United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General

Office of Audits

Audit of Overseas Laptop Computer Inventory Controls and Security Management

Report Number AUD/SI-10-08, January 2010

~~IMPORTANT NOTICE~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability and positive change in the Department of State and the Broadcasting Board of Governors.

This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

Harold W. Geisel
Deputy Inspector General

TABLE OF CONTENTS

Executive Summary 1

Background 5

Objective 9

Audit Results 11

Finding A. Laptop Computer Inventories Are Inaccurate and Incomplete 11

Finding B. Security Awareness Briefing Program Improvements Are Needed 28

Finding C. Hard Drive Disposition/Destruction Process Improvements Are Needed 33

Finding D. Overseas Post Encryption Rates for Laptop Computers Have Improved 35

Recommendations 39

Appendices

A. Scope and Methodology. 43

B. Bureau of Information Resource Management Response 45

C. Embassy Bogota Response. 49

D. Embassy Rome Response. 53

E. Embassy Tokyo Response. 55

F. Embassy Vienna Response. 57

Abbreviations 65

EXECUTIVE SUMMARY

Federal agencies are required by law and regulation to safeguard sensitive and personally identifiable information (PII) contained on laptop computers. Over the past several years, some agencies have lost laptops that contained PII, such as social security numbers, financial data, or addresses, or possibly sensitive information concerning agency operations. If unauthorized individuals obtain laptops that have this data, the compromised data could result in the identity theft of individuals or the disclosure of information that undermines U.S. interests.

The Office of Inspector General (OIG) conducted this audit to determine whether the Department of State overseas diplomatic posts were adequately accounting for their laptop computers, and were in compliance with security awareness and laptop encryption policies.

OIG performed a complete physical inventory of all laptop computers at six posts: Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and the American Institute in Taiwan (AIT Taipei). OIG found that Embassy Tokyo and AIT Taipei were able to account for all of their laptop computers, but that the inventories of laptop computers at the four other embassies were inaccurate and incomplete. OIG inventoried 706 laptops that were reported in the official inventories of record of the six posts and found that 37 laptop computers were missing. During the physical inventory at Embassies Bogota, Mexico City, Rome, and Vienna, OIG found 106 laptop computers that were not included in the official inventory, of which 96 were being used. Embassy officials reported that the remaining 10 were stolen or missing.

At Embassy Bogota, an additional nine laptops had been missing for 6 to 8 years, and had been improperly removed from the official inventory in 2008. Consequently, the Embassy did not know the locations of these nine laptops, they were not in the inventory of record provided to OIG, and they were not properly reported as missing.

OIG also found that there was not sufficient documentation to support that laptop users received the required laptop cyber security awareness briefing. OIG reviewed 154 laptop user files and found that 55 files (36 percent) did not contain laptop security awareness briefing acknowledgement forms. Overall, 40 (56 percent) of 71 users interviewed said that they had not received the required briefing.

OIG found that most posts visited were installing required encryption software onto the hard drives of each laptop. To determine whether the six posts complied with the Department's 100 percent encryption requirement, OIG tested 350 laptops and found that 298 (85 percent) of the laptop computers were encrypted. However, approximately 15 percent of sampled laptops had not been encrypted. At Embassy Mexico City, several users said that they had PII stored on their unencrypted laptops while traveling on temporary duty, which posed security vulnerabilities.

OIG attributed the inventory deficiencies and noncompliance to various internal control weaknesses, including the following:

- Failure to enter laptops into the official inventory or to enter the laptops into the system in a timely manner.
- Need for validation and reconciliation of laptop inventories.
- Deficient loan documentation processes.
- Lack of coordination among post sections.
- Need for investigation and reporting of missing laptops.
- Need to maintain documentation to support security awareness briefings.
- Need for proper disposition of hard drives.
- Need to meet the Department's encryption rate requirement.

Because the laptop computer inventories were inaccurate and incomplete, the likelihood that the laptops could be misplaced, lost, or compromised was increased. Inaccurate and incomplete inventories, as well as a lack of security awareness training and encryption, pose security vulnerabilities that PII or potentially sensitive information about Department operations could be compromised if those computers are lost or stolen.

Management Comments

In November 2009, a draft of this report was provided to the Bureau of Information Resource Management (IRM) and the Bureau of Administration (A Bureau); Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna; and AIT Taipei.

OIG made recommendations for IRM to direct posts to provide more effective control and monitoring of their laptop computers, investigate and report the circumstances surrounding missing laptops, clarify the roles and responsibilities of the Information Management Officers and the General Services Officers, and ensure that post personnel are properly briefed on laptop security requirements. In response

(Appendix B), IRM stated that it had issued a September 2009 ALDAC (All Diplomatic and Consular Posts) that contained guidance to address these issues. However, the ALDAC guidance was valid for only 90 days and therefore, the guidance is no longer effective in addressing the stated internal control weaknesses.

Embassy Bogota (Appendix C) agreed to take actions regarding laptop computer inventories, laptop loan-out procedures, the reporting of missing laptops, security awareness briefings, the disposition of hard drives and laptop shipping documentation, and laptop encryption.

Embassy Rome (Appendix D) stated that it had "developed and implemented standard operating procedures to improve coordination" between the General Services Officer and Information Management Officer sections.

Embassy Tokyo (Appendix E) agreed that all laptop users should take the security awareness briefing and described how the briefings were to be conducted, and how documentation acknowledging that the briefings had been conducted was to be maintained.

Embassy Vienna (Appendix F) agreed to improve the laptop inventory system and laptop loan-out procedures and documentation, to ensure that laptop users take the security awareness briefings and maintain associated acknowledgement forms, and to have laptops encrypted and/or obtain waivers to encryption as needed.

The A Bureau, Embassy Mexico City, and AIT Taipei did not respond to the draft report.

Based on the responses, OIG considers eight recommendations resolved, pending further action, and seven recommendations unresolved, including Recommendation 6. This recommendation pertained to the amount of time that loan documents should be retained for laptop computers. OIG has modified the recommendation and requests that IRM respond to the new Recommendation 6.

BACKGROUND

Technological advances have expanded the use of mobile computers capable of storing vast amounts of information on devices that are diminishing in size, increasing the possibility of pilferage. Mobile workers can process, transport, and transmit sensitive information anywhere they work. The very nature of the portability of laptops introduces information risk not associated with desktop computers. The increased use of laptop computers improves productivity yet enhances the risk that personally identifiable information (PII) or other sensitive information contained on the devices may be compromised if the laptops are lost or stolen.

Federal agencies have reported lost or stolen laptops that contained PII or sensitive information. In May 2006, a laptop computer was stolen from the home of a Department of Veterans Affairs employee. The laptop had 26.5 million records stored on it that contained PII, including names, social security numbers, and addresses. In July 2009, the Department of State, Office of Inspector General (OIG), issued the report *Audit of Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, DC, Metropolitan Area* (AUD/SI-09-15). In that report, OIG determined that out of a sample of 334 laptops in the inventory, 27 were missing and 172 of sampled laptops were not encrypted. OIG recommended that the bureaus develop procedures to improve accountability and inventory controls and develop a centralized method to track participation in security awareness training. Since the July 2009 report was issued, the Department has agreed to take corrective actions.

Under Title III of the E-Government Act of 2002, the Federal Information Security Management Act requires Federal Government agencies to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and the assets of the agency. Even earlier, the Privacy Act of 1974 set out general requirements addressing the need for the protection of PII.

The Office of Management and Budget (OMB) has primary oversight responsibility for information management and information security. Between 2006 and 2007, OMB issued several policy directives to require and remind departments to protect PII. Specifically, OMB Memorandum M-06-16, *Protection of Sensitive Agency Information,* June 2006, recommended that departments and agencies encrypt all data on mobile computers that carry agency data unless the data is determined to be nonsensitive. In addition, in May 2007, OMB issued Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* reemphasizing agency responsibilities to safeguard PII and requiring all agencies to develop and implement a breach notification policy and a policy on incident reporting and handling in order to effectively respond when an agency is faced with a security incident (such as the unauthorized release of PII through the loss of a laptop computer).

In response to OMB's memoranda, the Department issued notices on responsibilities related to handling PII and other sensitive agency data. The first in the series of related unclassified cables, STATE 00058726, "Protection of Personally Identifiable Information (PII) on Laptops," May 2007, was distributed to All Diplomatic and Consular Posts (ALDAC). It mandated that all Department laptop hard drives be encrypted. In a March 2008 ALDAC (STATE 00032537, "Unclassified and SBU Laptop Inventory and Encryption Responsibilities"), the Information Management Officer (IMO) was assigned responsibility for the inventory and security of all unclassified and sensitive but unclassified (SBU) laptops at the IMO's site, and was instructed to "review and validate the complete site inventory of existing laptops." This same ALDAC also reemphasized the need to immediately report all missing, lost, or stolen laptops to cognizant post officials; to immediately report all suspected or confirmed PII losses or thefts to the Bureau of Diplomatic Security (DS) Computer Incident Response Team; to ensure that all laptop users annually review DS's laptop cyber security awareness briefing; and to maintain records of such briefings.

Department Responsibilities

The Assistant Secretary of the Bureau of Information Resource Management (IRM), as the Chief Information Officer (CIO), serves as the principal adviser to the Secretary of State and other senior officials on matters pertaining to the application of information systems, and supports the achievement of strategic Department missions, including information security, in coordination with DS.[1] In this regard, the CIO is responsible for developing, promoting, and coordinating the Department-wide information security program activities. The Chief Information Security Officer (CISO) heads IRM's Office of Information Assurance (IRM/IA). The CISO is designated by the CIO to carry out the responsibilities under the Federal Information Security Management Act and to ensure the development and implementation of an agency-wide information security program. IRM's Operations Support Branch (IRM/OS) is the office responsible for ensuring valid, reliable, and timely informa-

[1] 44 U.S.C. 3506.

tion by providing systems and network administration for the Department's external and internal customers.

Key responsibilities relating to the management of accountable property at post are outlined in the Foreign Affairs Manual (FAM) (14 FAM 410).[2] The Property Management Officer (PMO) at each post oversees all property inventories. Accountable property includes information technology equipment. A physical inventory of all personal property must be taken annually, and be immediately reconciled with the property records. After the reconciliation, an inventory certification, Property Management Report, is required to be prepared by the PMO and submitted annually to the Bureau of Administration (A Bureau) by March 15 of each year.

The IMO is the senior information management individual at post. The IMO oversees all information management operations and personnel at post. STATE 00032537 states that the IMOs are responsible for the inventory and security of all unclassified and SBU laptops at their respective sites.

The General Services Officer (GSO) is responsible for a range of functions that involve the management of physical resources and logistical functions at diplomatic and consular posts. The GSOs develop, plan, implement, and manage an ongoing program of support that includes contracting, inventory/property, physical facilities, motor pool, and maintenance and repair.

Property Inventory Systems

The Non-Expendable Property Application (NEPA) is the primary property management system used at overseas posts to account for non-expendable property from receipt through disposal. The NEPA system is a property inventory system in the process of being replaced with the Integrated Logistics Management System (ILMS). ILMS is a single, integrated Web-based system that is designed to track purchasing, procurement, transport, storage, and disposal of Department property. ILMS has already been implemented domestically and is being deployed at overseas posts. As of April 2009, approximately 13 percent (35 of 277) of the overseas posts had converted to ILMS.

[2] 14 FAM 410, "Personal Property Management for Posts Abroad."

OBJECTIVE

The objective of the audit was to determine whether overseas posts adequately accounted for laptop computers, including inventory controls, and complied with security policies and procedures for encryption and security awareness briefings. (The audit's scope and methodology are detailed in Appendix A.)

AUDIT RESULTS

Finding A. Laptop Computer Inventories Are Inaccurate and Incomplete

OIG found that Embassy Tokyo and AIT Taipei were able to account for all of the laptop computers reported in their official inventories of record. However, at Embassies Bogota, Mexico City, Rome, and Vienna, 37 laptop computers in the embassies' official inventories of record were missing. During the physical inventory of laptops at these posts, OIG found that 106 laptop computers were not included in the official inventory, of which 96 were being used. Embassy officials reported that the remaining 10 were stolen or missing.

These conditions occurred because the GSO did not enter newly acquired laptop computers into the official inventory, the GSO and the IMO did not validate and reconcile laptop inventory discrepancies, the IMO needed to improve the process of documenting and controlling the loaning of laptops, and the PMO did not investigate and report missing laptops and those that were improperly removed from the official inventory.

Because the laptop computer inventories were inaccurate and incomplete, the likelihood that the laptops could be misplaced, lost, or compromised was increased. Inaccurate and incomplete inventories pose security vulnerability that PII or potentially sensitive information about Department operations could be compromised if those computers are lost or stolen.

Overseas Inventory Sample

OIG visited Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and AIT Taipei during February and March 2009 (the sampling methodology is in Appendix A). At these locations, OIG attempted to inspect all 706 laptop computers in the official inventories of record; however, only 653 laptop computers were available to be inventoried because 37 laptops were missing, 15 laptop computers were not physically available to be inspected, and one had been reported as stolen. However, OIG was able to obtain sufficient documentation to demonstrate that the 15 laptops not physically available were in use by embassy officials at off-site locations or were about to be destroyed.

During the physical inventory at Embassies Bogota, Mexico City, Rome, and Vienna, OIG found 106 laptop computers that were not included in the official inventory, of which 96 were being used. Embassy officials reported that the remaining 10 were stolen or missing. A summary of OIG's inventory of the laptop computers by location is in Table 1.

Table 1. Results of OIG's Physical Inventory of Laptop Computers

In Official Inventory	**Bogota**	**Mexico City**	**Rome**	**Tokyo**	**Vienna**	**Taipei**	**Totals**
Physically inspected	117	89	93	155	96	103	653
Missing	13	16	7	0	1	0	37
Reported by post as stolen	0	0	0	0	1	0	1
Not available with appropriate documentation at time of visit	3	3	6	1	2	0	15
Subtotal	**133**	**108**	**106**	**156**	**100**	**103**	**706**
Not in Official Inventory (Unrecorded)							
Physically inspected	27	43	2	0	24	0	96
Missing	9	0	0	0	0	0	9
Reported by post as stolen	0	1	0	0	0	0	1
Subtotal	**36**	**44**	**2**	**0**	**24**	**0**	**106**
Totals	**169**	**152**	**108**	**156**	**124**	**103**	**812**

Missing Laptops and Inaccurate Inventories

At Embassies Bogota, Mexico City, Rome, and Vienna, OIG was unable to locate 37 laptop computers, and it classified those laptops as missing. Embassy officials generally could not explain why the laptops were missing or the disposition of the computers. However, OIG noted internal control deficiencies in laptop administration that caused the laptops to be missing and unaccounted for, as described in the sections that follow. For example, the FAM (14 FAM 411.4)[3] requires that personal property, including laptop computers, be tracked on property records and inventoried regardless of cost. OIG found 96 laptop computers that were physically accounted for but that were not entered into the official inventory.

[3] 14 FAM 411.4, "Definition of Accountable Property."

Embassy Bogota. OIG identified 13 laptops at Embassy Bogota that were in ILMS but that could not be physically located. Embassy officials could not explain why the laptops were missing. OIG also found 27 laptop computers that had not been entered into ILMS, seven of which were not included in the IMO's unofficial listing. Four of the 27 were purchased in Washington, D.C., and were shipped to the Regional Security Officer (RSO) at the Embassy without having gone through the GSO or the IMO. As a result, the GSO was unaware of these laptops. In addition, OIG noted that 14 of the 27 laptops were purchased by the Narcotics Affairs Section (NAS) for subsequent use by the Columbian Government. NAS officials did not believe the GSO needed to be notified of these purchases. However, the NAS should have notified the GSO when American citizens at post began using the laptops to ensure they were properly recorded in the post property inventory for accountability and tracking purposes. Embassy officials did not explain why the remaining nine of 27 laptops had not been inventoried.

Embassy Mexico City. OIG identified 16 laptops at Embassy Mexico City that were recorded in ILMS but could not be located. Also, 43 laptop computers had not been recorded in ILMS. Of the 43 laptop computers, 26 computers were in the IMO's listing but not in ILMS, and 17 were not listed in either the IMO's listing or ILMS inventory, although OIG located them at the Embassy during its visit. Embassy officials did not explain why the laptops were missing or had not been recorded.

Embassy Rome. OIG found that seven laptops at Embassy Rome were in NEPA but could not be located. An internal Embassy memorandum dated February 11, 2008, requested that these computers be removed from NEPA and stated that they may have been unintentionally thrown away during the renovation of Embassy office space instead of being properly disposed of through the property disposal process. Also, two additional laptop computers were not entered into NEPA. Embassy officials said that they had planned to send the laptop hard drives to IRM for disposition, as required by the Foreign Affairs Handbook (FAH) (12 FAH-6 H-542.5-10).[4] The IMO had prepared disposition documentation for only one of the two hard drives and had not sent either laptop hard drive to IRM for disposition. Both laptops remained at post.

[4] 12 FAH-6 H-542.5-10, "Disposal/Disposition."

Embassy Vienna. OIG found that one laptop at Embassy Vienna was in NEPA but could not be located. Embassy officials could not explain why the laptop was missing. Also, 24 laptop computers were not entered into NEPA, of which 22 had been assigned to the Vienna Training Office (VTO) and had NEPA numbers affixed to them. OIG queried the inventory system for the NEPA numbers and serial numbers. For 11 NEPA numbers, a search of the system did not identify equipment of any kind, while the remaining 11 were listed as items such as chairs and desks, but none as computers. None of the serial numbers were found in the NEPA database, despite the FAM requirement (14 FAM 414. 1-1)[5] to track assets on property records.

In addressing why the VTO laptops had not been inventoried, one Embassy official said that the NEPA numbers may have been affixed to the computers by another post. However, post records showed that these computers were purchased by the Embassy in September 2006. The GSO said that he did not control the VTO laptop computer inventory; that VTO is, in essence, a separate entity from Embassy Vienna; and that the VTO chief is responsible for the 22 computers.

The VTO chief said that the Embassy had not performed an inventory of these computers during his tenure at the VTO. The Embassy requested and received an encryption waiver for 21 of the 22 computers. Although the laptop computers were used exclusively for VTO training, they are Department property, which needs to be properly controlled by the IMO and entered into NEPA, as required by the FAM (14 FAM 410).

Two laptops were purchased with year-end funds, but they had not been entered into NEPA as of the time the OIG team left Austria in March 2009. The purchaser did not notify the GSO of the laptop purchases. As a result, these computers had no NEPA labels and were not in the inventory database.

Factors Causing Inaccurate Laptop Inventories

Inventories at Embassies Bogota, Mexico City, Rome, and Vienna were inaccurate for various reasons. The GSOs were not always notified of new laptops, laptop inventories were not always validated and reconciled, laptops were not entered into the inventory in a timely manner, loaned laptop computers were not documented and controlled, and laptops were not investigated and reported when they were missing.

[5] 14 FAM 414.1-1, "Accountability Criteria."

Embassy sections or headquarters bureaus sometimes purchased laptops but did not inform the GSO when the items were received. As a result, these laptops did not get entered timely or at all into the official inventory.

GSOs Not Always Notified of New Laptops

The GSOs were not always notified of the arrival of new laptops by sections that procured and used laptops, which weakened internal controls. Instances of not being notified occurred, for example, at Embassies Bogota and Rome.

Embassy Bogota. The GSO did not ensure that all newly acquired laptop computers were entered into the official inventory because the NAS did not tell the GSO that the laptops had been received or record them into ILMS. At Embassy Bogota, 14 of the 27 laptops not recorded in ILMS belonged to the NAS, which procures and manages its own property at the Embassy. This contributed to the omission of laptops entered into the ILMS inventory. Furthermore, the unrecorded laptops were procured using funds from a Department program to support the Columbian Government's aviation law enforcement capabilities but were actually used by U.S. Embassy officials in support of the same program. NAS officials indicated that the laptops were initially intended to be given to the Columbian Government and that the GSO was therefore not initially informed of the laptops' existence.

Four other unrecorded laptops at the Embassy that were assigned to the RSO had been procured in Washington, D.C., and shipped directly to the RSO without going through the GSO or the IMO. STATE 00049731, "Diplomatic Security Laptops," May 2008, requires the RSO to ensure that all DS laptops owned by DS are in the official post inventory.

Embassy Rome. At Embassy Rome, the PMO said that the use of purchase cards could cause the lack of expeditious entry of laptop computers into the inventory system. If an Embassy section purchases laptops with a purchase card, and the laptops are delivered directly to the purchasing office, the GSO may not be initially aware of the purchase, although the GSO's monthly purchase card review of the bill might identify the purchase. However, the Supervisory GSO for the Embassy, the reviewer of this bill, said that sometimes there is not sufficient information on the bill to determine what was purchased. The PMO added that if the purchase is not detected at this time, and the time for the monthly review passes, the next chance for detecting the purchase is during the annual inventory. However, if the oversight is not caught during the annual inventory review, according to the official, there is no reason to believe it would be caught by anyone after that time.

Even though a purchase card is not used, laptops still might not get entered into NEPA. Laptop computers may be acquired via a purchase order through the GSO rather than a purchase card. The item is delivered directly to the requesting office, and that office completes the receiving report. Again, without notifying the GSO, the item is precluded from being entered into NEPA.

Laptop computers also may not get entered into NEPA when a secure order is placed through Washington, D.C. Laptop computers acquired in this manner could take longer than several months to arrive at the post, which could result in officials' losing track of the order date as well as the expected date of arrival. Upon arrival, the item is delivered to a secure place on the post; therefore, Foreign Service Nationals assigned to the GSO have no involvement with the item. Consequently, the item could be received and be in use, but would not have an inventory number (which signifies entry into the official inventory system) until much later than actual receipt at post, if at all.

The PMO for the Embassy further stated that the control of laptop computers is rather complicated because both the GSO and the IMO are involved. The GSO is concerned with purchasing laptops and the annual inventory, while the IMO is concerned with systems administration, such as updating patches and installing new virus protection software on laptops and other technology devices. However, STATE 00032537 states that the IMO is responsible for the inventory and security of all unclassified and SBU laptops at his or her respective site. As a result, there is some confusion and responsibility overlap in the administration and management of laptops at overseas posts.

Recommendation 1. OIG recommends that the Bureau of Information Resource Management emphasize, to Information Management Officers, their responsibility for entering all Department of State laptop computers under their control into the official inventory and entering them in a timely manner.

Management Response. IRM stated that it had issued guidance in the September 25, 2009, ALDAC 09 STATE 100287, "Unclassified and Sensitive but Unclassified Laptop Inventory and Encryption Responsibilities," to remind personnel about laptop inventory accountability responsibilities and requirements." IRM stated that this was "an action ALDAC that provides instructions for IMOs and ISSOs regarding laptop inventory and encryption activities."

OIG Reply. The FAH (7 FAH-1 H-145, "ALDACS") states, "Policies and procedures communicated in ALDAC's are limited in validity to 90 days, during which time continuing guidance is to be included in the FAM or the FAH." As such, the policies and procedures contained in the September 25, 2009, ALDAC have expired. Therefore, in accordance with the FAH, IRM should codify, in the FAM and/or the FAH, guidance for IMOs on procedures to follow to ensure that all laptops are posted timely to the property system.

Recommendation 1 is considered resolved, pending receipt of documentation showing that the IMOs' responsibilities regarding laptop inventory have been codified in the FAM and /or the FAH.

Recommendation 2. OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer and the General Services Officer to ensure that all laptops are properly entered into the post inventory system and periodically reconciled to manual records.

Management Response. Embassy Bogota agreed, stating that the IMO and the GSO "will ensure" that laptops are entered into ILMS, "even when the laptops are procured outside of normal Embassy procurement channels," and that NAS and RSO personnel "understand Post's policies." The Embassy further stated that the IMO is now managing the NAS laptop inventory so that the laptops are "properly inventoried."

Embassy Rome also agreed with the recommendation, stating that the GSO and the IMO sections "developed and implemented standard operating procedures to improve coordination."

Embassy Vienna generally agreed with the recommendation, stating that all of the laptops controlled by the IMO are "entered into the post NEPA database." The Embassy also stated that the Foreign Service Institute was responsible for controlling VTO laptop computers because these computers were outside the Embassy's area of responsibility. However, OIG notes that Department guidelines state that the IMO is responsible for the inventory and security of **all** Department-owned unclassified and SBU laptops at post, which would include VTO laptops.

Further, the Embassy stated that it had "full accountability" of its laptop computers and that it was "misleading" for OIG to "cite the NEPA inventory status as a problem," since at the time of OIG's audit, the Embassy was "in the middle of an exercise to dispose of old laptop computers and to prepare new laptop computers . . . for issue." However, during the audit, OIG did in fact take into account the recording of laptops being prepared for disposal and issuance, and OIG did not identify any laptops that had not been entered into the inventory.

OIG Reply. Embassies Bogota, Rome, and Vienna sufficiently addressed Recommendation 2, and Embassy Vienna needs to provide a summary of the next laptop inventory reconciliation based on a physical evaluation, to include those laptops used by the VTO. However, the recommendation is considered unresolved until Embassy Mexico City provides a response to the report.

Laptop Inventories Not Always Validated and Reconciled

OIG found a need for more effective coordination between the IMO and the GSO at Embassies Bogota and Mexico City to ensure laptops were regularly validated and reconciled. Specifically, the IMOs did not reconcile the IMO's unofficial listing of laptops to ILMS. At Embassy Bogota, the IMO was not aware of 33 laptops that were in ILMS, while 27 other laptops on the IMO's unofficial listing were not in ILMS. Similarly, at Embassy Mexico City, the ILMS inventory contained 63 laptops that the IMO was not aware of, while 27 laptop computers on IMO's unofficial listing were not reflected in ILMS, in addition to 16 computers not accounted for in either the official or the unofficial inventory. As a result, Embassies Bogota and Mexico City could not account for about 109 (76 percent) laptops classified by OIG as missing, stolen, or not inventoried.

STATE 00032537 states the IMO is responsible for the inventory and security of all unclassified and SBU laptops at post. Responsibilities include the review and validation of the complete site inventory of existing laptops. Also, all laptops must be physically located, recorded, and reconciled in the post's inventory system. The FAM (14 FAM 411.2-2)[6] states that the Accountable Property Officer's (APO) functional responsibility is inherent in the position of the GSO. The GSO is then responsible for the custody, care, and safekeeping of all property under control of the posts; accomplishment and reconciliation of the physical inventory; and the documentation

[6] 14 FAM 411.2-2, "Accountable Property Officer."

of inventory shortages. The policies assign a level of responsibility to both the IMO and the GSO for the validation and reconciliation of the laptop inventory with the site's official property inventory. To some extent, there is an overlapping of responsibilities, which may have caused some confusion over the roles of the IMO and the GSO.

Without efficient coordination and teamwork between the IMO and the GSO in the administration and management of laptop inventories, posts risk having an incomplete laptop inventory, thereby increasing the likelihood of theft or loss of these laptops. The incomplete inventory may also result in the failure to ensure that all laptops are encrypted, which places PII and sensitive information in jeopardy. Because of the importance of accounting for these sensitive items, having inventories conducted more frequently than annually would be a valuable management practice.

Recommendation 3. OIG recommends that the Bureau of Administration and the Bureau of Information Resource Management clarify the roles and responsibilities of the posts' Information Management Officer and the General Services Officer for controlling and inventorying laptop computers. They should also require posts to validate and reconcile the official laptop computer inventory data more frequently than annually.

Management Response. IRM stated that it had issued guidance to posts in the September 25, 2009, ALDAC 09 STATE 100287 that addressed the recommendation. IRM further stated that both it and the A Bureau did not agree that it was necessary for posts to validate and reconcile the official laptop computer inventory data more than annually. IRM said that this "would not be practical and would not produce substantially more benefits." However, IRM did state that post management should conduct "periodic reviews" of the equipment to ensure that the review results and the year-end inventory count agree.

OIG Reply. Although the September ALDAC is an effective reminder to the IMOs of their responsibilities, the policies and procedures of the ALDAC have expired (7 FAH-1 H-145). Therefore, in accordance with the FAH, IRM should codify, in the FAM and/or the FAH, guidance on the GSOs' inventory responsibility for computer laptops to preclude an overlapping of duties with the IMOs.

Recommendation 3 is considered resolved, pending receipt of documentation of the results of the first periodic review performed, which shows that the review results agree with the year-end inventory count, and documentation showing that the roles and responsibilities of post IMOs and GSOs have been clarified in the FAM and/or the FAH.

Recommendation 4. OIG recommends that Embassies Bogota and Mexico City require the Information Management Officer to submit the results of the next physical inventory of laptop computers, along with the accompanying reconciliation of the official inventory with the Information Management Officer's unofficial inventory, to the Bureau of Information Resource Management and the Office of Inspector General.

Management Response. Embassy Bogota agreed, stating that the IMO "is now responsible for all NAS laptops and will ensure" adherence to post and Department procedures.

OIG Reply. Embassy Bogota sufficiently addressed Recommendation 4, pending receipt of documentation showing the results of the next laptop computer physical inventory and reconciliation to the property system. However, the recommendation is considered unresolved until Embassy Mexico City provides a response to the report.

Laptops Not Entered Timely Into Inventory System

At Embassy Rome, OIG found that six laptop computers were inventoried in NEPA but were not entered into the system in a timely manner after receipt at the Embassy. OIG believes that a reasonable time period for entering laptops into the inventory should be no more than 2 months from the date of receipt. The average original entry date of the six laptops was more than 1 ½ years from the date of receipt. The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*[7] requires the timely recording of transactions as part of an effective internal control structure and safeguarding of sensitive assets. OIG could conduct only limited testing in this area because the date of entry into NEPA was not available to systems users. When pertinent Department ownership information of laptop computers, such as the serial number and NEPA number, has not been promptly recorded, the potential increases for laptop theft or loss.

[7] GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

The NEPA system does not provide a data field that identifies the date that an item is inventoried. Not putting the original entry date into NEPA adversely impacts internal control. According to the GAO standards, internal control should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. The inability to monitor the length of time it takes for a laptop computer to be entered into the inventory system because of the lack of the date of original entry into NEPA adversely impacts monitoring, which is an important aspect of internal control. OIG did not conduct this analysis at the other four embassies and AIT Taipei that it visited.

Recommendation 5. OIG recommends that the Bureau of Administration ensure that data fields for the dates of original entry for laptop computers are available in the Non-Expendable Property Application and the Integrated Logistics Management System to facilitate inventory monitoring efforts.

Management Response and OIG Reply. The A Bureau did not respond to Recommendation 5. Therefore, the recommendation is unresolved.

Loaned Laptop Computers Not Documented and Controlled

Embassies Bogota, Mexico City, Rome, and Vienna did not always follow Department-prescribed procedures for loaning and assigning laptops to employees. Specifically, OIG found that for 83 (30 percent) of 279 loan documents sampled, supervisory authorization signatures were missing, as shown in Table 2.[8] In addition, loan forms were not always properly filled out, and some posts were destroying loan documents when laptops were returned by users. While retaining documentation until the end of the loan period is permitted by regulations, OIG believes that also maintaining loan documents for at least 1 year after the laptop is returned would facilitate any future investigation into missing or misused laptops.

[8] Generally, OIG obtained its random sample from listings of all laptop computers that were on loan at the time of its site visits, as well as from listings of computers returned during 2008. However, OIG could not always sample returned forms because some embassies immediately destroyed the forms when the computers were returned. OIG was also able to review all the documents within its scope for Embassy Tokyo and AIT Taipei rather than a sample.

Table 2. Missing Authorization Signatures on Laptop Loan Documents

Posts	Number of Missing Signatures	Number of Loans Tested	Percent of Difference
Bogota	18	23	78
Mexico City	25	25	100
Rome	9	18	50
Tokyo	0	107	0
Vienna	30	32	94
AIT Taipei	1	74	1
Totals	**83**	**279**	**30**

Embassy Bogota. OIG found that 18 (78 percent) of 23 of the laptop loan documents reviewed at Embassy Bogota did not have authorizing signatures. Most of the documents were in the NAS, where officials said that they were not aware of the requirement to have authorizing signatures. OIG informed the NAS chief that all laptop loans required a supervisory authorizing official to sign the forms, and he agreed to ensure that this was done in the future.

Embassy Mexico City. OIG found that all 25 laptop loan documents sampled and tested at Embassy Mexico City did not have authorization signatures. The Embassy did not use the prescribed Department forms, DS-7642, Mobile Computing and Data Storage Request Form, and DS-584, Nonexpendable Property Transaction. Instead, the IMO section used a form it developed in-house that did not include places for signatures of the authorizing and approving officials, for the signature of the employee's supervisor, or for the authorization of the removal of the loaned equipment from the Embassy. In STATE 32537, the Department required posts to use Form DS-7642 to manage laptop control, to check out laptops, and to track the type of data stored on the laptop. The FAH (14 FAH-1 H-416)[9] also requires the use of Form DS-584 in managing the charge out of Department property.

Embassy Rome. OIG found that nine (50 percent) of 18 laptop loan documents at Embassy Rome did not have authorizing signatures. In addition, OIG found several other anomalies pertaining to the process of documenting and controlling laptop computers that were loaned to personnel for purposes such as for temporary duty assignments. In two instances, the borrower signed the loan form

[9] 14 FAH-1 H-416, "Personal Custody Records."

acknowledging receipt of the laptop computer after the loan date, which may indicate that loan forms were not always completed before the computers were provided to the borrowers. In one instance, the loan forms for an employee on a protracted temporary duty assignment may have been generated after the laptop computer had already been loaned to him. According to travel documents, this individual had left for Baghdad, Iraq, on October 20, 2008, and the individual had not completed his temporary duty assignment at the time the OIG team visited the Embassy on February 17–27, 2009. However, Form DS-584 was purportedly signed by this borrower on October 24, 2008, 4 days after his departure to Baghdad. The Information Security Officer, the official responsible for loaning laptop computers, could not explain the 4-day difference.

OIG found other instances in which loan forms at the Embassy were not always filled out before the computers were provided to the borrowers, as required by the FAM (14 FAM 416).[10] The FAM requires that laptop computers issued to an employee for the employee's use in the performance of official duties be documented on Form DS-584. For example, a laptop computer that was thought to be missing was found in the possession of an Embassy employee who was on temporary duty travel, but there was no loan document on file despite the requirement to maintain a record of the loan until the property is returned. This laptop computer was among the original eight missing computers that the Embassy had self-reported when the OIG team arrived at the Embassy. However, the Assistant GSO said that the computer had been located just before the OIG team left the Embassy. Despite verifying with the Information Security Officer to ensure that OIG had all the loan documents on file for laptops on loan at that time, no loan documents were found for this computer.

In addition, at least one of the remaining seven of the original eight missing laptop computers was also apparently issued without the required loan forms being completed. OIG found that Embassy Rome had loaned one of these seven laptop computers to Embassy Vatican and that the laptop was subsequently lost. However, no loan documents were on file.

OIG was unable to locate any loan documents for the remaining six of the original eight laptops that Embassy Rome had self-reported as missing. Therefore, OIG was unable to determine whether the six laptops had been issued to borrowers without the required loan forms having been completed, whether the laptops were lost while they were under the control of Embassy Rome, or whether it was a combination of both factors.

[10] 4 FAM 416, "Physical Inventory and Reconciliation."

Embassy Vienna. OIG found that 30 (94 percent) of 32 laptop loan documents sampled at Embassy Vienna were missing authorization signatures. Most of the loan documents reviewed were in-house forms rather than the required Department forms. However, OIG did find that two individuals had used the required Department forms. The use of an unauthorized form, coupled with the inconsistent use of the required Department forms, resulted in anomalies in addition to missing authorization signatures, such as missing borrower signatures, missing loan dates, and missing return dates.

Recommendation 6. OIG recommends that the Bureau of Information Resource Management ensure that embassies and posts properly complete loan documents for laptop computers and maintain them for at least 12 months after a laptop computer has been returned to allow for subsequent review, audit, or investigation if the laptop is damaged or missing.

Management Response. IRM stated that it had issued guidance to the IMOs in the September 25, 2009, ALDAC 09 STATE100287 on implementing a centralized laptop control and check-out procedure. IRM also stated that it would post guidance on its Web site on maintaining laptop loan documents for the duration of a loan.

OIG Reply. OIG requests that IRM provide documentation showing that all procedures pertaining to loaning and/or issuing laptops are incorporated into the FAM and/or the FAH. Also, the original Recommendation 6 implied that loan documentation for laptop computers should be kept for 12 to 18 months **after the laptop was loaned to the user**. However, OIG has modified Recommendation 6 for IRM to ensure that the loan documentation is retained for at least 12 months **after a laptop is returned.** This will allow for subsequent review, audit, or investigation if a laptop is damaged or missing. Therefore, IRM is requested to respond to the new Recommendation 6, which is unresolved.

Recommendation 7. OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer to ensure compliance with laptop loan-out procedures and the proper preparation of supporting documentation.

Management Response. Embassies Bogota, Rome, and Vienna concurred with Recommendation 7. Embassy Bogota stated that the IMO is now responsible for all NAS laptops, and will ensure that these laptops "adhere to all Post and Department procedures." Embassy Rome stated that the GSO and the IMO sections had "developed and implemented standard operating procedures to improve coordination." Embassy Vienna stated that it was in "the process of transitioning to the [required] four-page laptop loan out form[s]" and anticipated that the forms would be completed in January 2010.

OIG Reply. Embassies Bogota, Rome, and Vienna sufficiently addressed Recommendation 7, pending receipt of documentation showing that the posts have developed and implemented standard operating procedures pertaining to the proper preparation of laptop loan-out procedures. However, the recommendation is considered unresolved until Embassy Mexico City provides a response to the report.

Missing Laptops Not Investigated and Reported

Embassy Bogota removed missing laptops from inventory without approval and did not take required actions to review, investigate, and report those losses. This occurred because the Embassy's NAS and GSO did not follow required Department procedures for reporting missing laptops and other nonexpendable property items. Without a review and investigation of these missing items, the Government did not have complete accountability for and security over the laptops and the associated data stored on them.

During its review of laptop disposal procedures, OIG found documentation indicating that the Embassy had removed nine laptops from its official inventory that had been missing for 6 to 8 years and could not be located during previous annual inventories. NAS removed five of these laptops in February 2008 without completing Form DS-132, Property Disposal Authorization and Survey Report, and without taking required actions to review, investigate, and report these laptop losses. At the same time, the GSO identified and removed four other laptops before the PMO approved their disposal. The PMO did not approve the disposals until May 2008, more than 3 months after the inventory had been adjusted.

The FAM (14 FAM 416.5-1(A) and 14 FAM 416.5-1(B))[11] establishes the reporting requirements for missing property. It states that the APO must immediately report missing property to the PMO on Form DS-132 and that the PMO must investigate cases involving missing property, make a determination of financial liability, determine what corrective actions are necessary, and authorize adjustment of inventory records.

Because the laptops were missing items, the NAS should have reported these losses immediately to the IMO, the officer responsible for controlling laptop computers, and to the APO. As the GSO, the APO should have completed a Form DS-132 and obtained approval from the PMO to dispose of the laptops prior to removing the laptops from the inventory. The PMO should have investigated and prepared a report on the missing laptops before removing the laptops from the inventory. The loss of computers should be reported timely to ensure that a breach of PII or sensitive data does not occur. Once the PMO was made aware of the four missing GSO laptops from the Form DS-132, an investigation should have been conducted.

For the five NAS laptops, the lack of investigation and reporting occurred because NAS officials were not adequately informed of the property management and security procedures, including reporting inventory shortages and missing laptops. During its visit, OIG informed the NAS and the GSO of the need to immediately report the missing laptops to cognizant officials for appropriate actions, to include an investigation. In March 2009, the NAS prepared the required property disposal reports for its five laptops.

Without review, investigation, and proper reporting of lost, stolen, or missing property, the Government has no assurance that PII and sensitive data have not been compromised.

Recommendation 8. OIG recommends that the Bureau of Information Resource Management remind posts to immediately report stolen and missing laptops; complete Form DS-132, Property Disposal Authorization and Survey Report; and conduct investigations of stolen and missing laptops.

[11] 14 FAM 416.5-1(A), "APO [Accountable Property Officer] Action," and 14 FAM 416.5-1(B), "PMO [Property Management Officer] Action."

Management Response. IRM cited guidance it had provided to posts contained in the September 25, 2009, ALDAC 09 STATE 100287 regarding missing and stolen laptop computers.

OIG Reply. Although the September ALDAC is an effective reminder to posts of their responsibilities, the policies and procedures of the ALDAC have expired (7 FAH-1 H-145). Therefore, in accordance with the FAH, IRM should codify, in the FAM and/or the FAH, guidance on reporting stolen and missing laptop computers.

Recommendation 8 is considered resolved, pending receipt of documentation showing that the responsibilities for the posts to properly report stolen or missing laptops have been codified in the FAM and/or the FAH.

Recommendation 9. OIG recommends that Embassy Bogota require the Information Management Officer and the General Services Officer to investigate the disposition of each missing laptop and prepare the required documentation as necessary. The Bureau of Information Resource Management and the Office of the Inspector General should then be notified with the accompanying documentation.

Management Response. Embassy Bogota agreed with the recommendation, stating that the IMO "will remind NAS and GSO of the reporting requirement for missing property as directed in FAM" and that the IMO "is now responsible for all laptops so this issue should never recur."

OIG Reply. The Embassy did not address that part of the recommendation relating to investigating the disposition of the missing laptop computers that OIG discovered during its audit.

Recommendation 9 is considered resolved, pending receipt of documentation showing the results of the completed investigation of the five missing laptop computers.

Finding B. Security Awareness Briefing Program Improvements Are Needed

The IMOs at the six posts visited did not always maintain required documentation to support laptop user security briefings, and the briefing process at these posts was not adequate to ensure that the users received the briefings and clearly understood their responsibilities when using government-owned laptops. STATE 00032537 requires all laptop users to receive the DS Unclassified/SBU Laptop Cyber Security Awareness Briefing to understand the security requirements and risks before being issued a laptop. Users must also sign an acknowledgement form at the end of the briefing agreeing to adhere to those requirements. However, because of a lack of adequate controls for tracking and monitoring the security briefings, the posts' records were generally not complete and lacked evidence that some users had taken the briefings. OIG randomly reviewed 154 laptop user files to determine whether laptop computer users had acknowledged receiving the required briefing.[12] OIG found that 55 (36 percent) did not have an acknowledgement form on file. Additionally, based on random interviews of laptop users at each post, OIG found that 40 (56 percent) of 71 users overall stated that they had not received the required briefings. As a result, the posts could not provide assurance that all laptop users had sufficient knowledge to adequately protect PII and other sensitive data from unauthorized access and risk of loss.

Department Requirements for Awareness Briefing

In addition to requiring laptop users to take the required briefing, STATE 00032537 also requires records to be maintained that identify the individual laptop users who have received the required briefing. The required briefing includes instructions on overall laptop usage and on the proper storage of SBU and PII data; encryption requirements; and procedures for reporting missing, lost, or stolen laptops. The guidance in the briefing specifies adherence to Department security policies, such as that only system managers are authorized to install Department-owned and -approved hardware and software on laptops, that users must not disable or alter security features, and that passwords must adhere to Department password policies.

[12] Generally, OIG randomly sampled records pertaining to the required annual briefing. At Embassy Tokyo, however, OIG was able to test all pertinent documentation rather than a sample.

The briefing is available on DS's Web site and includes an acknowledgement form recommended by DS. The form includes signature lines for the prospective laptop user to acknowledge receipt of the awareness briefing, and to agree to abide by Department requirements set out in the briefing. The form also includes lines for the signatures of Department officials who provided the briefing and for the dates for tracking.

Laptop Users May Not Have Received Required Briefing

Of the random review of 154 laptop user files to determine whether laptop computer users had acknowledged receiving the required briefing, OIG found that 55 files (36 percent) did not contain acknowledgement forms.

OIG interviewed a cross section of laptop users to obtain a general understanding of laptop usage at each post. One question was whether the laptop users had taken the required DS Unclassified/SBU Laptop Cyber Security Awareness Briefing. Although results varied by embassy and AIT Taipei, 40 (56 percent) of 71 total laptop users interviewed said that they had not received the required briefing. Based on these statistics, OIG questions whether the process of user self-certification is achieving the desired results. For example, at Embassy Mexico City, 8 (57 percent) of 14 users interviewed said that they had not received the laptop briefing. Conversely, all nine recent laptop users interviewed at Embassy Rome said that they had received the briefing.

Embassy Bogota. At Embassy Bogota, the IMO policy was that a prospective laptop computer borrower was sent a copy of the DS laptop briefing via e-mail when the employee requested the use of a laptop. The IMO, or a point of contact within the employee's section, prepared the loan form, Form DS-7642, for the borrower. The borrower, upon arriving to pick up the laptop, signed the Form DS-7642 acknowledging that the required laptop security briefing had been taken. The Embassy did not use the DS-recommended acknowledgement form but instead relied on the Form DS-7642 self-certification in the loan document. OIG found that 4 (16 percent) of 25 user files reviewed did not contain signed acknowledgement forms. Of 13 users (62 percent) OIG interviewed, eight said that they had not received the briefing.

Embassy Mexico City. At Embassy Mexico City, the IMO provided the prospective laptop borrower a copy of the DS Unclassified/SBU Laptop Cyber Security Awareness Briefing to read prior to picking up a laptop. OIG found that none of the 27 laptop borrowers tested had signed an Embassy-specific laptop loan form acknowledging that they had received the briefing. OIG noted that 23 of the 27 users had signed an Embassy-specific acknowledgement form attesting to the fact that they had received the required annual cyber security awareness training, which is different from the laptop-specific briefing. The four remaining laptop users signed another Embassy-specific form that did not include an acknowledgement section regarding security training. Of 14 users OIG interviewed, eight (57 percent) said that they had not received the briefing.

Embassy Rome. According to the Information Security Officer, Embassy Rome did not have a mechanism in place to ensure that the training was received annually; rather, the borrowers self-certified that they had taken the training when they signed out the computers. Prospective laptop users were advised by the ISO of the DS cyber security briefing on the Web site. The ISO said that he destroys laptop loan documents immediately when loaned laptops are returned and does not maintain a log of users who have received the briefing. Therefore, at any given time, records are available only for laptops currently on loan. During OIG's visit, 18 laptops were on loan, and all the borrowers had signed Form DS-7642. All nine laptop users OIG interviewed said that they had been briefed.

To comply with Department policy, the IMO needs to ensure that laptop users have received the required laptop security briefing and have signed an acknowledgement form. OIG concluded, based on its analyses, that not all users had been briefed on their laptop security requirements. This occurred because of the described weaknesses over presenting users with the briefing information. To ensure that all users are properly briefed each year, a formal training session is preferable to reviewing briefing slides or visiting the DS Web site. This type of session would allow for student-instructor interaction and would provide the most up-to-date information on the subject.

There is precedent for conducting laptop briefings in this manner. On June 17, 2009, DS issued a Department Notice, Laptop Cyber Security Awareness Briefing Schedule, which stated that all users in the Washington, D.C., area who had been assigned an unclassified/SBU laptop computer were required to attend an initial briefing and to renew their certification annually. DS schedules two briefings each month that last 1 hour each. The potential for compromised laptop data is greater overseas than domestically, and face-to-face briefings could readily be duplicated at overseas embassies and posts. These briefings would likely enhance the security awareness of laptop users. Domestic bureaus can continue to provide staff with their own laptop security briefings rather than the DS version.

Embassy Tokyo. The Information Systems Security Officer at Embassy Tokyo said that he required users to review the DS briefing in the IMO section's office area before he issued the loaned laptop. The user and the Information Systems Security Officer then signed the recommended DS briefing acknowledgement form. OIG believes this policy is more robust than policies at the other locations visited, as it requires the user to actually view the briefing. Nonetheless, OIG found that six (23 percent) of the 26 user files it reviewed did not contain signed acknowledgement forms, and the IMO could not provide reasons for the omissions.

Embassy Vienna. IMO policy at Embassy Vienna is to send the prospective laptop users an e-mail that contains the link to the DS Web site and instructs the users to review the briefing material on that site. When users pick up their laptops, they sign the DS-recommended acknowledgement form. OIG found that 14 (50 percent) of the 28 laptop user files did not contain signed acknowledgement forms. Of eight laptop users interviewed, only one said that he had not been briefed.

AIT Taipei. The Information Systems Security Officer at AIT Taipei required all users to take the DS briefing from the DS Web site. After taking the briefing, the user printed out the training certificate and signed it, which acknowledged receipt of the awareness briefing. The user then provided a copy of the certificate to the Information Systems Security Officer, who retained the certificate for 1 year. When the training was documented, the Information Systems Security Officer loaned the user a laptop. OIG found that for 26 of the 30 laptops on loan at the time of its visit, a completed laptop user acknowledgement form was on file, reflecting an 87 percent compliance rate. This was the highest rate of acknowledgement certificates for the six locations in OIG's sample. All three of the laptop users interviewed said that they had received a laptop security briefing.

Recommendation 10. OIG recommends that the Bureau of Information Resource Management (IRM) reinforce the requirements that all laptop users should receive the Bureau of Diplomatic Services Unclassified/SBU Laptop Cyber Security Briefing and that the employee and the Information Management Office briefer should sign and retain the accompanying acknowledgement form. In addition, IRM should encourage all embassies and posts to provide, to laptop users, interactive annual briefings.

Management Response. IRM said that it had issued guidance to posts to address this recommendation in the September 25, 2009, ALDAC 09 STATE 100287 that "remind[s] personnel about laptop inventory accountability responsibilities."

OIG Reply. However, the ALDAC, which has expired, did not discuss the part of the recommendation relating to encouraging posts to ensure that laptop users are fully aware of their responsibilities. In that regard, interactive briefings, with opportunities for users to ask questions and receive answers, should be provided to potential laptop users. OIG believes that this approach would strengthen the briefing process and help ensure that users understand their responsibilities before they receive their laptops.

Recommendation 10 is considered resolved, pending receipt of documentation showing that IRM has codified, in the FAM and/or the FAH, guidance for the posts to make laptop users more fully aware of their responsibilities regarding laptops, such as by encouraging posts to conduct interactive briefing sessions annually.

Recommendation 11. OIG recommends that Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and the American Institute in Taiwan require the Information Management Officer to ensure that all laptop users receive the annual cyber security awareness briefing and to maintain documentation to support that the briefing was presented.

Management Response. Embassy Bogota agreed, stating that the IMO "is now managing the complete laptop program." The Embassy further stated that the user acknowledges that the briefing has been completed by "signing the form DS-7642 Mobile Computing and Data Storage Request." Embassy Rome stated that the GSO and the IMO sections had developed and implemented operating procedures to improve coordination between the offices and to address this recommendation. Embassy Tokyo agreed with the recommendation, stating that its ISO ensures that all laptop users receive the briefing, which "must take place on a stand-alone computer within the Information Systems Center (ISC)." Embassy Tokyo also stated that the ISC "maintains documentation" supporting that the briefing was presented. Embassy Vienna stated that it was updating its cybersecurity acknowledgement forms.

OIG Reply. As stated in Recommendation 10, all posts should have interactive briefing sessions given by the ISSO, and an acknowledgement form developed by DS or a similar form should be filled out and certified by both the briefer and the laptop user. The signing of Form DS-7642 is not a substitute for the DS acknowledgement form, which serves as a certificate of training completion.

Embassies Bogota, Rome, Tokyo, and Vienna sufficiently addressed Recommendation 11, pending receipt of confirmation showing that the laptop users actually received the security awareness briefing. However, the recommendation is considered unresolved until Embassy Mexico City and AIT Taipei provide responses to the recommendation.

Finding C. Hard Drive Disposition/Destruction Process Improvements Are Needed

Although four of the six sites visited followed proper laptop hard drive disposition/destruction procedures, procedures at Embassy Bogota and AIT Taipei needed improvement. Specifically, Embassy Bogota's NAS officials did not send their laptop hard drives to IRM for disposition/destruction as required, and AIT Taipei did not maintain documentation to support that the hard drives were destroyed in accordance with the FAH (12 FAH-6 H-542.5-10). Without adhering to these controls, the Department had no assurance that accountability over hard drive disposition was being maintained, and data on the hard drives could be at risk of unauthorized disclosure and use.

Embassy Bogota. During FY 2008, Embassy Bogota's NAS disposed of 14 laptops through auction, but the NAS did not follow the Department's regulation for the proper disposition of hard drives. The FAH (12 FAH-6 H-542.5-10) requires all hard drives to be sent via classified pouch to IRM for disposition.

NAS officials said that the hard drives had been erased with Department-approved software to remove any information prior to sale. However, all hard drives must be sent via classified pouch to IRM for disposition. The NAS officials further stated that they were unaware of the requirement to send the hard drives to IRM and that it was the NAS's understanding that embassies and posts were allowed to sanitize hard drives and to destroy them in accordance with local procedures.

AIT Taipei. AIT Taipei officials could not account for 14 hard drives. The Information Systems Security Officer said that the hard drives were shipped back to Washington, D.C., for destruction and provided OIG with supporting documentation. The documentation included a shipping telegram and two diplomatic pouch receipts (Form OF-120, Diplomatic Pouch Mail Registration) to support the shipment of various hard drives. However, the receipts did not identify serial numbers, NEPA numbers, or other specific information that could be traced back to AIT Taipei inventory records.

AIT Taipei officials were using a disposition request telegram that did not have sufficient detail to identify the shipped hard drives. AIT Taipei officials did not follow IRM's Web site guidance, under the template "Sample Disposal Telegram," which provides directions to posts and recommends that posts send a telegram to IRM requesting disposition instructions before shipping items for destruction. In the telegram, IRM requires detailed descriptive information on each shipped item, to include manufacturer, model, serial number, bar code, classification, and location.

Because the 14 hard drives could not be accounted for, there was no assurance that they were properly destroyed. Therefore, data stored on these hard drives may be at risk of improper dissemination and use.

Recommendation 12. OIG recommends that the Bureau of Information Resource Management (IRM) direct all overseas embassies and posts to comply with the requirements stipulated on IRM's Web site for the proper disposition/destruction of hard drives on laptop computers.

Management Response. IRM provided information contained in its September 25, 2009, ALDAC 09 STATE 100287 regarding embassy and post compliance on IRM's Web site for the proper disposition/destruction of hard drives.

OIG Reply. However, in accordance with the FAH (7 FAH-1 H-145), information contained in this ALDAC has expired. In accordance with the FAH, IRM should codify, in the FAM and/or the FAH, guidance on appropriate procedures for the IMOs to follow regarding the disposition/destruction of laptop computers.

Recommendation 12 is considered resolved, pending receipt of documentation showing that the procedures specified have been codified.

Recommendation 13. OIG recommends that Embassy Bogota and the American Institute in Taiwan require the Information Management Officer to comply with the provisions of the Foreign Affairs Handbook (12 FAH-6 H-542.5-10) for hard drive disposition and the proper preparation of laptop shipping documentation.

Management Response. Embassy Bogota agreed with Recommendation 13, stating that the IMO "is now managing the laptop program including all NAS laptops." The Embassy further stated, "Disposition of all NAS laptops and hard drives will comply with the provisions of 12 FAH-6 H-542.5-10."

OIG Reply. Embassy Bogota sufficiently addressed Recommendation 13. However, the recommendation is considered unresolved until AIT Taipei provides a response to the report.

Finding D. Overseas Post Encryption Rates for Laptop Computers Have Improved

The Department requires that all laptop computers be encrypted. In that regard, OIG found, in a sample[13] of 350 laptop computers, that 298 (85 percent) laptop computers tested were encrypted, as shown in Table 3. The encryption rates varied considerably by location and ranged from 28 percent at Embassy Mexico City to 100 percent at Embassy Rome. Encryption of laptop computers is critical because it reduces the likelihood that data stored on laptops will be compromised. The three embassies (Embassies Bogota, Mexico City, and Vienna) that had not encrypted all of their laptops were aware of the requirement, but for operational reasons, they had not achieved a 100 percent encryption rate at the time of OIG's review.

[13] Generally, OIG randomly sampled laptop computers to test for encryption. However, OIG tested only those laptop computers for encryption that were operational. Computers in the process of being disposed of with the hard drives removed were not tested. Additionally, laptop computers with encryption waivers were not subjected to testing. At Embassy Tokyo and AIT Taipei, OIG was able to test all laptop computers for encryption rather than just a sample.

Table 3. Results of Encryption Testing of Laptop Computers

	Bogota	Mexico City	Rome	Tokyo	Vienna	Taipei	Totals
Number of laptops tested	32	32	49	105	69	63	350
Number of laptops encrypted	25	9	49	104	49	62	298
Number of laptops not encrypted	7	23	0	1	20	1	52
Percent of encrypted laptops	78	28	100	99	71	98	85

The Department issued ALDAC STATE 00064226, "Reminder: Unclassified and SBU Laptop Encryption Responsibilities," June 2008, to all diplomatic and consular posts that reminded IMOs and Information Systems Security Officers of their responsibilities to ensure that all Department-owned laptops are encrypted, and it established a date of July 1, 2008, for that goal to be achieved.

Embassy Bogota. At Embassy Bogota, OIG found that 25 (78 percent) of 32 laptops it tested for encryption were actually encrypted. Embassy officials said that some laptops had not been encrypted because they were too old, were waiting for disposal, or had insufficient memory. Despite these circumstances, however, sufficient time had elapsed since the Department notification (June 2008) for all posts to take the actions specified in the telegram regarding laptops that cannot be encrypted.

Embassy Mexico City. At Embassy Mexico City, only nine (28 percent) of 32 laptops were encrypted. The other 23 laptops were not encrypted. Embassy officials said that they did not know that those laptops were in the Embassy's inventory. The users said that three of the 23 unencrypted laptops had PII stored on them.

Embassy Vienna. At Embassy Vienna, 49 (71 percent) of 69 laptops tested were fully encrypted. Embassy officials said that some laptops had not been encrypted because they were too old, had insufficient memory, or were used exclusively for training. Moreover, Embassy officials had problems encrypting laptops because the Embassy was used as a lead post for the Department's encryption initiative and the officials said that they had to work out issues involving the Protect-Drive encryption software.

Embassy Tokyo and AIT Taipei. Embassy Tokyo and AIT Taipei had only one laptop each that was not encrypted. The Embassy's laptop was not encrypted because of compatibility issues between the encryption software and the operating system, and AIT Taipei's laptop was not encrypted because of the laptop's age and its specialized use.

Again, in each circumstance where laptops were not encrypted, sufficient time had elapsed since the Department notification for all posts to have taken appropriate actions in accordance with the guidance. When laptops could not be encrypted, they should have been excessed or had encryption waivers obtained for them, as addressed in STATE 00064226.

Because of the importance inherent in safeguarding sensitive information (that is, national security or PII) from unauthorized viewing, coupled with the heightened concern over the extent to which sensitive information maintained by federal agencies is vulnerable to theft or compromise, the Department and particularly the CIO need a greater level of assurance from the posts that all Department-owned laptop computers and other mobile computing devices used by personnel at overseas posts have been configured with approved encryption software to protect information stored on these devices. Therefore, OIG believes that one approach to gain greater assurance that appropriate and continuous actions are being taken is to have the IMOs inform IRM annually of the program status at their respective embassies and posts.

Recommendation 14. OIG recommends that the Bureau of Information Resource Management (IRM) require each embassy and post to certify annually that all laptop computers have been encrypted. In addition, for laptops that cannot be encrypted or where there is a valid operational justification for the laptops not to be encrypted, IRM should remind embassies and posts of the requirement to obtain waivers from IRM's Information Assurance Office.

Management Response. IRM stated that it "will work with the Bureau of Diplomatic Security to require each embassy and post to certify, annually, that all laptop computers have been encrypted." IRM also stated that its September 25, 2009, ALDAC 09 STATE 100287 reminds posts of the requirement to obtain waivers to laptop encryption from IRM/IA. IRM cited two paragraphs (Nos. 3F and 4) in the ALDAC that directed posts to a Web link at IRM/IA to obtain more information on the laptop encryption waiver request process.

OIG Reply. In accordance with the FAH (7 FAH-1 H-145), information policies and procedures contained in the September ALDAC have expired. Therefore, in accordance with the FAH, IRM should codify, in the FAM and/or the FAH, specific guidance to the posts on how to obtain laptop encryption waivers.

Recommendation 14 is considered resolved, pending receipt of documentation showing that guidance on how to obtain laptop encryption waivers has been codified in the FAM and/or the FAH.

Recommendation 15. OIG recommends that Embassies Bogota, Mexico City, and Vienna require the Information Management Officer to comply with Department of State policy to encrypt all laptops or to obtain waivers when there is a valid operational justification.

Management Response. Embassy Bogota stated that the IMO is now managing the laptop program, that all laptops have been encrypted, and that the NAS and the RSO laptops that were too old for encryption have been disposed of.

Embassy Vienna stated that "all laptops under [its] control are being encrypted" and that it had requested and obtained waivers as was recommended.

OIG Reply. Embassies Bogota and Vienna sufficiently addressed Recommendation 15. However, the recommendation is considered unresolved until Embassy Mexico City provides a response to the report.

RECOMMENDATIONS

Recommendation 1. OIG recommends that the Bureau of Information Resource Management emphasize, to Information Management Officers, their responsibility for entering all Department of State laptop computers under their control into the official inventory and entering them in a timely manner.

Recommendation 2. OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer and the General Services Officer to ensure that all laptops are properly entered into the post inventory system and periodically reconciled to manual records.

Recommendation 3. OIG recommends that the Bureau of Administration and the Bureau of Information Resource Management clarify the roles and responsibilities of the posts' Information Management Officer and the General Services Officer for controlling and inventorying laptop computers. They should also require posts to validate and reconcile the official laptop computer inventory data more frequently than annually.

Recommendation 4. OIG recommends that Embassies Bogota and Mexico City require the Information Management Officer to submit the results of the next physical inventory of laptop computers, along with the accompanying reconciliation of the official inventory with the Information Management Officer's unofficial inventory, to the Bureau of Information Resource Management and the Office of Inspector General.

Recommendation 5. OIG recommends that the Bureau of Administration ensure that data fields for the dates of original entry for laptop computers are available in the Non-Expendable Property Application and the Integrated Logistics Management System to facilitate inventory monitoring efforts.

Recommendation 6. OIG recommends that the Bureau of Information Resource Management ensure that embassies and posts properly complete loan documents and maintain them for at least 12 months after a laptop computer has been returned to allow for subsequent review, audit, or investigation if the laptop computer is damaged or missing.

Recommendation 7. OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer to ensure compliance with laptop loan-out procedures and the proper preparation of supporting documentation.

Recommendation 8. OIG recommends that the Bureau of Information Resource Management remind posts to immediately report stolen and missing laptops; complete Form DS-132, Property Disposal Authorization and Survey Report; and conduct investigations of stolen and missing laptops.

Recommendation 9. OIG recommends that Embassy Bogota require the Information Management Officer and the General Services Officer to investigate the disposition of each missing laptop and prepare the required documentation as necessary. The Bureau of Information Resource Management and the Office of the Inspector General should then be notified with the accompanying documentation.

Recommendation 10. OIG recommends that the Bureau of Information Resource Management (IRM) reinforce the requirements that all laptop users should receive the Bureau of Diplomatic Services Unclassified/SBU Laptop Cyber Security Briefing and that the employee and the Information Management Office briefer should sign and retain the accompanying acknowledgement form. In addition, IRM should encourage all embassies and posts to provide, to laptop users, interactive annual briefings.

Recommendation 11. OIG recommends that Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and the American Institute in Taiwan require the Information Management Officer to ensure that all laptop users receive the annual cyber security awareness briefing and to maintain documentation to support that the briefing was presented.

Recommendation 12. OIG recommends that the Bureau of Information Resource Management (IRM) direct all overseas embassies and posts to comply with the requirements stipulated on IRM's Web site for the proper disposition/destruction of hard drives on laptop computers.

Recommendation 13. OIG recommends that Embassy Bogota and the American Institute in Taiwan require the Information Management Officer to comply with the provisions of the Foreign Affairs Handbook (12 FAH-6 H-542.5-10) for hard drive disposition and the proper preparation of laptop shipping documentation.

Recommendation 14. OIG recommends that the Bureau of Information Resource Management (IRM) require each embassy and post to certify annually that all laptop computers have been encrypted. In addition, for laptops that cannot be encrypted or where there is a valid operational justification for the laptops not to be encrypted, IRM should remind embassies and posts of the requirement to obtain waivers from IRM's Information Assurance Office.

Recommendation 15. OIG recommends that Embassies Bogota, Mexico City, and Vienna require the Information Management Officer to comply with Department of State policy to encrypt all laptops or to obtain waivers when there is a valid operational justification.

APPENDIX A

Scope and Methodology

The Office of Inspector General (OIG) visited Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and the American Institute of Taiwan (AIT) in Taipei during February and March 2009. OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those 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 objectives. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

OIG analyzed Department of State policies and procedures, as well as other relevant laws, regulations, and standards, including the Foreign Affairs Manual, the Foreign Affairs Handbook, the Government Accountability Office's Standards for Internal Control in the Federal Government, and Office of Management and Budget directives. OIG also interviewed officials who were responsible for managing and maintaining the laptop computers, applicable records, and inventory and acquisition systems at the embassies and posts. OIG also interviewed officials from the Bureau of Information Resource Management (IRM), the Bureau of Diplomatic Security, and the Bureau of Administration who were involved with laptop computers at Department headquarters. Moreover, OIG interviewed representatives of the regional bureaus to obtain their perspectives and understanding of their roles and responsibilities with respect to accounting for and providing security over laptop computers at post.

The overseas posts were selected for site visits and review using a nonstatistical sampling method known as judgmental sampling. Rather than basing the selection criteria on the laws of probability, a judgment sample is chosen via the use of discretionary criteria. The criteria for selection of posts included the number of laptop computers reported by the posts in response to an IRM survey, the self-reported encryption rates reported in this survey, failure to respond to the IRM survey, the inventory control system in place (Non-Expendable Property Application or Integrated Logistics Management System), geographical distribution, and the recency of OIG visits.

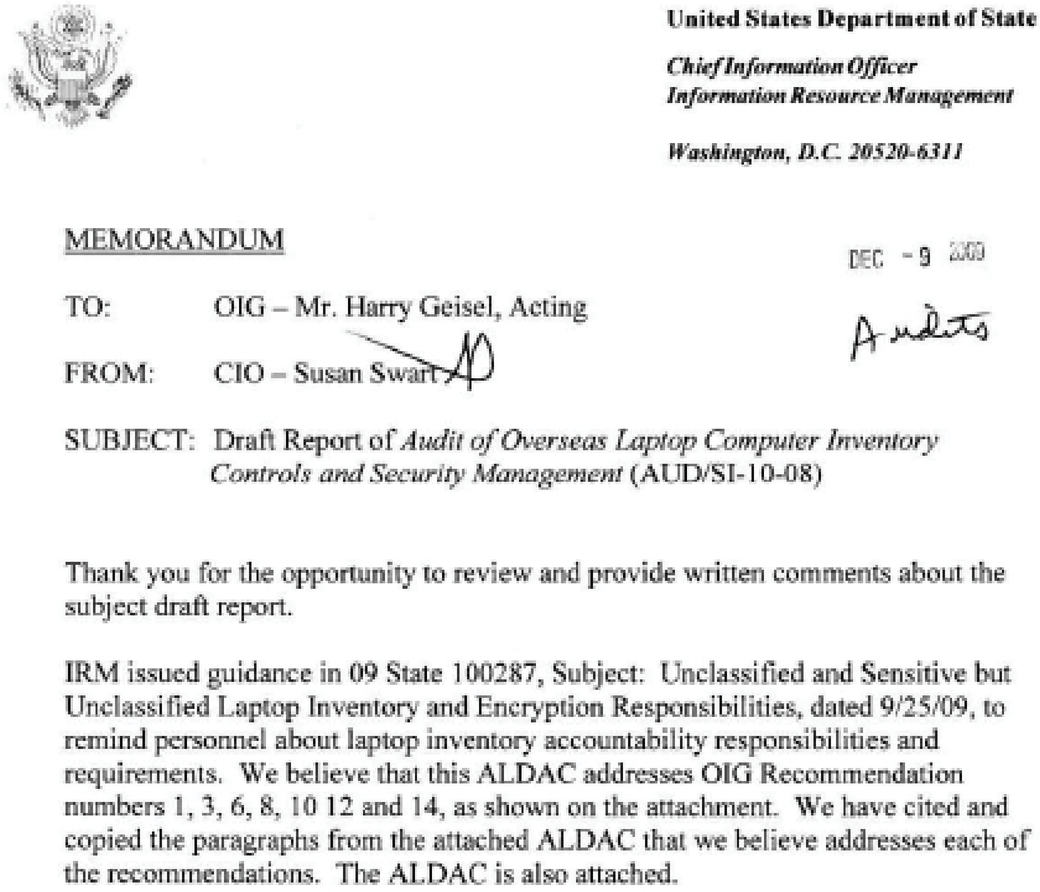
With respect to selecting individual items to test at each post, one of three procedures was used. In order of preference, the procedures were census (that is, complete enumeration of a population), statistical sampling, and nonstatistical sampling. Regardless of the sampling procedure chosen for a particular test, the actual selection of the specific items was accomplished via the use of random numbers whenever practicable, even if a nonstatistical sample, such as judgment sampling, was used in order to preclude the introduction of bias into the selection process. Factors considered in determining the particular method chosen included time constraints and the adequacy of the embassies' or posts' records.

Other areas of testing included a review of the adequacy of laptop computer loan documentation, compliance with disposal procedures, and the completeness of documentation to support the required cyber security awareness briefing. All OIG testing, including the results, is detailed in appropriate sections of the report.

Review of Internal Controls

OIG tested the official inventory lists provided for existence and completeness to assess whether the system of internal controls over the inventory of laptop computers was effective (that is, whether it provided reasonable assurance as to the reliability of inventory information and accountability of the individual computers). As stated in the report, OIG identified internal control weaknesses in recording laptops in the official inventory and/or in entering the laptops into the inventory in a timely manner, in the laptop loan documentation process, and in the coordination between post sections for validating and reconciling the inventory of laptops.

APPENDIX B



United States Department of State

Chief Information Officer
Information Resource Management

Washington, D.C. 20520-6311

MEMORANDUM

DEC -9 2009

Audits

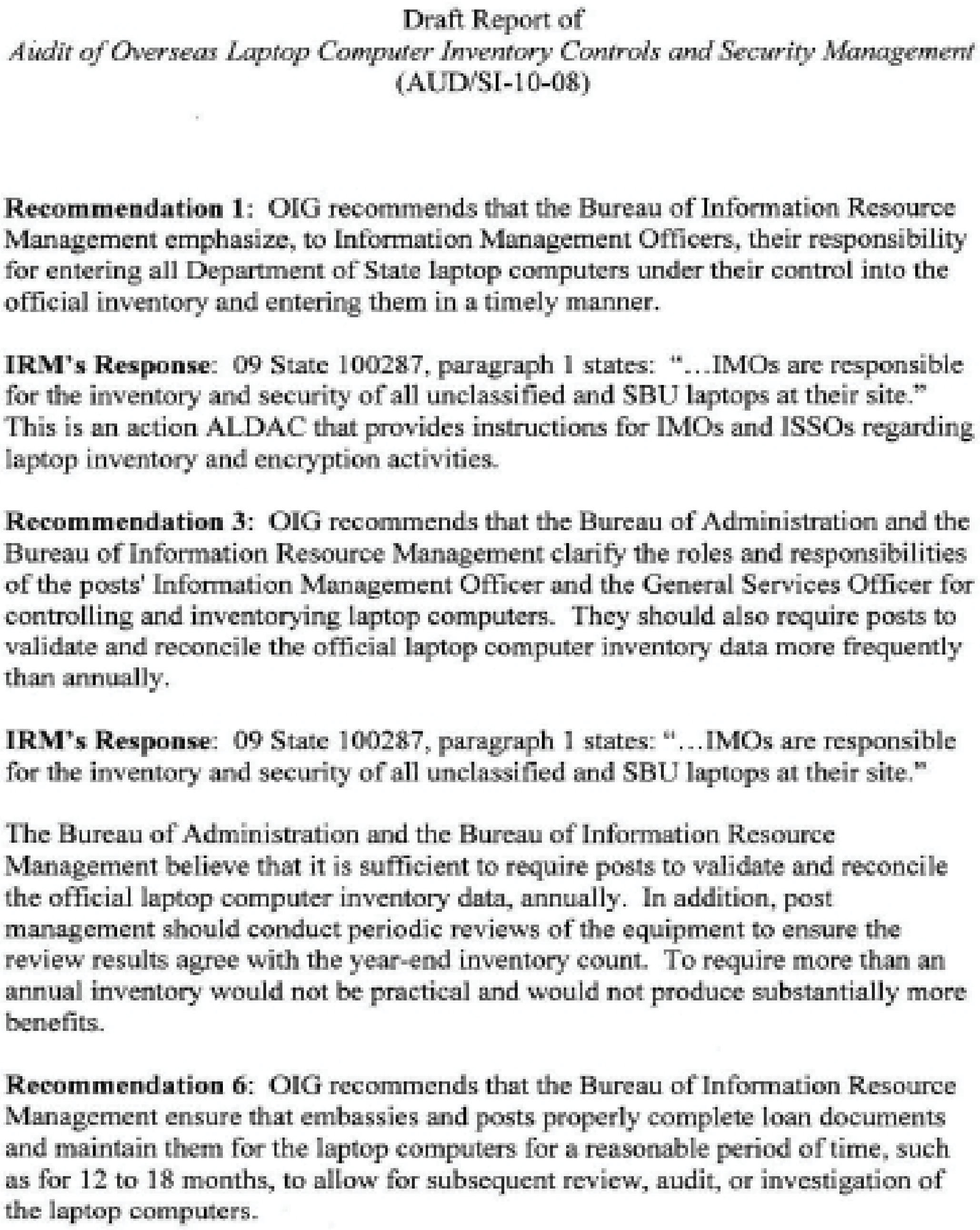
TO: OIG – Mr. Harry Geisel, Acting

FROM: CIO – Susan Swart

SUBJECT: Draft Report of *Audit of Overseas Laptop Computer Inventory Controls and Security Management* (AUD/SI-10-08)

Thank you for the opportunity to review and provide written comments about the subject draft report.

IRM issued guidance in 09 State 100287, Subject: Unclassified and Sensitive but Unclassified Laptop Inventory and Encryption Responsibilities, dated 9/25/09, to remind personnel about laptop inventory accountability responsibilities and requirements. We believe that this ALDAC addresses OIG Recommendation numbers 1, 3, 6, 8, 10 12 and 14, as shown on the attachment. We have cited and copied the paragraphs from the attached ALDAC that we believe addresses each of the recommendations. The ALDAC is also attached.



Draft Report of
Audit of Overseas Laptop Computer Inventory Controls and Security Management
(AUD/SI-10-08)

Recommendation 1: OIG recommends that the Bureau of Information Resource Management emphasize, to Information Management Officers, their responsibility for entering all Department of State laptop computers under their control into the official inventory and entering them in a timely manner.

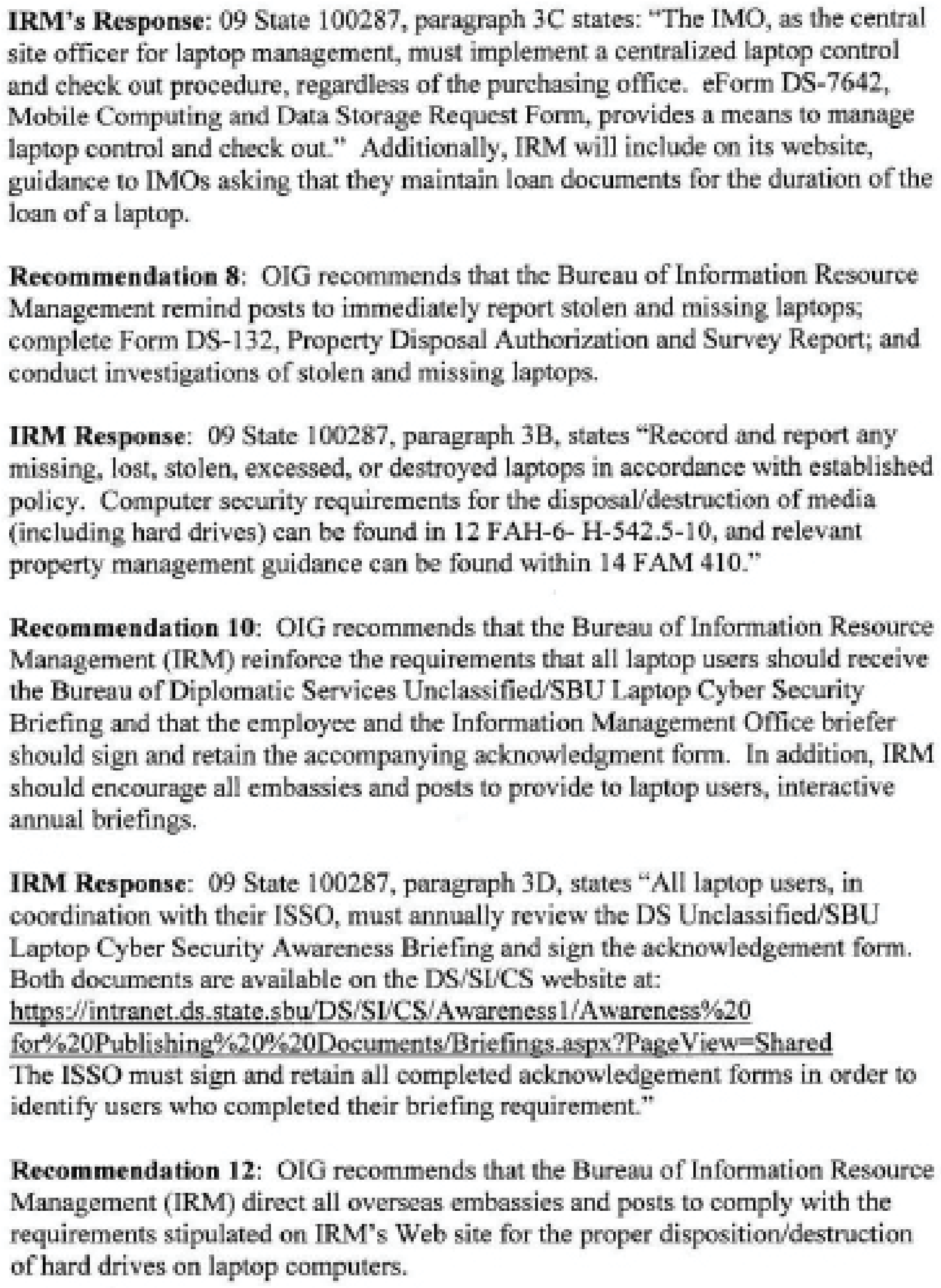
IRM's Response: 09 State 100287, paragraph 1 states: "…IMOs are responsible for the inventory and security of all unclassified and SBU laptops at their site." This is an action ALDAC that provides instructions for IMOs and ISSOs regarding laptop inventory and encryption activities.

Recommendation 3: OIG recommends that the Bureau of Administration and the Bureau of Information Resource Management clarify the roles and responsibilities of the posts' Information Management Officer and the General Services Officer for controlling and inventorying laptop computers. They should also require posts to validate and reconcile the official laptop computer inventory data more frequently than annually.

IRM's Response: 09 State 100287, paragraph 1 states: "…IMOs are responsible for the inventory and security of all unclassified and SBU laptops at their site."

The Bureau of Administration and the Bureau of Information Resource Management believe that it is sufficient to require posts to validate and reconcile the official laptop computer inventory data, annually. In addition, post management should conduct periodic reviews of the equipment to ensure the review results agree with the year-end inventory count. To require more than an annual inventory would not be practical and would not produce substantially more benefits.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management ensure that embassies and posts properly complete loan documents and maintain them for the laptop computers for a reasonable period of time, such as for 12 to 18 months, to allow for subsequent review, audit, or investigation of the laptop computers.



IRM's Response: 09 State 100287, paragraph 3C states: "The IMO, as the central site officer for laptop management, must implement a centralized laptop control and check out procedure, regardless of the purchasing office. eForm DS-7642, Mobile Computing and Data Storage Request Form, provides a means to manage laptop control and check out." Additionally, IRM will include on its website, guidance to IMOs asking that they maintain loan documents for the duration of the loan of a laptop.

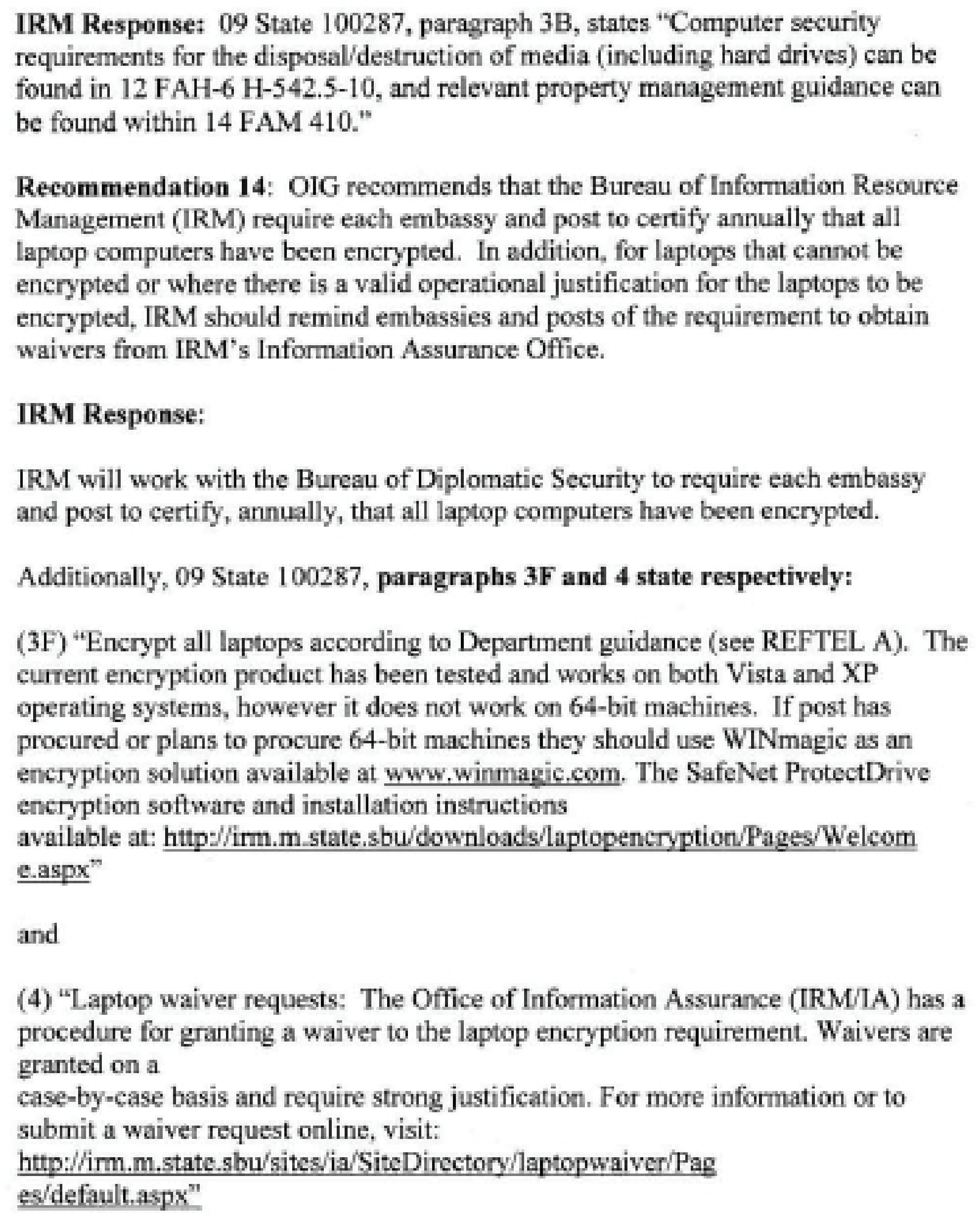
Recommendation 8: OIG recommends that the Bureau of Information Resource Management remind posts to immediately report stolen and missing laptops; complete Form DS-132, Property Disposal Authorization and Survey Report; and conduct investigations of stolen and missing laptops.

IRM Response: 09 State 100287, paragraph 3B, states "Record and report any missing, lost, stolen, excessed, or destroyed laptops in accordance with established policy. Computer security requirements for the disposal/destruction of media (including hard drives) can be found in 12 FAH-6- H-542.5-10, and relevant property management guidance can be found within 14 FAM 410."

Recommendation 10: OIG recommends that the Bureau of Information Resource Management (IRM) reinforce the requirements that all laptop users should receive the Bureau of Diplomatic Services Unclassified/SBU Laptop Cyber Security Briefing and that the employee and the Information Management Office briefer should sign and retain the accompanying acknowledgment form. In addition, IRM should encourage all embassies and posts to provide to laptop users, interactive annual briefings.

IRM Response: 09 State 100287, paragraph 3D, states "All laptop users, in coordination with their ISSO, must annually review the DS Unclassified/SBU Laptop Cyber Security Awareness Briefing and sign the acknowledgement form. Both documents are available on the DS/SI/CS website at:
https://intranet.ds.state.sbu/DS/SI/CS/Awareness1/Awareness%20for%20Publishing%20%20Documents/Briefings.aspx?PageView=Shared
The ISSO must sign and retain all completed acknowledgement forms in order to identify users who completed their briefing requirement."

Recommendation 12: OIG recommends that the Bureau of Information Resource Management (IRM) direct all overseas embassies and posts to comply with the requirements stipulated on IRM's Web site for the proper disposition/destruction of hard drives on laptop computers.



IRM Response: 09 State 100287, paragraph 3B, states "Computer security requirements for the disposal/destruction of media (including hard drives) can be found in 12 FAH-6 H-542.5-10, and relevant property management guidance can be found within 14 FAM 410."

Recommendation 14: OIG recommends that the Bureau of Information Resource Management (IRM) require each embassy and post to certify annually that all laptop computers have been encrypted. In addition, for laptops that cannot be encrypted or where there is a valid operational justification for the laptops to be encrypted, IRM should remind embassies and posts of the requirement to obtain waivers from IRM's Information Assurance Office.

IRM Response:

IRM will work with the Bureau of Diplomatic Security to require each embassy and post to certify, annually, that all laptop computers have been encrypted.

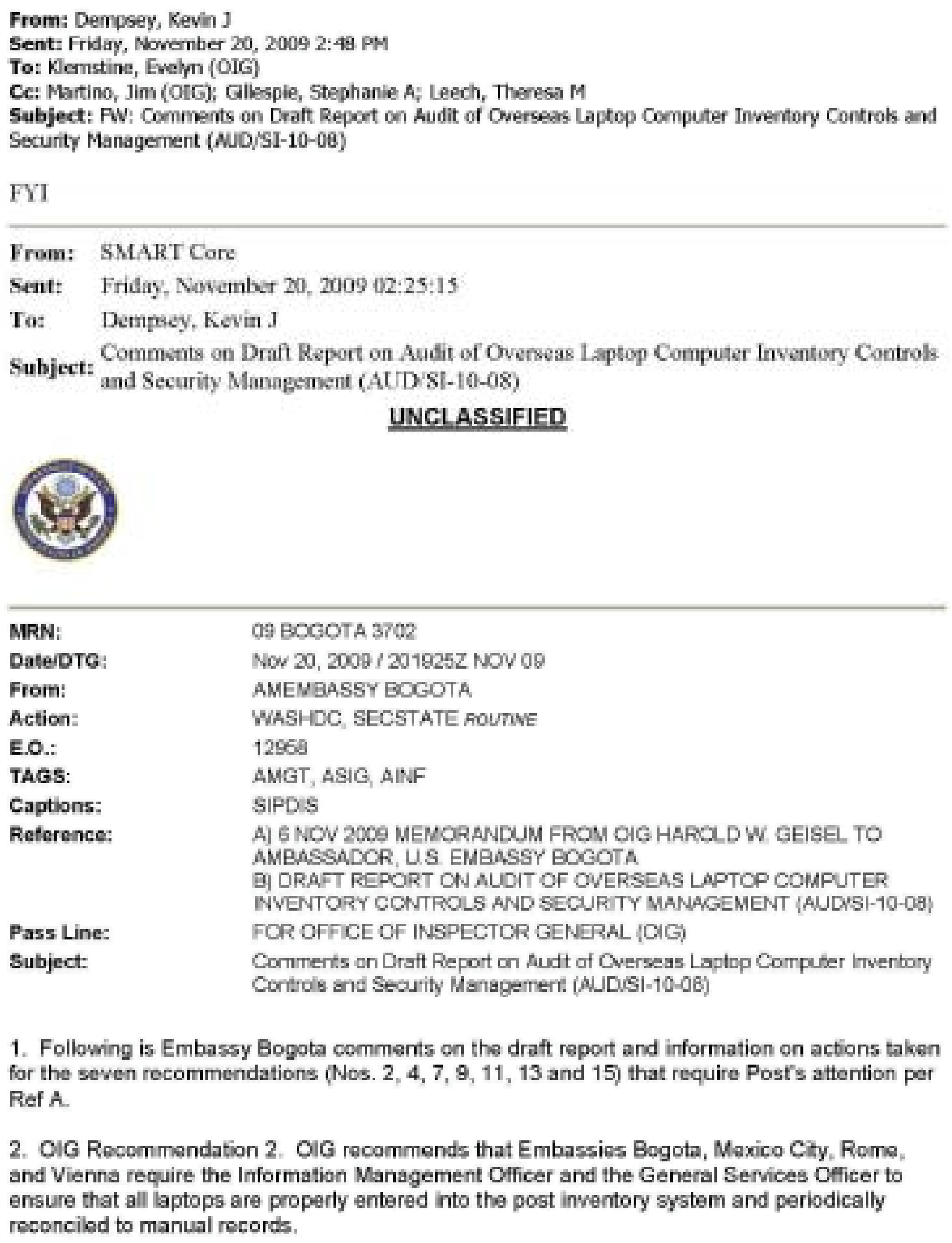
Additionally, 09 State 100287, **paragraphs 3F and 4 state respectively:**

(3F) "Encrypt all laptops according to Department guidance (see REFTEL A). The current encryption product has been tested and works on both Vista and XP operating systems, however it does not work on 64-bit machines. If post has procured or plans to procure 64-bit machines they should use WINmagic as an encryption solution available at www.winmagic.com. The SafeNet ProtectDrive encryption software and installation instructions available at: http://irm.m.state.sbu/downloads/laptopencryption/Pages/Welcome.aspx"

and

(4) "Laptop waiver requests: The Office of Information Assurance (IRM/IA) has a procedure for granting a waiver to the laptop encryption requirement. Waivers are granted on a case-by-case basis and require strong justification. For more information or to submit a waiver request online, visit: http://irm.m.state.sbu/sites/ia/SiteDirectory/laptopwaiver/Pages/default.aspx"

APPENDIX C



From: Dempsey, Kevin J
Sent: Friday, November 20, 2009 2:48 PM
To: Klemstine, Evelyn (OIG)
Cc: Martino, Jim (OIG); Gillespie, Stephanie A; Leech, Theresa M
Subject: FW: Comments on Draft Report on Audit of Overseas Laptop Computer Inventory Controls and Security Management (AUD/SI-10-08)

FYI

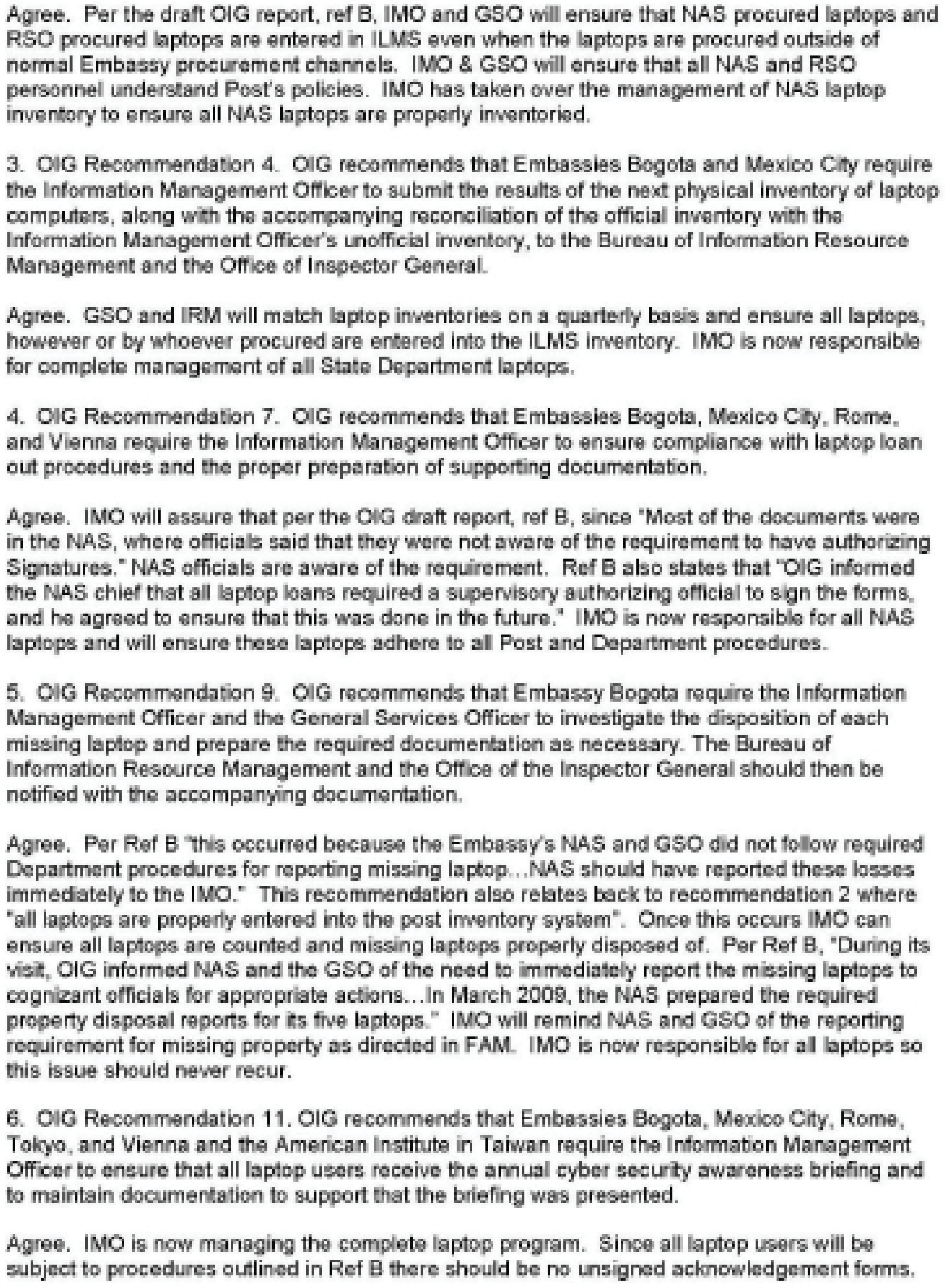
From: SMART Core
Sent: Friday, November 20, 2009 02:25:15
To: Dempsey, Kevin J
Subject: Comments on Draft Report on Audit of Overseas Laptop Computer Inventory Controls and Security Management (AUD/SI-10-08)

UNCLASSIFIED

MRN:	09 BOGOTA 3702
Date/DTG:	Nov 20, 2009 / 201925Z NOV 09
From:	AMEMBASSY BOGOTA
Action:	WASHDC, SECSTATE *ROUTINE*
E.O.:	12958
TAGS:	AMGT, ASIG, AINF
Captions:	SIPDIS
Reference:	A) 6 NOV 2009 MEMORANDUM FROM OIG HAROLD W. GEISEL TO AMBASSADOR, U.S. EMBASSY BOGOTA B) DRAFT REPORT ON AUDIT OF OVERSEAS LAPTOP COMPUTER INVENTORY CONTROLS AND SECURITY MANAGEMENT (AUD/SI-10-08)
Pass Line:	FOR OFFICE OF INSPECTOR GENERAL (OIG)
Subject:	Comments on Draft Report on Audit of Overseas Laptop Computer Inventory Controls and Security Management (AUD/SI-10-08)

1. Following is Embassy Bogota comments on the draft report and information on actions taken for the seven recommendations (Nos. 2, 4, 7, 9, 11, 13 and 15) that require Post's attention per Ref A.

2. OIG Recommendation 2. OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer and the General Services Officer to ensure that all laptops are properly entered into the post inventory system and periodically reconciled to manual records.



Agree. Per the draft OIG report, ref B, IMO and GSO will ensure that NAS procured laptops and RSO procured laptops are entered in ILMS even when the laptops are procured outside of normal Embassy procurement channels. IMO & GSO will ensure that all NAS and RSO personnel understand Post's policies. IMO has taken over the management of NAS laptop inventory to ensure all NAS laptops are properly inventoried.

3. OIG Recommendation 4. OIG recommends that Embassies Bogota and Mexico City require the Information Management Officer to submit the results of the next physical inventory of laptop computers, along with the accompanying reconciliation of the official inventory with the Information Management Officer's unofficial inventory, to the Bureau of Information Resource Management and the Office of Inspector General.

Agree. GSO and IRM will match laptop inventories on a quarterly basis and ensure all laptops, however or by whoever procured are entered into the ILMS inventory. IMO is now responsible for complete management of all State Department laptops.

4. OIG Recommendation 7. OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer to ensure compliance with laptop loan out procedures and the proper preparation of supporting documentation.

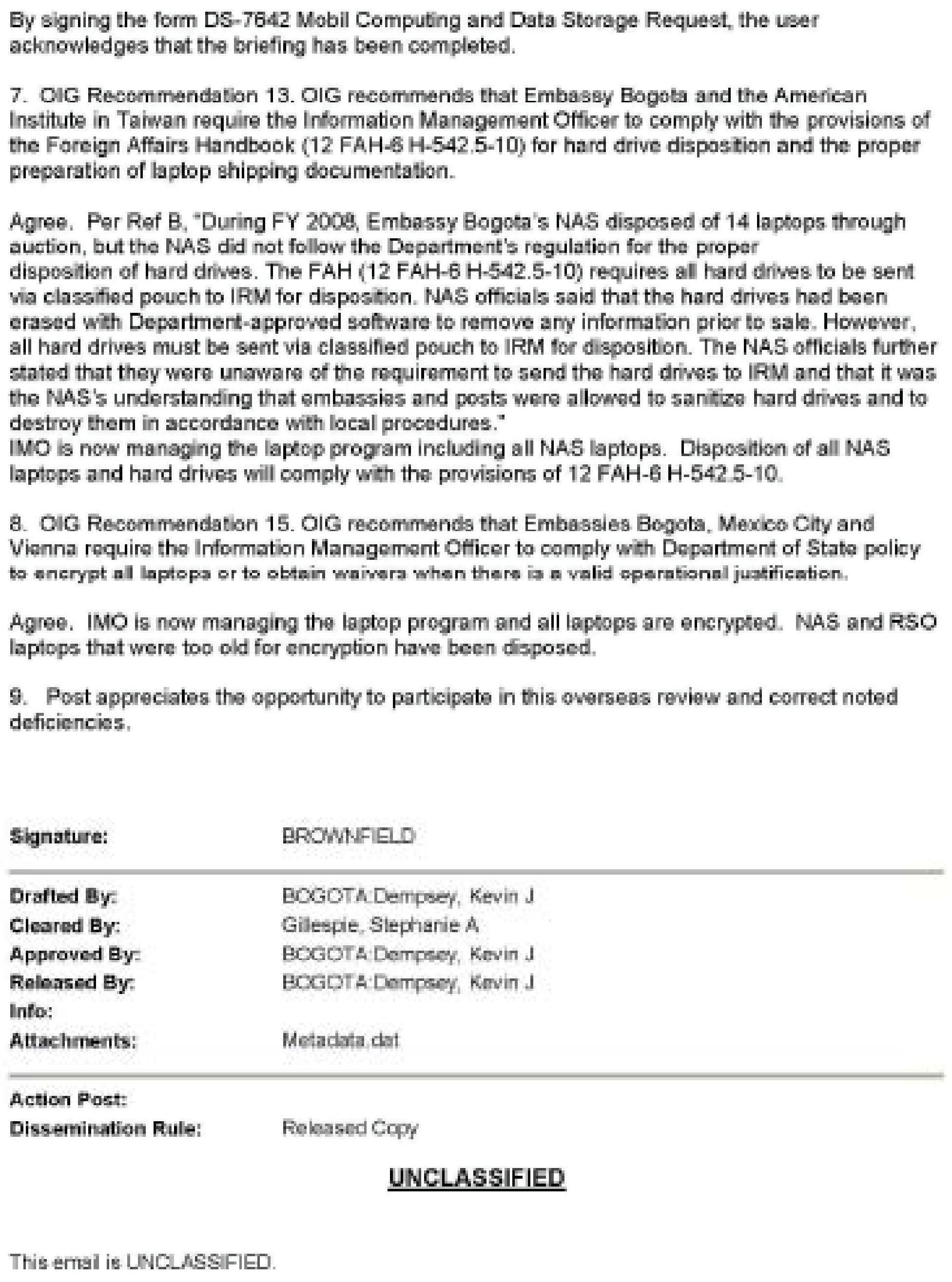
Agree. IMO will assure that per the OIG draft report, ref B, since "Most of the documents were in the NAS, where officials said that they were not aware of the requirement to have authorizing Signatures." NAS officials are aware of the requirement. Ref B also states that "OIG informed the NAS chief that all laptop loans required a supervisory authorizing official to sign the forms, and he agreed to ensure that this was done in the future." IMO is now responsible for all NAS laptops and will ensure these laptops adhere to all Post and Department procedures.

5. OIG Recommendation 9. OIG recommends that Embassy Bogota require the Information Management Officer and the General Services Officer to investigate the disposition of each missing laptop and prepare the required documentation as necessary. The Bureau of Information Resource Management and the Office of the Inspector General should then be notified with the accompanying documentation.

Agree. Per Ref B "this occurred because the Embassy's NAS and GSO did not follow required Department procedures for reporting missing laptop…NAS should have reported these losses immediately to the IMO." This recommendation also relates back to recommendation 2 where "all laptops are properly entered into the post inventory system". Once this occurs IMO can ensure all laptops are counted and missing laptops properly disposed of. Per Ref B, "During its visit, OIG informed NAS and the GSO of the need to immediately report the missing laptops to cognizant officials for appropriate actions…In March 2009, the NAS prepared the required property disposal reports for its five laptops." IMO will remind NAS and GSO of the reporting requirement for missing property as directed in FAM. IMO is now responsible for all laptops so this issue should never recur.

6. OIG Recommendation 11. OIG recommends that Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and the American Institute in Taiwan require the Information Management Officer to ensure that all laptop users receive the annual cyber security awareness briefing and to maintain documentation to support that the briefing was presented.

Agree. IMO is now managing the complete laptop program. Since all laptop users will be subject to procedures outlined in Ref B there should be no unsigned acknowledgement forms.



By signing the form DS-7642 Mobil Computing and Data Storage Request, the user acknowledges that the briefing has been completed.

7. OIG Recommendation 13. OIG recommends that Embassy Bogota and the American Institute in Taiwan require the Information Management Officer to comply with the provisions of the Foreign Affairs Handbook (12 FAH-6 H-542.5-10) for hard drive disposition and the proper preparation of laptop shipping documentation.

Agree. Per Ref B, "During FY 2008, Embassy Bogota's NAS disposed of 14 laptops through auction, but the NAS did not follow the Department's regulation for the proper disposition of hard drives. The FAH (12 FAH-6 H-542.5-10) requires all hard drives to be sent via classified pouch to IRM for disposition. NAS officials said that the hard drives had been erased with Department-approved software to remove any information prior to sale. However, all hard drives must be sent via classified pouch to IRM for disposition. The NAS officials further stated that they were unaware of the requirement to send the hard drives to IRM and that it was the NAS's understanding that embassies and posts were allowed to sanitize hard drives and to destroy them in accordance with local procedures."
IMO is now managing the laptop program including all NAS laptops. Disposition of all NAS laptops and hard drives will comply with the provisions of 12 FAH-6 H-542.5-10.

8. OIG Recommendation 15. OIG recommends that Embassies Bogota, Mexico City and Vienna require the Information Management Officer to comply with Department of State policy to encrypt all laptops or to obtain waivers when there is a valid operational justification.

Agree. IMO is now managing the laptop program and all laptops are encrypted. NAS and RSO laptops that were too old for encryption have been disposed.

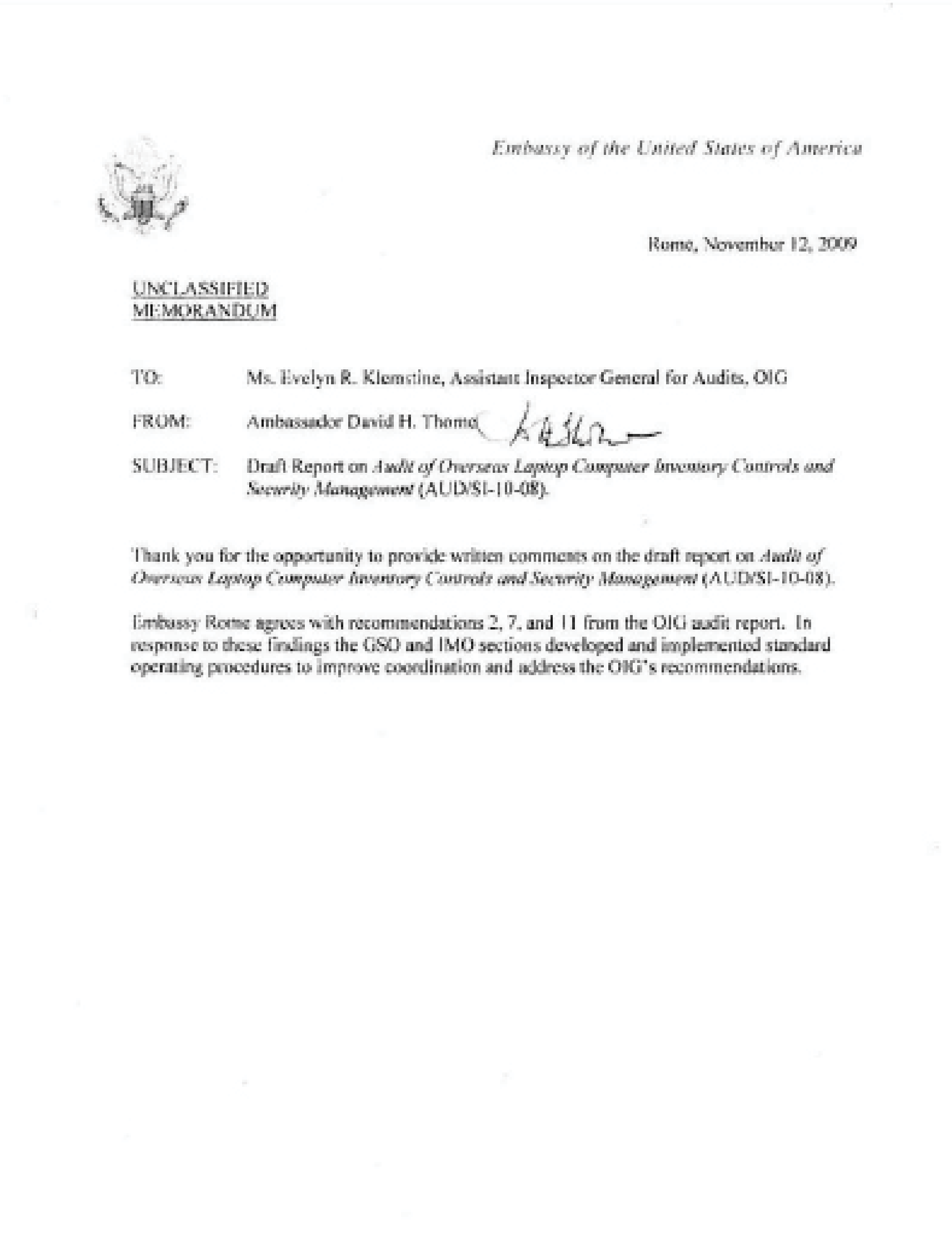
9. Post appreciates the opportunity to participate in this overseas review and correct noted deficiencies.

Signature:	BROWNFIELD
Drafted By:	BOGOTA:Dempsey, Kevin J
Cleared By:	Gillespie, Stephanie A
Approved By:	BOGOTA:Dempsey, Kevin J
Released By:	BOGOTA:Dempsey, Kevin J
Info:	
Attachments:	Metadata.dat
Action Post:	
Dissemination Rule:	Released Copy

UNCLASSIFIED

This email is UNCLASSIFIED.

APPENDIX D



Embassy of the United States of America

Rome, November 12, 2009

UNCLASSIFIED
MEMORANDUM

TO: Ms. Evelyn R. Klemstine, Assistant Inspector General for Audits, OIG

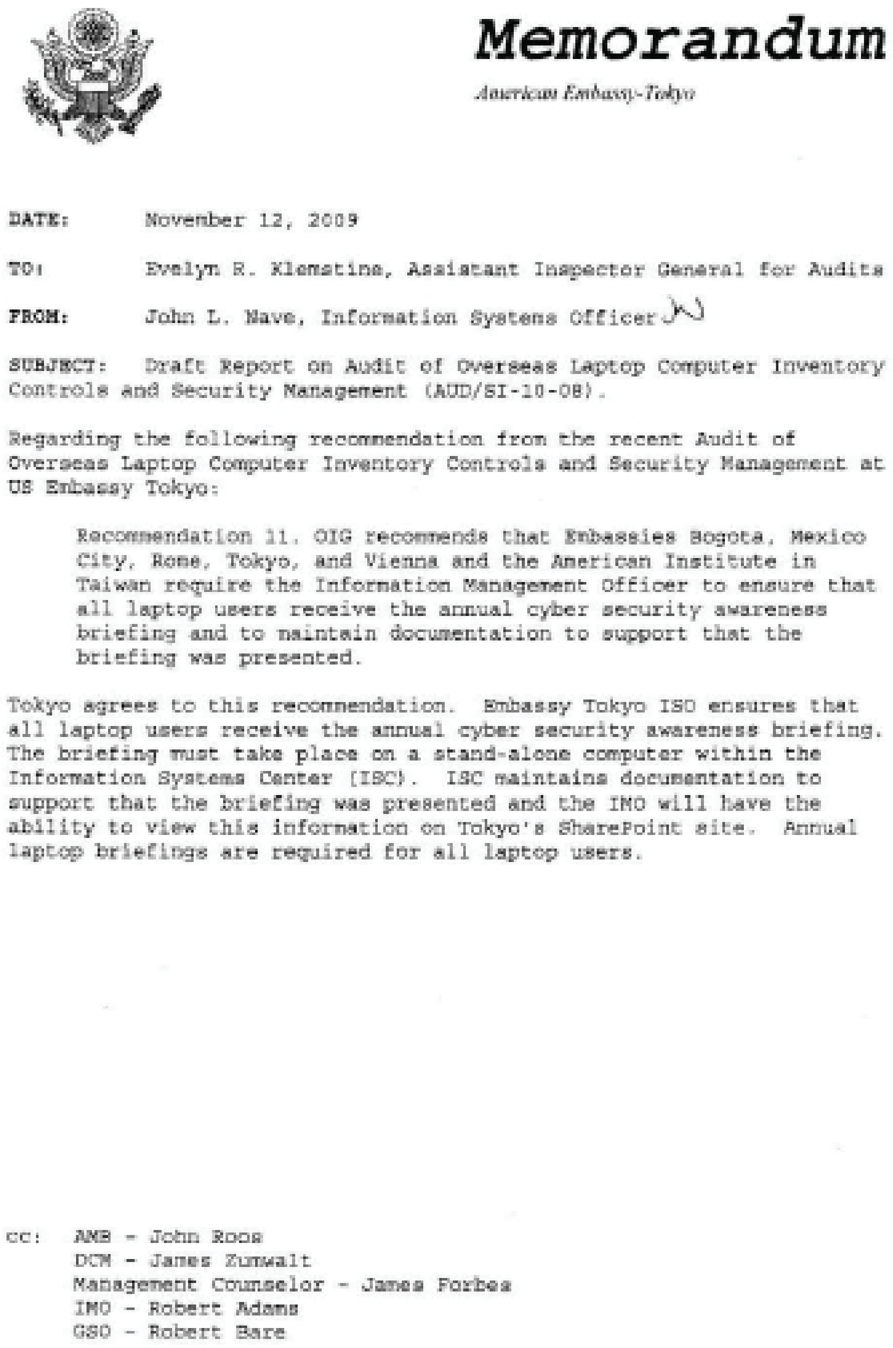
FROM: Ambassador David H. Thorne

SUBJECT: Draft Report on *Audit of Overseas Laptop Computer Inventory Controls and Security Management* (AUD/SI-10-08).

Thank you for the opportunity to provide written comments on the draft report on *Audit of Overseas Laptop Computer Inventory Controls and Security Management* (AUD/SI-10-08).

Embassy Rome agrees with recommendations 2, 7, and 11 from the OIG audit report. In response to these findings the GSO and IMO sections developed and implemented standard operating procedures to improve coordination and address the OIG's recommendations.

APPENDIX E



Memorandum

American Embassy-Tokyo

DATE: November 12, 2009

TO: Evelyn R. Klemstine, Assistant Inspector General for Audits

FROM: John L. Nave, Information Systems Officer

SUBJECT: Draft Report on Audit of Overseas Laptop Computer Inventory Controls and Security Management (AUD/SI-10-08).

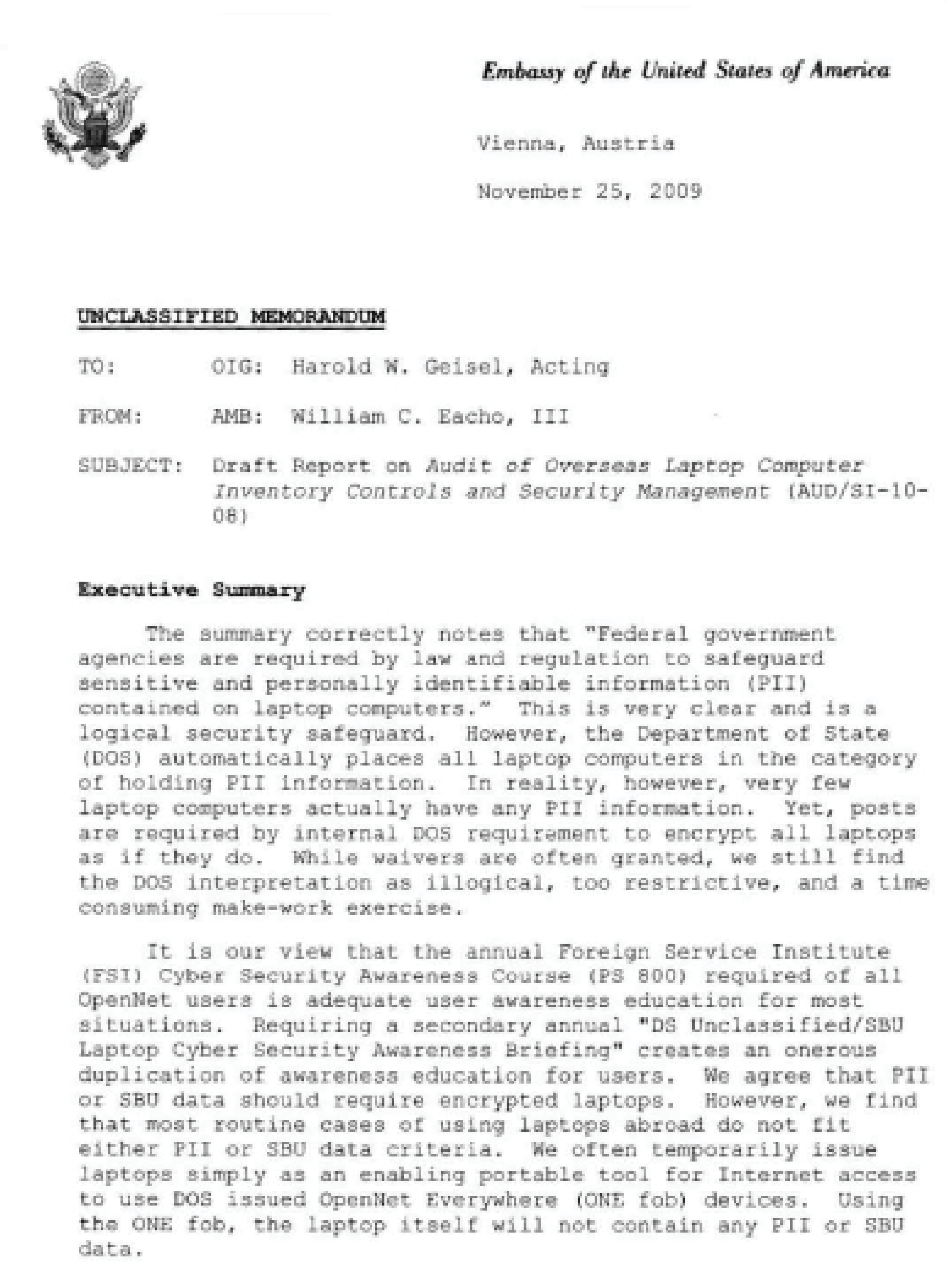
Regarding the following recommendation from the recent Audit of Overseas Laptop Computer Inventory Controls and Security Management at US Embassy Tokyo:

> Recommendation 11. OIG recommends that Embassies Bogota, Mexico City, Rome, Tokyo, and Vienna and the American Institute in Taiwan require the Information Management Officer to ensure that all laptop users receive the annual cyber security awareness briefing and to maintain documentation to support that the briefing was presented.

Tokyo agrees to this recommendation. Embassy Tokyo ISO ensures that all laptop users receive the annual cyber security awareness briefing. The briefing must take place on a stand-alone computer within the Information Systems Center (ISC). ISC maintains documentation to support that the briefing was presented and the IMO will have the ability to view this information on Tokyo's SharePoint site. Annual laptop briefings are required for all laptop users.

cc: AMB - John Roos
DCM - James Zumwalt
Management Counselor - James Forbes
IMO - Robert Adams
GSO - Robert Bare

APPENDIX F



Embassy of the United States of America

Vienna, Austria

November 25, 2009

UNCLASSIFIED MEMORANDUM

TO: OIG: Harold W. Geisel, Acting

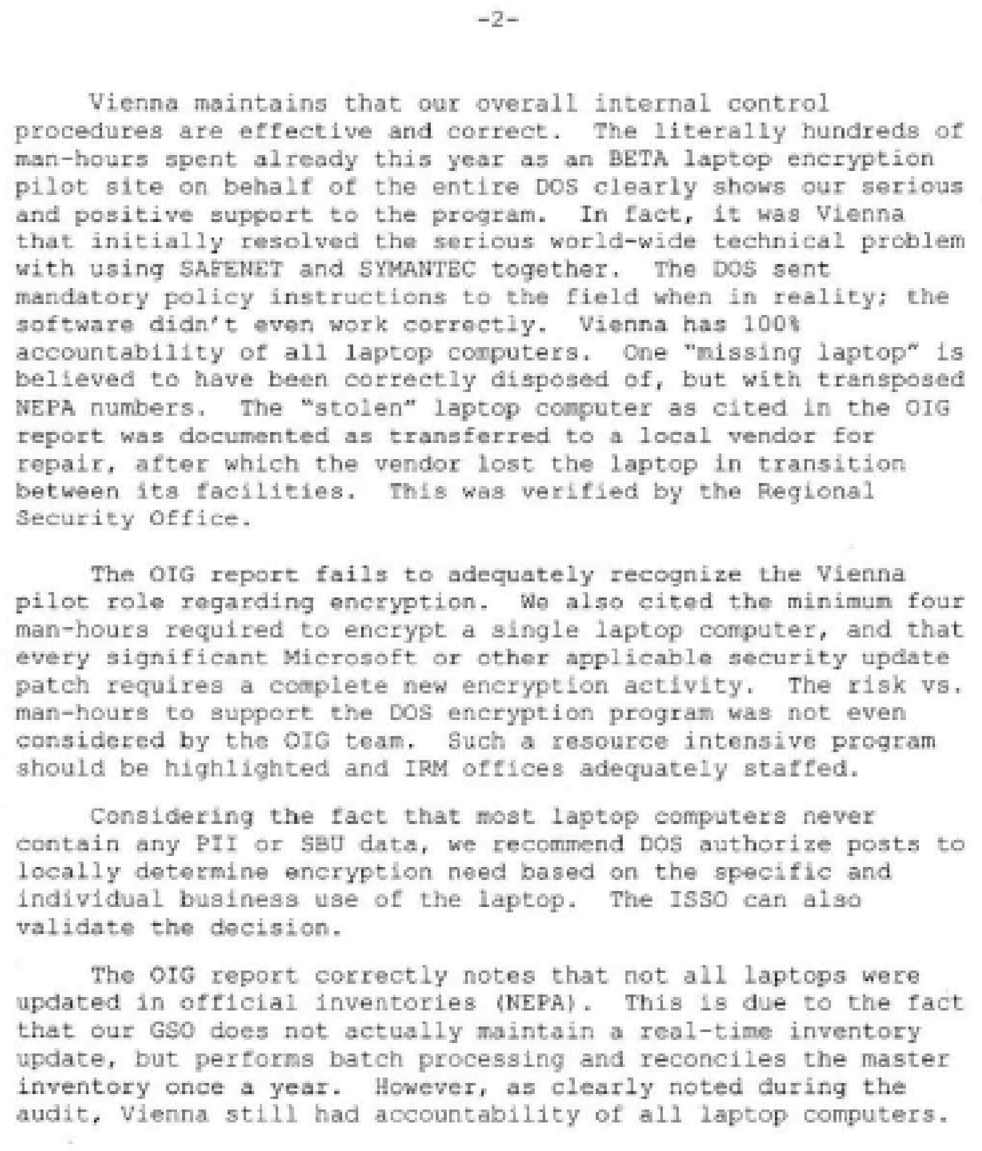
FROM: AMB: William C. Eacho, III

SUBJECT: Draft Report on *Audit of Overseas Laptop Computer Inventory Controls and Security Management* (AUD/SI-10-08)

Executive Summary

The summary correctly notes that "Federal government agencies are required by law and regulation to safeguard sensitive and personally identifiable information (PII) contained on laptop computers." This is very clear and is a logical security safeguard. However, the Department of State (DOS) automatically places all laptop computers in the category of holding PII information. In reality, however, very few laptop computers actually have any PII information. Yet, posts are required by internal DOS requirement to encrypt all laptops as if they do. While waivers are often granted, we still find the DOS interpretation as illogical, too restrictive, and a time consuming make-work exercise.

It is our view that the annual Foreign Service Institute (FSI) Cyber Security Awareness Course (PS 800) required of all OpenNet users is adequate user awareness education for most situations. Requiring a secondary annual "DS Unclassified/SBU Laptop Cyber Security Awareness Briefing" creates an onerous duplication of awareness education for users. We agree that PII or SBU data should require encrypted laptops. However, we find that most routine cases of using laptops abroad do not fit either PII or SBU data criteria. We often temporarily issue laptops simply as an enabling portable tool for Internet access to use DOS issued OpenNet Everywhere (ONE fob) devices. Using the ONE fob, the laptop itself will not contain any PII or SBU data.



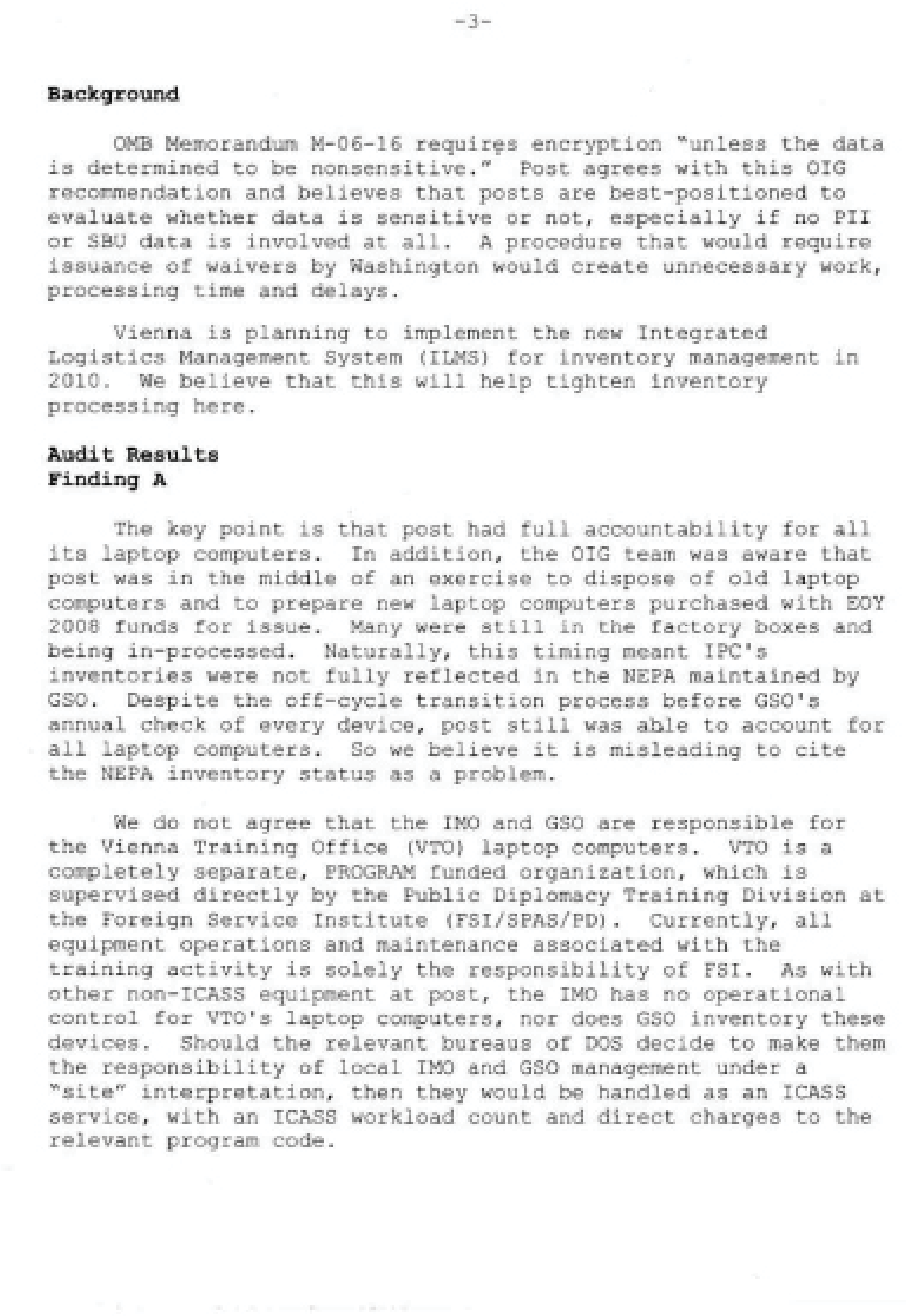
-2-

Vienna maintains that our overall internal control procedures are effective and correct. The literally hundreds of man-hours spent already this year as an BETA laptop encryption pilot site on behalf of the entire DOS clearly shows our serious and positive support to the program. In fact, it was Vienna that initially resolved the serious world-wide technical problem with using SAFENET and SYMANTEC together. The DOS sent mandatory policy instructions to the field when in reality; the software didn't even work correctly. Vienna has 100% accountability of all laptop computers. One "missing laptop" is believed to have been correctly disposed of, but with transposed NEPA numbers. The "stolen" laptop computer as cited in the OIG report was documented as transferred to a local vendor for repair, after which the vendor lost the laptop in transition between its facilities. This was verified by the Regional Security Office.

The OIG report fails to adequately recognize the Vienna pilot role regarding encryption. We also cited the minimum four man-hours required to encrypt a single laptop computer, and that every significant Microsoft or other applicable security update patch requires a complete new encryption activity. The risk vs. man-hours to support the DOS encryption program was not even considered by the OIG team. Such a resource intensive program should be highlighted and IRM offices adequately staffed.

Considering the fact that most laptop computers never contain any PII or SBU data, we recommend DOS authorize posts to locally determine encryption need based on the specific and individual business use of the laptop. The ISSO can also validate the decision.

The OIG report correctly notes that not all laptops were updated in official inventories (NEPA). This is due to the fact that our GSO does not actually maintain a real-time inventory update, but performs batch processing and reconciles the master inventory once a year. However, as clearly noted during the audit, Vienna still had accountability of all laptop computers.



Background

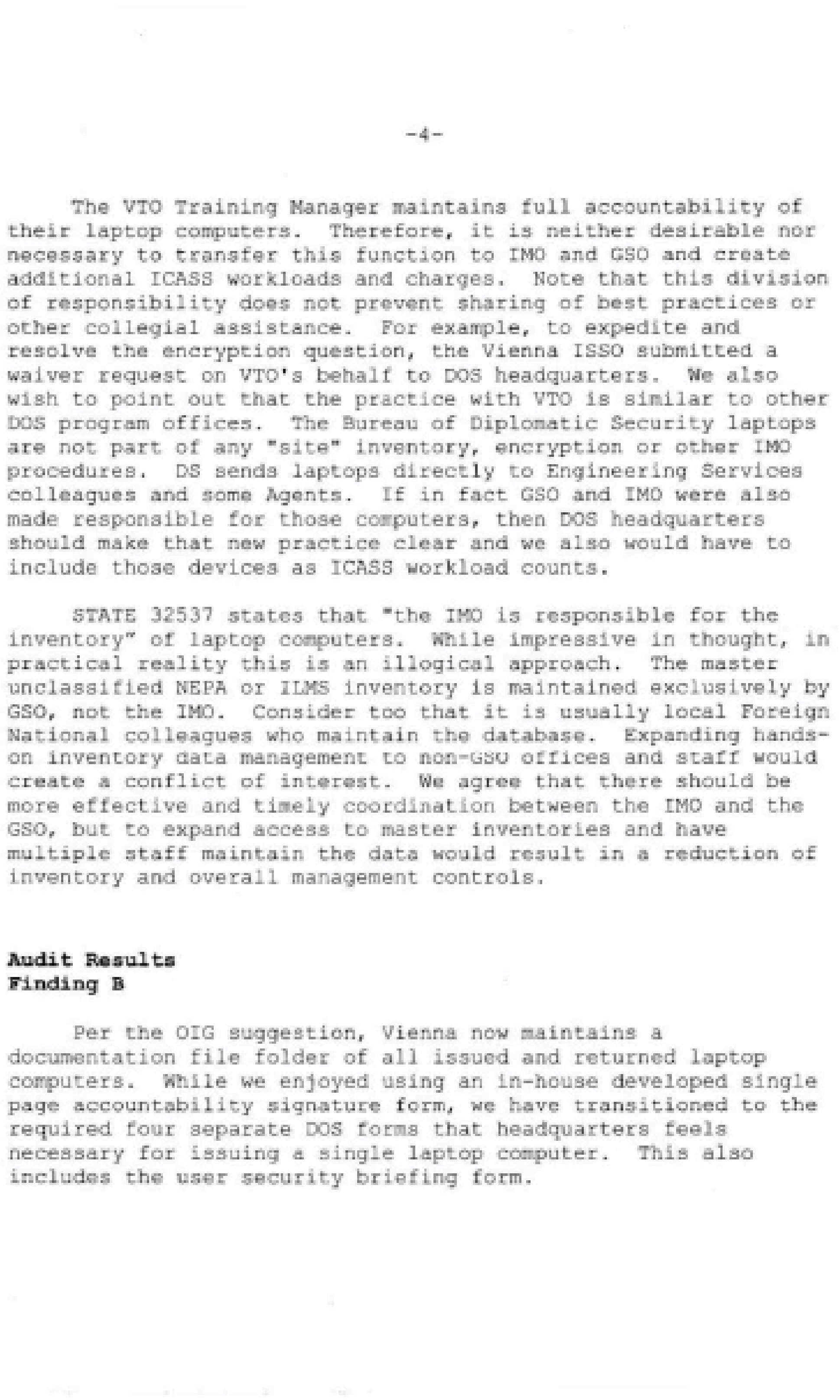
OMB Memorandum M-06-16 requires encryption "unless the data is determined to be nonsensitive." Post agrees with this OIG recommendation and believes that posts are best-positioned to evaluate whether data is sensitive or not, especially if no PII or SBU data is involved at all. A procedure that would require issuance of waivers by Washington would create unnecessary work, processing time and delays.

Vienna is planning to implement the new Integrated Logistics Management System (ILMS) for inventory management in 2010. We believe that this will help tighten inventory processing here.

Audit Results
Finding A

The key point is that post had full accountability for all its laptop computers. In addition, the OIG team was aware that post was in the middle of an exercise to dispose of old laptop computers and to prepare new laptop computers purchased with EOY 2008 funds for issue. Many were still in the factory boxes and being in-processed. Naturally, this timing meant IPC's inventories were not fully reflected in the NEPA maintained by GSO. Despite the off-cycle transition process before GSO's annual check of every device, post still was able to account for all laptop computers. So we believe it is misleading to cite the NEPA inventory status as a problem.

We do not agree that the IMO and GSO are responsible for the Vienna Training Office (VTO) laptop computers. VTO is a completely separate, PROGRAM funded organization, which is supervised directly by the Public Diplomacy Training Division at the Foreign Service Institute (FSI/SPAS/PD). Currently, all equipment operations and maintenance associated with the training activity is solely the responsibility of FSI. As with other non-ICASS equipment at post, the IMO has no operational control for VTO's laptop computers, nor does GSO inventory these devices. Should the relevant bureaus of DOS decide to make them the responsibility of local IMO and GSO management under a "site" interpretation, then they would be handled as an ICASS service, with an ICASS workload count and direct charges to the relevant program code.



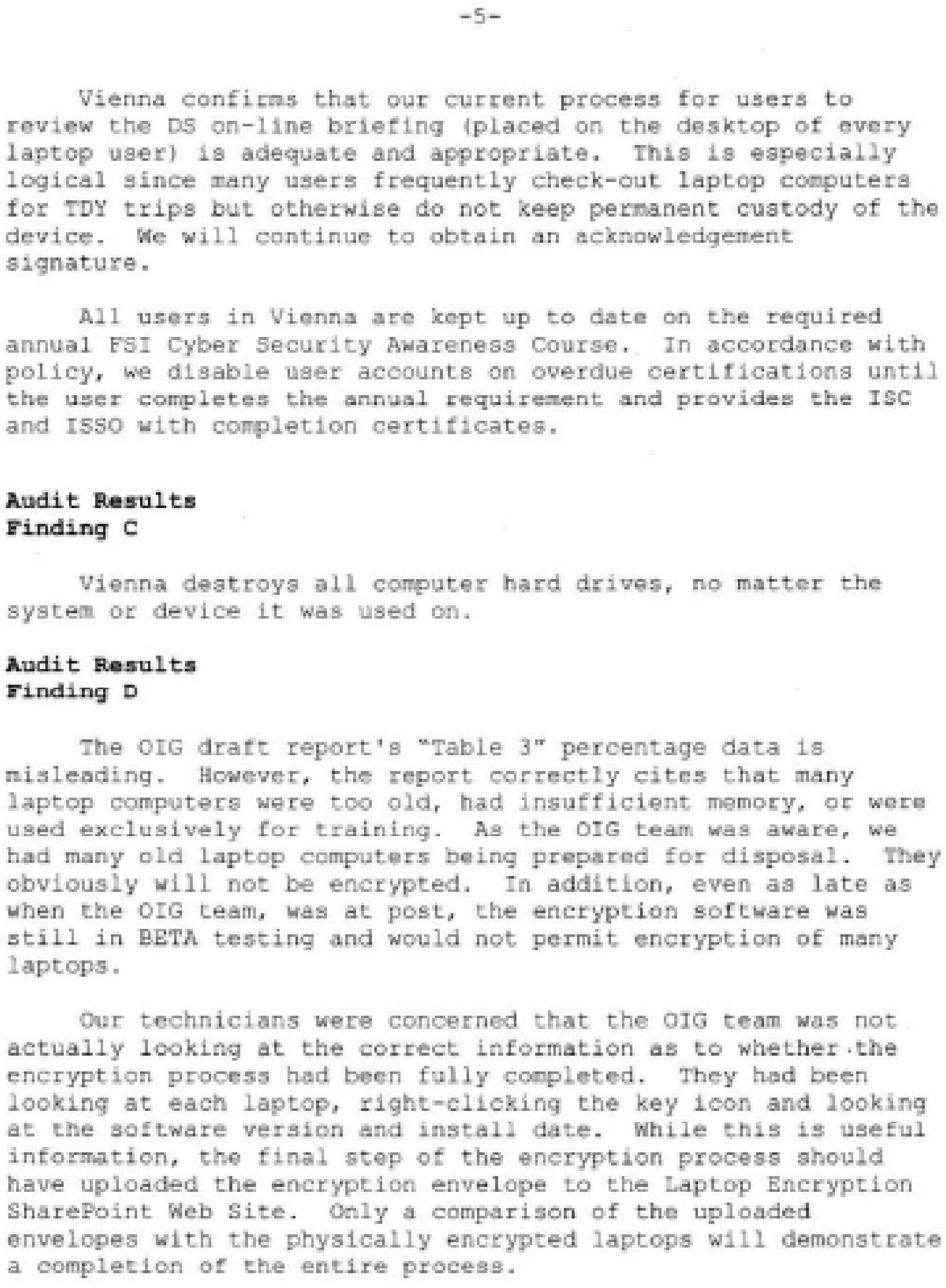
-4-

The VTO Training Manager maintains full accountability of their laptop computers. Therefore, it is neither desirable nor necessary to transfer this function to IMO and GSO and create additional ICASS workloads and charges. Note that this division of responsibility does not prevent sharing of best practices or other collegial assistance. For example, to expedite and resolve the encryption question, the Vienna ISSO submitted a waiver request on VTO's behalf to DOS headquarters. We also wish to point out that the practice with VTO is similar to other DOS program offices. The Bureau of Diplomatic Security laptops are not part of any "site" inventory, encryption or other IMO procedures. DS sends laptops directly to Engineering Services colleagues and some Agents. If in fact GSO and IMO were also made responsible for those computers, then DOS headquarters should make that new practice clear and we also would have to include those devices as ICASS workload counts.

STATE 32537 states that "the IMO is responsible for the inventory" of laptop computers. While impressive in thought, in practical reality this is an illogical approach. The master unclassified NEPA or ILMS inventory is maintained exclusively by GSO, not the IMO. Consider too that it is usually local Foreign National colleagues who maintain the database. Expanding hands-on inventory data management to non-GSO offices and staff would create a conflict of interest. We agree that there should be more effective and timely coordination between the IMO and the GSO, but to expand access to master inventories and have multiple staff maintain the data would result in a reduction of inventory and overall management controls.

Audit Results
Finding B

Per the OIG suggestion, Vienna now maintains a documentation file folder of all issued and returned laptop computers. While we enjoyed using an in-house developed single page accountability signature form, we have transitioned to the required four separate DOS forms that headquarters feels necessary for issuing a single laptop computer. This also includes the user security briefing form.



-5-

Vienna confirms that our current process for users to review the DS on-line briefing (placed on the desktop of every laptop user) is adequate and appropriate. This is especially logical since many users frequently check-out laptop computers for TDY trips but otherwise do not keep permanent custody of the device. We will continue to obtain an acknowledgement signature.

All users in Vienna are kept up to date on the required annual FSI Cyber Security Awareness Course. In accordance with policy, we disable user accounts on overdue certifications until the user completes the annual requirement and provides the ISC and ISSO with completion certificates.

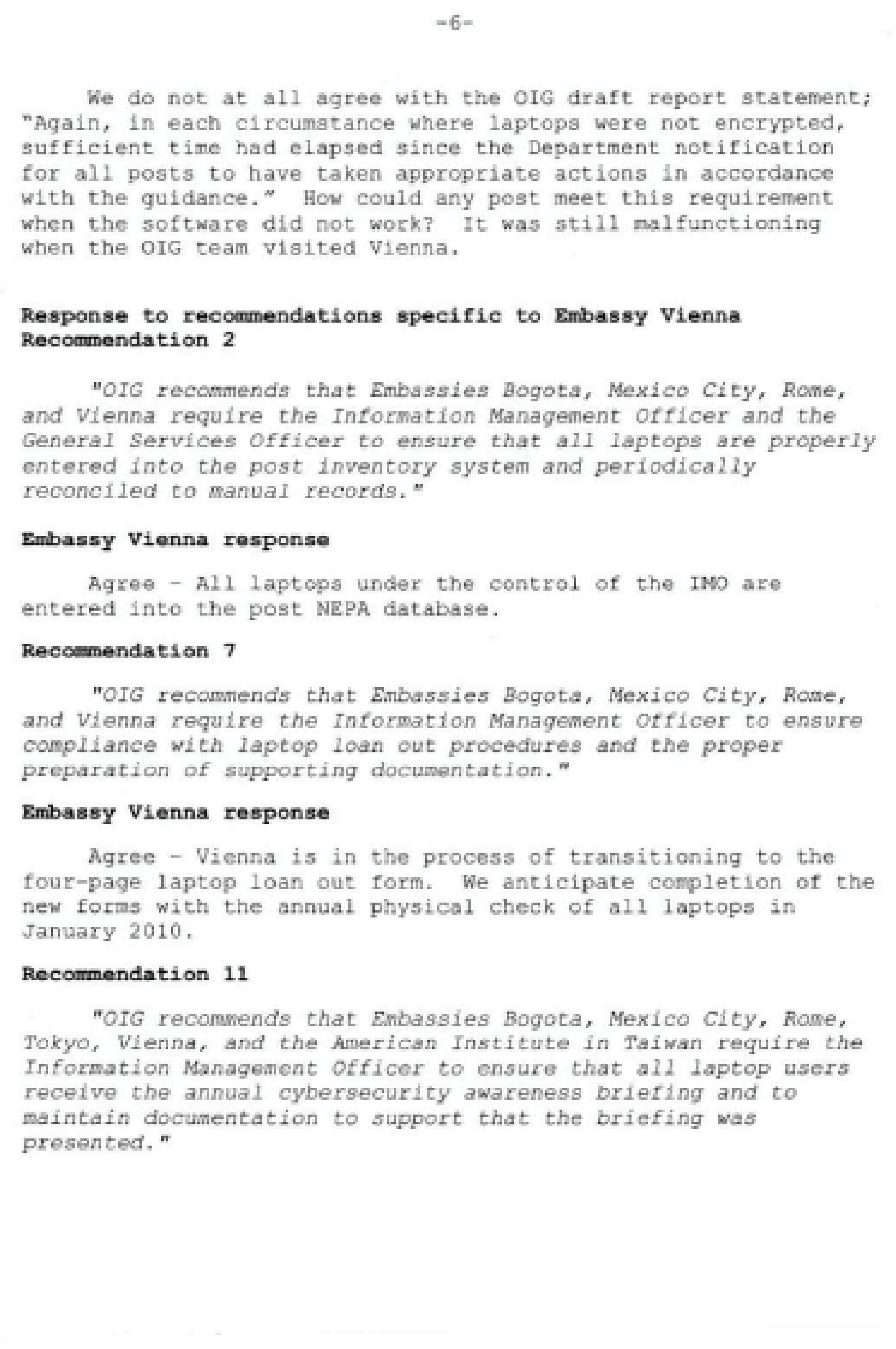
Audit Results
Finding C

Vienna destroys all computer hard drives, no matter the system or device it was used on.

Audit Results
Finding D

The OIG draft report's "Table 3" percentage data is misleading. However, the report correctly cites that many laptop computers were too old, had insufficient memory, or were used exclusively for training. As the OIG team was aware, we had many old laptop computers being prepared for disposal. They obviously will not be encrypted. In addition, even as late as when the OIG team, was at post, the encryption software was still in BETA testing and would not permit encryption of many laptops.

Our technicians were concerned that the OIG team was not actually looking at the correct information as to whether the encryption process had been fully completed. They had been looking at each laptop, right-clicking the key icon and looking at the software version and install date. While this is useful information, the final step of the encryption process should have uploaded the encryption envelope to the Laptop Encryption SharePoint Web Site. Only a comparison of the uploaded envelopes with the physically encrypted laptops will demonstrate a completion of the entire process.



-6-

We do not at all agree with the OIG draft report statement; "Again, in each circumstance where laptops were not encrypted, sufficient time had elapsed since the Department notification for all posts to have taken appropriate actions in accordance with the guidance." How could any post meet this requirement when the software did not work? It was still malfunctioning when the OIG team visited Vienna.

Response to recommendations specific to Embassy Vienna
Recommendation 2

"OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer and the General Services Officer to ensure that all laptops are properly entered into the post inventory system and periodically reconciled to manual records."

Embassy Vienna response

Agree – All laptops under the control of the IMO are entered into the post NEPA database.

Recommendation 7

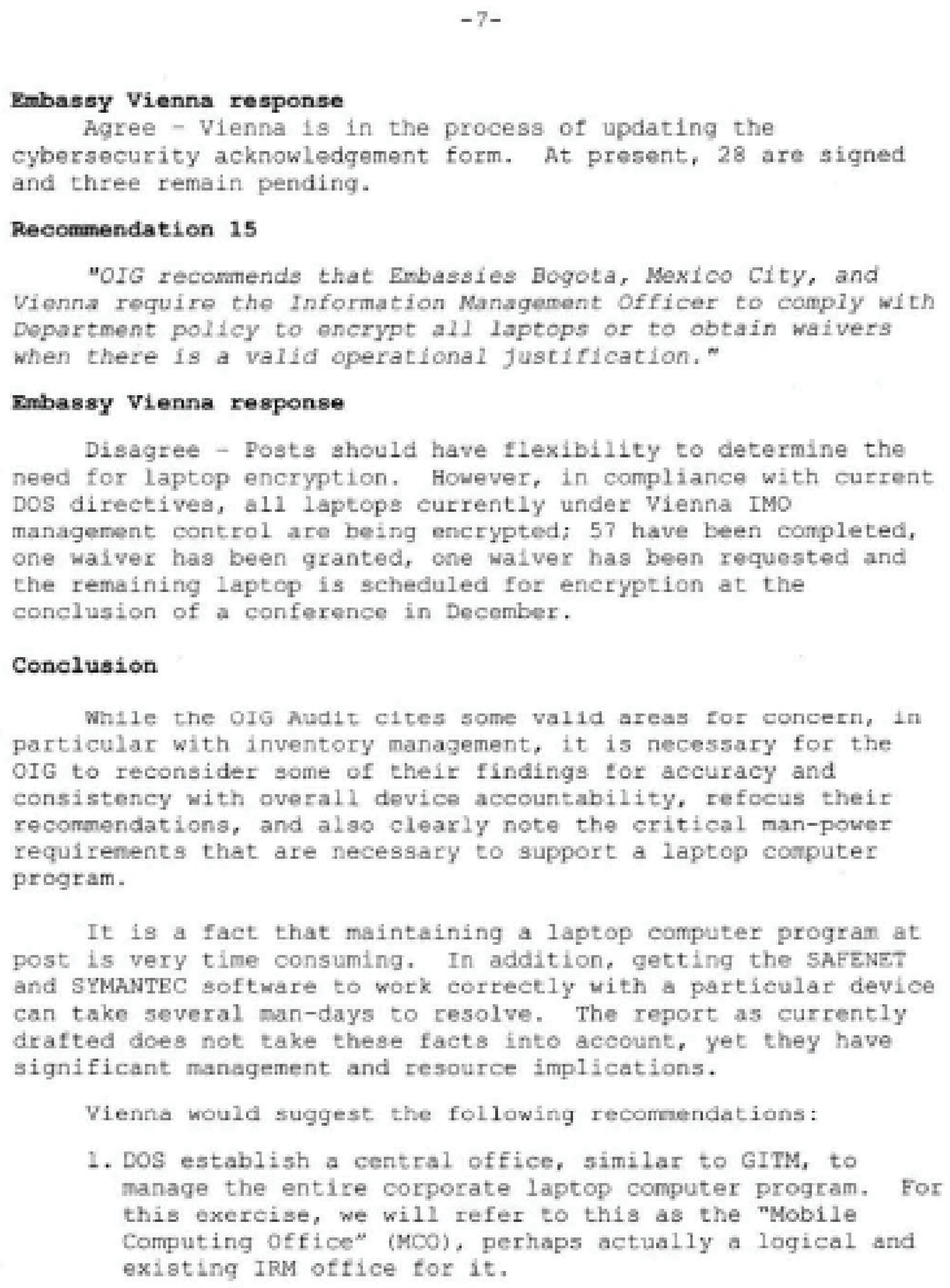
"OIG recommends that Embassies Bogota, Mexico City, Rome, and Vienna require the Information Management Officer to ensure compliance with laptop loan out procedures and the proper preparation of supporting documentation."

Embassy Vienna response

Agree – Vienna is in the process of transitioning to the four-page laptop loan out form. We anticipate completion of the new forms with the annual physical check of all laptops in January 2010.

Recommendation 11

"OIG recommends that Embassies Bogota, Mexico City, Rome, Tokyo, Vienna, and the American Institute in Taiwan require the Information Management Officer to ensure that all laptop users receive the annual cybersecurity awareness briefing and to maintain documentation to support that the briefing was presented."



-7-

Embassy Vienna response

Agree - Vienna is in the process of updating the cybersecurity acknowledgement form. At present, 28 are signed and three remain pending.

Recommendation 15

"OIG recommends that Embassies Bogota, Mexico City, and Vienna require the Information Management Officer to comply with Department policy to encrypt all laptops or to obtain waivers when there is a valid operational justification."

Embassy Vienna response

Disagree - Posts should have flexibility to determine the need for laptop encryption. However, in compliance with current DOS directives, all laptops currently under Vienna IMO management control are being encrypted; 57 have been completed, one waiver has been granted, one waiver has been requested and the remaining laptop is scheduled for encryption at the conclusion of a conference in December.

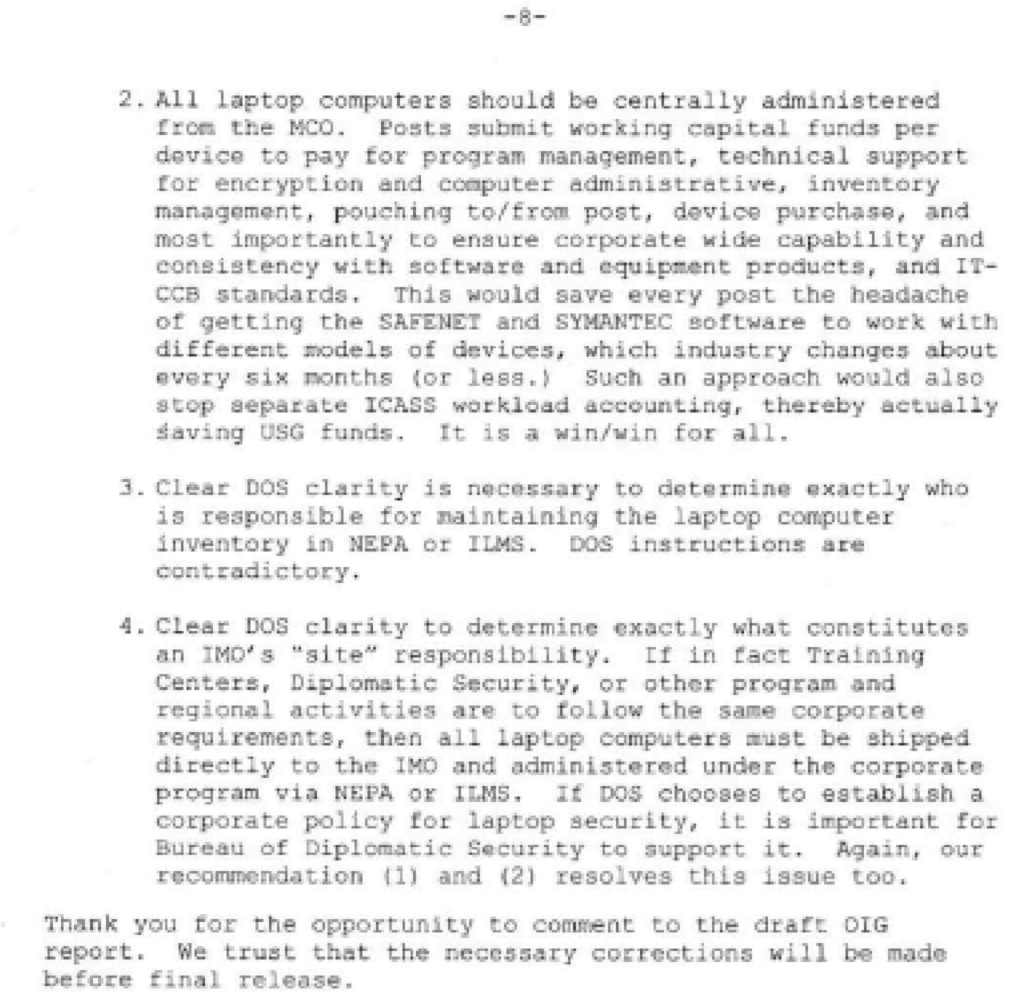
Conclusion

While the OIG Audit cites some valid areas for concern, in particular with inventory management, it is necessary for the OIG to reconsider some of their findings for accuracy and consistency with overall device accountability, refocus their recommendations, and also clearly note the critical man-power requirements that are necessary to support a laptop computer program.

It is a fact that maintaining a laptop computer program at post is very time consuming. In addition, getting the SAFENET and SYMANTEC software to work correctly with a particular device can take several man-days to resolve. The report as currently drafted does not take these facts into account, yet they have significant management and resource implications.

Vienna would suggest the following recommendations:

1. DOS establish a central office, similar to GITM, to manage the entire corporate laptop computer program. For this exercise, we will refer to this as the "Mobile Computing Office" (MCO), perhaps actually a logical and existing IRM office for it.



2. All laptop computers should be centrally administered from the MCO. Posts submit working capital funds per device to pay for program management, technical support for encryption and computer administrative, inventory management, pouching to/from post, device purchase, and most importantly to ensure corporate wide capability and consistency with software and equipment products, and IT-CCB standards. This would save every post the headache of getting the SAFENET and SYMANTEC software to work with different models of devices, which industry changes about every six months (or less.) Such an approach would also stop separate ICASS workload accounting, thereby actually saving USG funds. It is a win/win for all.

3. Clear DOS clarity is necessary to determine exactly who is responsible for maintaining the laptop computer inventory in NEPA or ILMS. DOS instructions are contradictory.

4. Clear DOS clarity to determine exactly what constitutes an IMO's "site" responsibility. If in fact Training Centers, Diplomatic Security, or other program and regional activities are to follow the same corporate requirements, then all laptop computers must be shipped directly to the IMO and administered under the corporate program via NEPA or ILMS. If DOS chooses to establish a corporate policy for laptop security, it is important for Bureau of Diplomatic Security to support it. Again, our recommendation (1) and (2) resolves this issue too.

Thank you for the opportunity to comment to the draft OIG report. We trust that the necessary corrections will be made before final release.

ABBREVIATIONS

A Bureau	Bureau of Administration
AIT Taipei	American Institute in Taiwan
ALDAC	All Diplomatic and Consular Posts
APO	Accountable Property Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DS	Bureau of Diplomatic Security
FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
GAO	Government Accountability Office
GSO	General Services Office/Officer
ILMS	Integrated Logistics Management System
IMO	Information Management Officer
IRM	Bureau of Information Resource Management
IRM/IA	Office of Information Assurance
IRM/OS	Operations Support Branch
NAS	Narcotics Affairs Section
NEPA	Non-Expendable Property Application
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PMO	Property Management Officer
RSO	Regional Security Office
SBU	sensitive but unclassified
VTO	Vienna Training Office

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202-647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our Web site at:
http://oig.state.gov

Cables to the Inspector General
should be slugged “OIG Channel”
to ensure confidentiality.