Smithsonian Institution

Office of the Inspector General

Date March 4, 2013

To Albert Horvath, Under Secretary for Finance and Administration and Chief Financial Officer
Deron Burba, Chief Information Officer

cc Patricia Bartlett, Chief of Staff, Office of the Secretary
Judith Leonard, General Counsel
Rebecca Hutchings, Acting Director of IT Security

From Scott S. Dahl, Inspector General

Subject Management Advisory Regarding Portable Computer Encryption (M-13-01)

INTRODUCTION

In our fiscal year 2010 FISMA review of the Smithsonian's information security program (Smithsonian Institution Information Security Program, March 15, 2011, Report No. A-10-01), we found that the Smithsonian was not enforcing its policy requiring that all mobile devices that may be used to store sensitive information be encrypted. We recommended that the Smithsonian implement controls to ensure that policy is enforced.

In a memorandum dated September 30, 2012, management informed us that it implemented the recommendation and requested that we close it. To determine if the actions management took were effective, we examined a sample of portable computers in units that routinely handle sensitive information. We found that most of the portable computers we tested were not encrypted. Management needs to ensure that portable computers that may be used to store sensitive information are properly encrypted. In addition, management needs to ensure that users are aware if a laptop is unencrypted and that it should not be used to store sensitive information. Therefore, we are keeping the recommendation open and making three more recommendations to assist management in implementing the original one.

BACKGROUND

The Office of Management and Budget issued Memorandum M-06-16 in June 2006 requiring all executive departments and agencies to encrypt all data on mobile computers/devices which carry agency data, unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or designee. The Smithsonian is not required to follow OMB memorandums but has issued policies requiring devices containing sensitive data be encrypted.

Smithsonian Directive 931, *Use of Computers, Telecommunication Devices and Networks*, dated September 18, 2009, requires users to ensure that sensitive data stored on laptops or other portable hardware is encrypted. The OCIO technical note IT-930-TN28 establishes the procedures and responsibilities for implementing encryption. According to the technical note, the computing device user is responsible for determining that the device may be used to store sensitive information. The computing device user contacts the unit's IT staff, who is responsible for licensing and installing encryption software. The technical note establishes that whole disk encryption must be used if sensitive data is stored on a laptop computer.

In response to the original audit recommendation, management took the following measures:

The Office of the Chief Information Officer (OCIO) provided information for Smithsonian units to directly procure a range of approved encrypted devices and encryption software. The CIO distributed a Smithsonian-wide email to remind staff of their role and responsibilities for protecting sensitive Smithsonian information using these approved technologies. In addition, OCIO installs encryption on portable or desktop computers on request.

RESULTS OF OIG REVIEW

In December 2012 and January 2013, we tested a sample of laptops in four units that routinely handle sensitive information and found that many laptop computers were not encrypted. We found that 11 of 15 laptops tested did not have whole disk encryption installed. Of the four units visited, three units did not have encryption installed on any of the laptop computers tested. Several of the computers tested were used by senior-level management. Several staff indicated that they assumed the laptop computers were configured according to Smithsonian requirements and were unaware that encryption was not installed.

If a laptop computer that is not secured with encryption is lost or stolen, the information contained on the laptop can be easily obtained without knowledge of user passwords. If the information on the laptop computer is securely encrypted, it would be unlikely or impractical for anyone to retrieve it without the decryption key.

CONCLUSION AND RECOMMENDATION

The controls in place are not adequate to ensure that laptop computers that may contain sensitive information are secured with an appropriate encryption technology. Staff were not knowledgeable about how the equipment they use was configured and expected it to be configured appropriately for its intended use. Therefore, the original recommendation will remain open and we further recommend that the USFA/CFO, in coordination with the other Under Secretaries, direct Unit IT staff to:

1. Determine which laptop computers in their inventory may be used to store sensitive data and, with assistance from OCIO, configure those computers with whole drive encryption.

2. Identify all laptop computers that will not be configured with encryption and clearly indicate to users with a prominent label that those computers must not be used to store sensitive information.

In addition, we recommend that the Chief Information Officer:

3. Revise IT-930-TN28 to assign responsibility to staff with the knowledge and skills to ensure laptop computers are configured with appropriate encryption technology.

Management has concurred with the recommendations and developed a plan to implement them. We believe that the proposed actions, when implemented, will meet the intent of these recommendations. We have included management's full response in Appendix A.

We note that the original recommendation is to enforce the existing Smithsonian policy, which requires all mobile devices that may be used to store sensitive information be encrypted. This includes devices such as portable storage, tablets, and smart phones. When requesting that we close the original recommendation, please address how the Smithsonian is implementing its policy with respect to other types of mobile devices.

APPENDIX A. MANAGEMENT'S RESPONSE

Smithsonian Institution

Office of the Chief Information Officer

Memo

Date February 25, 2013

To Michael Sinko, Assistant Inspector General for Audits

From Deron Burba, Chief Information Officer

cc Susan Avery, Associate Director, Personal Property Management
Patricia Bartlett, Chief of Staff, Office of the Secretary
Albert Horvath, Under Secretary for Finance and Administration/CFO
William Hoyt, Director of IT, OIG
Rebecca Hutchings, Acting Director of IT Security
Judith Leonard, General Counsel
Cindy Zarate, Acting Smithsonian Privacy Officer

Subject Response to Management Advisory Regarding Portable Computer Encryption

To address the recommendations in the OIG's Management Advisory, the Office of the Chief Information Officer (OCIO) is planning to work along with the Office of Contracting and Personal Property Management (OCON&PPM), the Units' Accountable Property Officers, and the IT support staff from SI's larger Units.

Based on the Assistant IG's three (3) recommendations, the OCIO provides the following response:

Recommend the USFA/CFO, in coordination with the other Under Secretaries, direct Unit IT staff to:

1. Determine which laptop computers in their inventory may be used to store sensitive data, and with the assistance from the OCIO, configure those computers with whole drive encryption.

Concur. A new "Property Management Laptop Form" will be developed to help the Units recognize sensitive information usage. Unit Accountable Property Officers will then survey existing and new laptop usage requirements to determine which laptops will be used to store sensitive data. OCIO's helpdesk will be notified as to which laptops need to be encrypted. Unit and OCIO Completion Date: 15 December 2013

2. Identify all laptop computers that will <u>not</u> be configured with encryption and clearly indicate to users with a prominent label that those computers must not be used to store sensitive information.

Concur. The unit Accountable Property Officers and Property Custodians will attach the stickers indicating not authorized for storage of sensitive data. Unit Completion Date: 15 December 2013

380 Herndon Parkway
Herndon, Virginia 20170
(202) 633-4901 Telephone
(202) 312-2804 Fax

APPENDIX A. MANAGEMENT'S RESPONSE (CONTINUED)

3. OCIO to Revise IT-930-TN28 to assign responsibilities to staff with the knowledge and skills to ensure laptop computers are configured with appropriate encryption technology.

Concur. The OCIO will update *Encrypting Sensitive Information on User Devices* (IT-930-TN28) to clarify roles and responsibilities of the Unit Accountable Property Officers, the end user responsibilities in identifying any needs to store sensitive data and the role of OCIO for technology support. OCIO Completion Date: 01 May 2013

The Office of the Chief Information Officer plans to send to the Office of the Inspector General a closure request for this management advisory as well as the original audit finding by 15 December 2013.

Any follow up fieldwork by the OIG with the Units is projected to occur between 15 January 2014 and 15 February 2014.

The Chief Information Officer and the Associate Director for Personal Property Management both acknowledge the OIG's Management Advisory and have identified the original A-10-01-05 (#755) Laptop Encryption finding with a new Scheduled Completion Date of 15 March 2014.

Thank you for your consideration. Please do not hesitate to contact me with any questions you may have regarding this response at burbad@si.edu or 202-633-4901.

380 Herndon Parkway
Herndon, Virginia 20170
(202) 633-4901Telephone
(202) 312-2804 Fax