifier, and the information is sorted into critical, major, and minor event categories.[27] From October 1, 2015, to January 1, 2017, the ADC software identified 259,658 incidents where someone attempted to use unapproved USBs on OpenNet. This listing consisted of 19 different types of devices that were blocked at 86 different locations worldwide. According to the Systems Integrity Division officials, analysts review each report generated from the ADC software and informally follow up on some incidents. In general, the reviews are based on the "intuition" of each analyst. For example, if an analyst sees significant increases in the number of exceptions from one post or if critical exceptions are identified, then the Systems Integrity Division analyst may assess the item.

When an analyst decides to follow up on exceptions included in the report, the Systems Integrity Division analyst might contact a post to determine why there is an increase in the number of exceptions. According to the Systems Integrity Division officials, in such cases, a post has often not requested that a type of portable device be included on the Enterprise Master List of devices authorized for use. Although this follow up is a useful control that can limit the misuse of portable devices, the Systems Integrity Division has not formalized the analysis of the ADC reports or the overall follow-up process for identified incidents. According to the Systems Integrity Division officials, analysts do not maintain information on the incidents that received follow-up or the resolution of those incidents.

In addition to performing its own analysis, the Systems Integrity Division electronically transfers data from the ADC reports to DS every 2 calendar days. The data is transferred to electronic software used by DS known as Splunk. Splunk searches and analyzes streams of machine data generated by an IT system and allows users to investigate security incidents more quickly. According to DS officials, the information from the ADC software provided by the Systems Integrity Division is archived in Splunk; however, DS officials stated that DS generally does not

[27] A critical event represents a significant risk for a security incident, and a minor event is considered low risk. Attempting to connect an unapproved portable device to OpenNet is normally considered to be a minor event.

use the provided data. DS may use the information on an ad hoc basis and only if it is following up on another issue, such as a zero day vulnerability[28] or ransomware.

Although DS does not routinely analyze the ADC data provided by the Systems Integrity Division, DS officials stated that DS follows up on any unauthorized portable devices reported by a Department employee to CIRT. Part of the DS remediation process includes notifying the Cybersecurity Incident Program[29] of the potential issue. DS also contacts the information system security officers from the bureaus or offices that reported the incidents to confirm that they are aware of the incidents and the required remediation. In total, from October 1, 2015, to January 1, 2017, CIRT received and documented 48 reports of unapproved portable devices. Although DS stated that it follows up on each item reported to CIRT, for 48 incidents of unapproved portable devices reported to DS, OIG tested a sample of 10[30] and noted 2 occasions in which DS could not demonstrate that the incident had been remediated. One of the two incidents occurred at Consulate Mumbai, India, when a smart phone being charged in a user workstation was visually identified. The second incident occurred at a Bureau of Consular Affairs' office, when an IPod was found to have been connected to the system. In both cases, no documentation supported that the incident was fully addressed.

Process Could Be Improved by Developing Policies and Clarifying Roles and Responsibilities

According to the Government Accountability Office, management should implement control activities through policies, and these policies should be documented.[31] The Department could improve its efforts to address the use of unapproved portable devices if the Systems Integrity Division formalized its processes for analyzing the ADC reports, following up on incidents included in the ADC reports and documenting the remediation of the incident. The Systems Integrity Division does not have internal operating procedures to provide guidance on how to analyze the ADC reports or how to identify the highest risk exceptions that require follow-up. Furthermore, the Systems Integrity Division does not have policies and procedures requiring analysts to document efforts to follow up on incidents or any remediation taken as a result.

The Department could also improve its efforts to address the use of unapproved portable devices by clarifying the roles and responsibilities of the Systems Integrity Division and DS. According to the Foreign Affairs Manual, (FAM) , the Systems Integrity Division is responsible for administering key management infrastructure policy, standards, and procedures regarding information assurance and systems integrity.[32] DS is responsible for ensuring the security of the

[28] A zero day vulnerability is a vulnerability whose details are unknown by the vendor or users. The vulnerability can then be exploited by a hacker before the user becomes aware of it.

[29] The Cybersecurity Incident Program is administered by the Program Application Division within DS.

[30] The final sample was eight, as two of the sampled incidents were identified as duplicates.

[31] Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

[32] 1 FAM 275.2-3, "Systems Integrity Division."

Department's global information and information assets, managing the security incidents program, and managing the insider threat program. The Systems Integrity Division officials expressed their belief that DS should have a more prominent role in assessing the exceptions identified by the ADC software. However, DS officials stated that, because the vast majority of attempts to use unauthorized USB devices on OpenNet are "policy violations," not malicious activity, the Systems Integrity Division should be responsible. To ensure effective oversight of the use of unapproved portable devices, it is essential for involved parties to have a clear understanding of their roles and responsibilities.

Cybersecurity Violations May Not Be Identified and Malware May Be Spread

According to the FAM, connecting unauthorized hardware or electronic devices to Department networks is a cybersecurity violation.[33] Although the Department is mitigating much of the risk of losing data by blocking the use of unapproved portable devices, the Department does not follow up on all instances in which employees attempt to use an unapproved portable device. As a result, it is not documenting all cybersecurity violations. Furthermore, according to US-CERT, "25 percent of malware (malicious programs) is spread today through USB devices."[34] These devices may contain malware that can be copied to the computer unknowingly. Once the malware infects a computer, it can spread to other computers on the network. Unless employees who are violating Department policies are identified and the issue is promptly addressed, employees may repeatedly attempt to connect unapproved devices, thereby increasing the risk of malicious code being uploaded to the Department's network. In addition, blocking the use of unapproved devices helps to safeguard the Department's network. However, to detect and address instances in which unapproved or excluded devices are added to the network, it is vital that the list of authorized and excluded devices is kept current and complete. Because of the possibility of inaccurate or incomplete information regarding authorized devices, the Department faces an ongoing risk that someone may inappropriately take sensitive data from the Department. Keeping the list of authorized and excluded devices current may mitigate this risk.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management develop and implement formal, standardized procedures for regularly performing an analysis of the Symantec Endpoint Protection Application and Device Control reports. At a minimum, the procedures should provide guidance for analysts on how to review the Symantec reports, how to identify high risk exceptions for follow-up, what actions should be taken during follow-up, and how to document the follow-up and the remediation taken.

[33] "Cyber Security Violations," 12 FAM 592.2, identifies a list of cybersecurity violations, one of which is "(9) Connection of unauthorized hardware/electronic devices to Department networks."

[34] *The Risks of Using Portable Devices*, by Pennie Walters, Carnegie Mellon University, 2012. Produced for US-CERT, a Government organization.

Management Response: IRM concurred with the recommendation stating that it will "develop and implement formal, standardized procedures related to the analysis of the Symantec Endpoint Protection Application and Device Control reports. These reports will include guidance for analysis on how to review the Symantec reports, how to identify high risk exceptions for follow up, what actions should be taken during follow up, how to document the follow up, and the remediation taken."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has developed and implemented formal, standardized procedures for regularly performing an analysis of the Symantec Endpoint Protection Application and Device Control reports.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, develop and implement formal procedures to identify and remediate cybersecurity policy violations created when employees connect unapproved portable devices to OpenNet. The formal procedures should include a description of each bureau's roles and responsibilities in the process.

Management Response: IRM concurred with the recommendation stating that it will work with Diplomatic Security to document roles and responsibilities as well as the implementation of formal procedures to identify and remediate cybersecurity violations associated with unapproved portable devices.

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM, in coordination with DS, has developed and implemented formal procedures to identify and remediate cybersecurity violations associated with unapproved portable devices.

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically verify that the Enterprise Master List is kept current and complete.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management (IRM) develop and implement a process to verify that a Local Configuration Control Board has authorized the type of portable device requested each time a bureau or post requests that IRM add a type of portable device to the Enterprise Master List.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management enforce its authority to administer the use of portable devices in the Department of State, as well as the policies, standards, and procedures related to portable devices.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management (IRM) perform and document an analysis of the advantages and disadvantages to limiting the brands of portable devices that are allowed to be connected to OpenNet, including connection though local networks. From the completed analysis, IRM should determine whether to limit or not limit the brands of portable devices.

Recommendation 5: If the Bureau of Information Resource Management (IRM) determines that it should limit the brands of portable devices that are allowed to be connected to OpenNet (Recommendation 4), OIG recommends that IRM develop and issue a policy that implements this determination.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management develop and implement formal, standardized procedures for regularly performing an analysis of the Symantec Endpoint Protection Application and Device Control reports. At a minimum, the procedures should provide guidance for analysts on how to review the Symantec reports, how to identify high risk exceptions for follow-up, what actions should be taken during follow-up, and how to document the follow-up and the remediation taken.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, develop and implement formal procedures to identify and remediate cybersecurity policy violations created when employees connect unapproved portable devices to OpenNet. The formal procedures should include a description of each bureau's roles and responsibilities in the process.

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

The Office of Inspector General (OIG) conducted this audit to determine whether the Department of State (Department) has implemented a process to detect the use of unapproved portable devices, as required by Federal and Department requirements, and has taken action to address instances in which unapproved portable devices have been used.

The Office of Audits performed this audit from December 2016 to June 2017. Audit work was performed in the Washington, DC, metropolitan area. OIG conducted this performance audit in accordance with generally accepted Government auditing standards. These standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions presented in this report.

To obtain background information for this audit, including criteria, OIG researched and reviewed Federal policies relating to maintaining controls over portable devices, such as guidance from the National Institute of Science and Technology (including the Federal Information Processing Standard) and the United States Computer Emergency Readiness Team, as well as Department policies such as the Foreign Affairs Manual (FAM) and the Foreign Affairs Handbook. OIG also interviewed key personnel, including individuals from the Bureau of Information Resource Management (IRM) and the Bureau of Diplomatic Security (DS) to gain an understanding of the Department's processes and to evaluate operational controls. Furthermore, OIG observed daily operations and collected written documents to supplement observations and interviews. These observations included a walkthrough of the Symantec Endpoint Protection Application and Device Control (ADC) operations, including adding a new device to the Enterprise Master List. OIG observed the process for generating ADC application logs after system scans have been performed. In addition, OIG performed a walkthrough of the remediation process with DS officials using the BMC Remedy system.[1] OIG reviewed historical data for the application logs from the Splunk tool to determine the number of blocked device incidents recorded during the period of review.

Work Related to Internal Controls

OIG performed steps to assess the adequacy of internal controls related to the areas audited. For example, OIG reviewed the IronKey Administrative Manual for an overview of the IronKey Enterprise program. In addition, OIG reviewed relevant FAM and Foreign Affairs Handbook chapters on both the use of portable devices and the penalties associated with misuse of

[1] BMC stands for the first initial of the three founder's last names. BMC Software founders Scott Boulette, John Moores, and Dan Cloer. Remedy is a trouble ticketing application used by organizations to track internal problems and customer reported issues. https://www.techwalla.com/articles/how-to-use-the-remedy-ticketing-system, accessed April 19, 2017.

portable devices. OIG also interviewed IRM and DS officials to obtain information on identifying unapproved portable devices. Issues identified during audit work related to internal controls are detailed in the "Audit Results" section of this report.

Use of Computer-Processed Data

In the course of this audit, OIG used electronically process data from the Symantec Endpoint Protection ADC software and the DS BMC Remedy Ticket system.

Symantec Endpoint Protection Application and Device Control Software

OIG assessed the reliability of the Enterprise Master List and the application logs (scan results) that are a product of the ADC application. OIG interviewed individuals knowledgeable of the system to gain an understanding of the list and application logs. To test the data, OIG used a search engine to filter the list for only Universal Serial Bus (USB) devices on the Enterprise Master List. After applying the filter, OIG selected the first 112 recorded USB devices from the list of 2,146 devices on the Enterprise Master List to gain specific information, such as locations of devices that were non-enterprise. IRM was unable to provide a location for 109 (97 percent) of the 112 selected devices. OIG determined that the IRM's inability to maintain locations of devices demonstrates insufficient information systems security controls. In addition, OIG requested documentation demonstrating that incidents identified in the application logs had been resolved. IRM officials stated they had no documentation to support that follow-up had occurred. As a result of these findings, OIG determined that the data received from the ADC tool, which included the Enterprise Master List and the application logs (scan results), was not sufficiently reliable. Therefore, OIG performed additional interviews and analyzed supplementary documentation to obtain sufficient information to fulfill the objective of the audit.

BMC Remedy Ticket System

OIG assessed the reliability of the DS BMC Remedy Ticket system. OIG interviewed individuals knowledgeable about the system to gain an understanding of the system. To test the data, OIG selected 10[2] of 48 remedy tickets related to USB incidents to evaluate the accuracy of the remediation of unapproved devices for the audit period. OIG reviewed the selected incidents with DS personnel in the Remedy Ticket Archive System and concluded that the information in the DS BMC Remedy Ticket system was sufficiently reliable to support the conclusions and recommendations presented in this report.

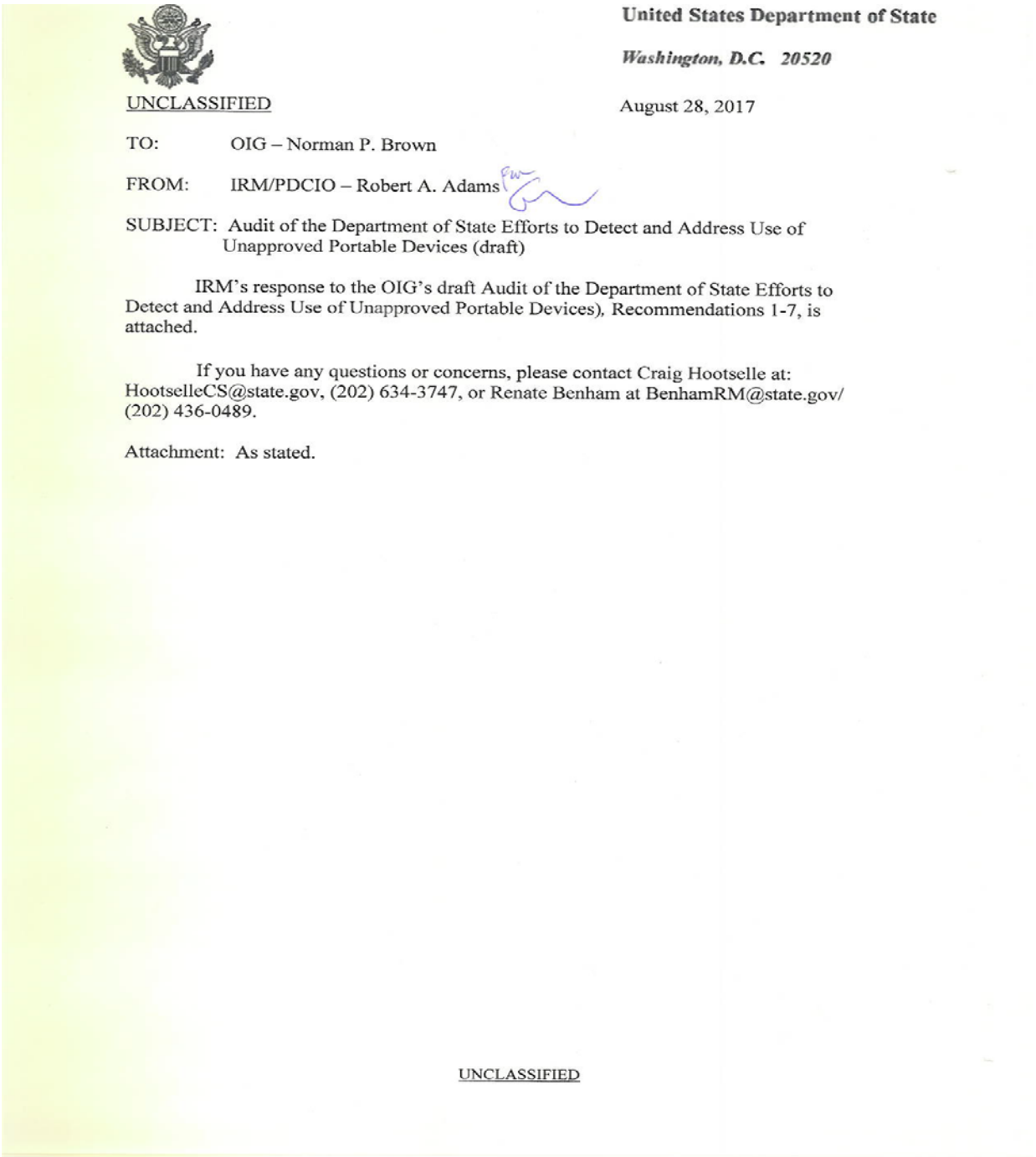
[2] The selection process is mentioned in the subsequent section.

Detailed Sampling Methodology

OIG's sampling objective was to test the effectiveness of the Department's implementation of information system security controls for detecting and addressing instances where unapproved portable devices were used. Specifically, OIG planned to assess the actions taken by the Department to address instances in which unapproved portable devices had been used.

DS provided OIG a universe of 48 incidents related to the use of unapproved devices, which DS remediated during OIG's review period from October 1, 2015, to January 1, 2017. OIG selected a group of tickets as a target universe to evaluate the effectiveness of the actions taken for remediation of unapproved devices. OIG selected 10 (21 percent) of 48 USB remedy tickets. The 10 tickets were chosen using the "Summary" and "Operational Categorization Tier 2" description of the incident, which aided the auditor's selection. OIG selected unauthorized removable media devices, computer security policy violations, and unauthorized connected hardware. After selecting the 10 tickets, two of the incidents were identified as duplicate incidents. For the remaining 8 tickets, OIG reviewed the items with DS personnel in the Remedy Ticket Archive System and determined that DS adequately managed the incidents reported to CIRT through the Remedy Ticket Archive System. OIG's results identified two incidents that lacked supporting documentation to demonstrate that DS had fully addressed the incidents. Details of these two incidents are presented in the "Audit Results" section of this report.

APPENDIX B: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE



United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

August 28, 2017

TO: OIG – Norman P. Brown

FROM: IRM/PDCIO – Robert A. Adams

SUBJECT: Audit of the Department of State Efforts to Detect and Address Use of Unapproved Portable Devices (draft)

IRM's response to the OIG's draft Audit of the Department of State Efforts to Detect and Address Use of Unapproved Portable Devices), Recommendations 1-7, is attached.

If you have any questions or concerns, please contact Craig Hootselle at: HootselleCS@state.gov, (202) 634-3747, or Renate Benham at BenhamRM@state.gov/ (202) 436-0489.

Attachment: As stated.

UNCLASSIFIED

Approved:	IRM: Frontis B. Wiggins	(ok)
Drafted:	IRM/BMP/SPO/SPD: Renate M. Benham (202) 436-0489 August 25, 2017	
Cleared:	IRM/PDCIO: Robert L. Adams	(ok)
	IRM/FO: Glenn W. Miller	(ok)
	IRM/IA: Al J. Bowden	(ok)
	IRM/OPS: Glen H. Johnson	(ok)
	IRM/BMP: Karen E. Mummaw	(ok)
	IRM/BMP/SPO: Kenneth D. Rogers	(ok)

(U) OIG Resolution Analysis
(U) *Audit of Department of State Efforts to Detect and Address Use of Unapproved Portable Devices (draft)*

(U) Recommendation 1: OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically verify that the Enterprise Master List is kept current and complete.

(U) Management Response to Draft Report: IRM concurs with this recommendation. Procedures have been established to ensure only accurate information is populated in the Enterprise Master List. IRM will expand procedures to ensure the list is validated quarterly and is as accurate as possible.

(U) Recommendation 2: OIG recommends that the Bureau of Information Resource Management (IRM) develop and implement a process to verify that a Local Configuration Control Board has authorized the type of portable device requested each time a bureau or post requests that IRM add a type of portable device to the Enterprise Master List.

(U) Management Response to Draft Report: IRM concurs with this recommendation. IRM is reviewing and analyzing all process and policies related to Local Configuration Control Boards (LCCB) 5 FAM 862.

(U) Recommendation 3: OIG recommends that the Bureau of Information Resource Management enforce its authority to administer the use of portable devices in the Department of State, as well as the policies, standards, and procedures related to portable devices.

(U) Management Response to Draft Report: IRM concurs with this recommendation. IRM is reviewing and analyzing all process and policies related to Local Configuration Control Boards (LCCB) 5 FAM 862.

(U) Recommendation 4: OIG recommends that the Bureau of Information Resource Management determine whether it should limited the brands of portable devices and are allowed to be connected to OpenNet, including connection through local networks, by identifying and analyzing the advantages and disadvantages.

(U) Management Response to Draft Report: IRM does not concur with this recommendation. Each device is submitted to the Enterprise Configuration Control Board and is examined prior to allowing it to be added to the network. This board ensures all applicable safeguards and requirements are incorporated into the devices. Because of this, restricting devices based on brand name will not increase the security of the network and would remove vendor competition. This would result in increased costs to the Department.

Recommendation 5: If the Bureau of Information Resource Management determines that it should limit the brands of portable devices that are allowed to be connected to OpenNet (Recommendation 4), OIG recommends that the Bureau of Information Resource Management develop and issue a policy that implements this determination.

(U) Management Response to Draft Report: IRM does not concur with this recommendation based on explanations cited in responses to Recommendations 3 and 4.

(U) Recommendation 6: OIG recommends that the Bureau of Information Resource Management develop and implement formal, standardized procedures for regularly performing an analysis of the Symantec Endpoint Protection Application and Device Control reports. At a minimum, the procedures should provide guidance for analysts on how to review the Symantec reports, how to identify high risk exceptions for follow-up, what actions should be taken during follow up, and how to document the follow up and the remediation taken.

(U) Management Response to Draft Report: IRM concurs with this recommendation. IRM will develop and implement formal, standardized procedures related to the analysis of the Symantec Endpoint Protection Application and Device Control reports. These reports will include guidance for analysis on how to review the Symantec reports, how to identify high risk exceptions for follow up, what actions should be taken during follow up, and how to document the follow up and the remediation taken.

(U) Recommendation 7: OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, develop and implement formal procedures to identify and remediate cybersecurity policy violations created when employees connect unapproved portable devices to OpenNet. The formal procedures should include a description of each bureau's roles and responsibilities in the process.

(U) Management Response to Draft Report: IRM concurs with this recommendation. IRM will work with Diplomatic Security to document roles and responsibilities as well as the implementation of formal procedures to identify and remediate cyber security violations associated with unapproved portable devices.

ABBREVIATIONS

ADC	Application and Device Control
CCB	Configuration Control Board
CIRT	Cyber Incident Response Team
DS	Bureau of Diplomatic Security
FAM	Foreign Affairs Manual
FIPS	Federal Information Processing Standard
IRM	Bureau of Information Resource Management
IT CCB	Information Technology Configuration Control Board
NIST	National Institute of Standards and Technology
PII	personally identifiable information
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team

OIG AUDIT TEAM MEMBERS

Jerry Rainwaters, Director
Information Technology Division
Office of Audits

Steve Matthews, Audit Manager
Information Technology Division
Office of Audits

James DeLoach, Senior IT Auditor in Charge
Information Technology Division
Office of Audits

Cassandra Williams, Senior Auditor
Information Technology Division
Office of Audits

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
HOTLINE@stateoig.gov
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
WPEAOmbuds@stateoig.gov