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

Office of Audits

Audit of Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, DC, Metropolitan Area

Report Number AUD/SI-09-15, July 2009

~~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
Acting Inspector General

TABLE OF CONTENTS

Section **Page**

EXECUTIVE SUMMARY

Since 2006, the Office of Management and Budget (OMB) has issued several policy directives to require and remind departments and agencies to protect sensitive agency information and personally identifiable information (PII). These requirements include safeguarding information on mobile computers/devices to include encrypting[1] all data on laptop computers unless the data is determined to be non-sensitive. During 2007 and 2008, the Secretary of State and the Chief Information Officer (CIO) issued several notices and guidance to Department of State (Department) officials to implement the OMB directives, including the responsibility for protecting information on the Department's laptop computers. Because of the attention to and importance of these requirements, the Office of Inspector General (OIG) initiated this audit to review, on a sample basis, the Department's implementation of these mandates related to property accountability and inventory controls over Department-owned laptop computers, encryption, and security awareness training. This audit was conducted on the inventory of laptop computers located in four bureaus in the Washington, DC, metropolitan area.

The Department does not have an accurate accounting for and has not encrypted all of its classified and unclassified laptop computers in the Washington, DC, area for the four bureaus included in OIG's audit. Three of the four bureaus were not able to fully account for each of the laptop computers in the sample. The Department's Integrated Logistics Management System (ILMS), which is maintained by the Bureau of Administration (A Bureau), is the official inventory of record and is used to manage the inventory of classified, sensitive but unclassified (SBU), and unclassified laptop computers from acquisition through disposal. Contrary to the Department's official inventory records, OIG was unable to inspect 119 laptop computers in its sample size of 334[2] because they were missing (27); were not physically located in the Washington, DC, area or were otherwise unable to be physically inspected (35); or had been disposed of (57). Of the 215 that were physically inspected, 172 were not encrypted and 43 were encrypted.

[1] Encryption is a subset of cryptography, which is used to secure transactions by providing ways to ensure data confidentiality (assurance that the information will be protected from unauthorized access), data integrity (assurance that data have not been accidentally or deliberately altered), authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party). [Source: Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains (GAO-08-525, June 2008)].

[2] OIG randomly selected 341 laptop computers; however, OIG's work disclosed that seven items were incorrectly coded and were not laptop computers.

Regarding the 27 missing laptop computers, Department officials could not determine the disposition of 23 of them. Officials said that three of the remaining four laptop computers were returned to the vendor and that one was destroyed in a fire, but they could not provide proper asset tracking documentation to support these events. As a result, OIG could not verify the locations of those four items, and none had been properly removed from the official inventory system. After several attempts by OIG, Department officials provided proper documentation to change the classification for only one of the 27 laptop computers to "missing" by the end of its verification. Officials prepared documentation for 18 of the 27 missing laptops after OIG had completed its verification. The estimated cost of the missing laptop computers is about $55,000. More importantly, Department officials could not provide to OIG documentation to support their assertions that the hard drives of the missing laptop computers did not contain PII or classified information. Because the content and the encryption status of the missing laptop computers are unknown, there is a risk that PII and other sensitive Department information may be susceptible to unauthorized access and use.

Included in the sample of 334 were 14 classified laptop computers labeled "Secret," all of which were located and physically inspected. However, OIG's verification found that there was no encryption software installed on nine of these classified laptop computers. Although the Department had issued a series of mandates regarding responsibilities for protecting unclassified and SBU laptop computers, including encryption requirements, it had not done so for the more security-sensitive classified laptop computers.

OIG also determined that there was no requirement to identify computers designated as "classified" in ILMS. Furthermore, the Department did not have, through any other means, a centralized inventory of classified laptop computers in the Washington, DC, area. Officials with the Bureau of Intelligence and Research (INR) stated that INR's inventory of classified computers is not maintained in ILMS because INR is "uncomfortable identifying classified equipment in an unclassified inventory system resident on an open network." However, each bureau included in OIG's sample group provided an internal count for its inventory of classified laptop computers in response to a data call OIG sent to identify classified laptop computers. Because ILMS is not capturing identifiers for classified laptop computers, it is not a viable resource, thereby making inventory accountability and visibility over this security-sensitive equipment fractured.

To determine a sample of laptop computers to review, OIG selected the three bureaus with the largest number of laptop computers located domestically—the Bureau of Diplomatic Security (DS), the Bureau of Information Resource Management

(IRM), and the Bureau of Overseas Buildings Operations (OBO). OIG also selected INR because it processes intelligence information and had previously reported one classified laptop computer as lost in 2000. The disposition of the 334 laptops is summarized in Table 1. (Table 1 is also presented in the Audit Results section in this report.)

Table 1. Results of Testing for Inventory and Encryption of 334 Laptop Computers Included in Sample Group

LAPTOP COMPUTERS IN SAMPLE GROUP									
Bureau	Number and Type of Laptops			Results of Inventory and Encryption Testing					
	Unclassified and SBU	Classified	Total Sample Group	Missing	Encrypted	Not Encrypted	Located but Unable to Test for Encryption	Disposed	Total Sample Group
DS	97	0	97	6	13	45	7	26	97
INR	31	8	39	0	0	39	0	0	39
IRM	95	3	98	18	14	26	19	21	98
OBO	97	3	100	3	16	62	9	10	100
Total	320	14	334	27	43	172	35	57	334
% of Total	96%	4%	100%	8.0%	13.0%	52%	10%	17.0%	100%

Note: Percentages adjusted for rounding.

As the table shows, 57 laptop computers had been disposed of. The laptops were either transferred to excess property (51) or had been donated to schools (6). However, similar to the missing laptop computers, ILMS had not been updated to remove these disposed items from the current inventory prior to OIG's selection of its sample group. Until inventory events are properly reflected in ILMS, the information contained in this inventory system will continue to be inaccurate.

According to documentation provided to OIG, DS has conducted biweekly Unclassified/SBU Laptop Cyber Security Awareness Briefings since July 2007 to address laptop computer security responsibilities for users, including reporting a missing, lost, or stolen laptop. These briefings cover the requirements for protecting Department-owned laptop computers and the data stored on them. However, the Department did not have a centralized tracking system to record those individuals who had taken the briefings. Officials in each of the four bureaus included in this audit said that the respective bureaus maintained their own training participation records. However, OIG reviewed those records and found them to be incomplete. OIG noted this same decentralized condition in a separate 2008 review of the Department's overall security awareness training program as it related to the Federal Information Security Management Act.[3] Without centralized tracking for all forms of information security training, including for laptop computer users, the Department cannot ensure that all personnel are receiving required training, thus obtaining a comprehensive awareness of individual security responsibilities.

Given the government-wide importance and attention placed on protecting PII and sensitive agency information, more aggressive and consistent action is needed by the A Bureau's Office of Logistics Management (A/LM) to improve the functionality of ILMS and by DS, INR, IRM, and OBO to enforce the various internal and federal requirements relating to laptop computer inventory and encryption responsibilities. Furthermore, bureau officials should continue to make all attempts to locate the missing laptop computers identified by OIG and to determine the type of information that may potentially be contained on each. If a potential or actual incident is suspected (such as loss, theft, or tampering), responsible officials should ensure that the required notices are made to OIG, designated Department officials, and external entities of potential risk as warranted, such as to DS' Computer Incident Response Team (CIRT) or the United States Computer Emergency Readiness Team (US-CERT), of which the latter is a partnership between the Department of Homeland Security and the public and private sectors.

Management Comments and OIG Response

OIG met with Department officials throughout the audit to discuss its findings. During these meetings, the officials generally agreed with the audit results. A draft of this report was provided to officials of each of the four bureaus included in this audit and the A Bureau, which maintains ILMS. All the bureaus responded to the draft report and, in some cases, described actions taken or underway to address the recommendations. OIG has addressed the responsiveness of those actions.

Of the three bureaus with missing laptop computers, OBO responded that it had conducted a search of its three missing laptop computers, identified the last known disposition for two of them, and is verifying the suspected location of the third. All three are still missing or lost. However, OBO has described actions it is taking to strengthen its laptop computer accountability and is conducting a scheduled "recall" of all of its laptop computers for replacement, update, and/or service. Neither DS nor IRM responded to the recommendations (Nos. 1 and 3, respectively) that each should attempt to locate its missing laptop computers.

[3] Review of the Information Security Program at the Department of State (AUD/IT-08-36, Oct. 2008).

All comments received from the bureaus have been considered and incorporated into the final report as appropriate. The bureaus' comments are summarized after each recommendation, and their responses are presented in the appendices. (Attachments consisting of many pages that were included with bureau responses were not included in the appendices, but they are referred to in the summarizations.) Responses from DS, IRM, the A Bureau, INR, and OBO are in Appendices C-G, respectively.

BACKGROUND

Between 2006 and 2007, the Office of Management and Budget (OMB) issued several policy directives to require and remind departments and agencies to protect sensitive agency information and personally identifiable information (PII). These requirements address safeguarding information on mobile computers/devices to include encrypting all data on laptop computers unless the data is determined to be nonsensitive. Specific actions are to be taken for the protection of PII that is "accessed remotely; or physically transported outside of the agency's secured, physical perimeter." Further, in 2007, OMB required agencies to develop and implement a breach notification policy to respond to the breach of PII. These OMB directives include the following:

- M-06-15, "Safeguarding Personally Identifiable Information" (May 22, 2006)
- M-06-16, "Protection of Sensitive Agency Information" (June 23, 2006)
- M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments" (July 12, 2006)
- M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007)

During 2007 and 2008, the Secretary of State issued several notices and guidance to Department of State officials to implement the OMB directives, including the responsibility for protecting information on the Department's laptop computers. The Chief Information Officer (CIO) also issued notices and guidance on this subject to Bureau of Information Resource Management (IRM) personnel. The internal mandates emphasize control of the laptop inventory, encryption of the hard drive of all laptop computers, and laptop user awareness training. These Department notices and guidance are described in Appendix A.

The Bureau of Administration's (A Bureau) Office of Logistics Management (A/LM) is responsible for the Integrated Logistics Management System (ILMS), which provides functionality for an end-to-end supply chain, including procurement, property management, and physical inventory. ILMS is the Department's official nonexpendable property inventory of record for the Washington, DC, area and domestic field offices, and it is being implemented at overseas posts.[4] ILMS is used to manage the inventory of both classified and unclassified laptop computers from acquisition through disposal. ILMS contains detailed laptop inventory data, such as the serial number, model, location, staff assignment, and acquisition cost. ILMS uses two purchase modules, Ariba and Momentum, in which property is acquired through purchase card transactions and blanket purchase agreements, respectively. The Asset Management module of ILMS is used to track the property inventory for each bureau and major office of the Department. For reconciliation with and updates to ILMS, property custodians are required to conduct annual physical inventories of property and to record new acquisitions, disposals, and losses of property, including laptop computers, when they occur.

Property Management Requirements

The Department has identified key responsibilities relating to the management of accountable property, including laptop computers, in its Foreign Affairs Manual (FAM) as follows:

- 14 FAM 420, "Domestic Personal Property Management," requires that compliance with property management regulations be monitored by property management reports, Property Management Branch staff visits, as well as Office of Inspector General (OIG) visits. The Agency Property Management Officer is responsible for managing ILMS and must be notified of any noncompliance with the property regulations and will notify the appropriate Accountable Property Officer (APO).

- 14 FAM 422, "Definitions," defines accountable property as personal property that must be tracked on property records. This includes nonexpendable personal property with an acquisition cost of $5,000 or more per item. It also includes serialized property, including information technology equipment, with an acquisition cost of $500 or more per item, and property of any value that is sensitive by nature and attractive for personal use as identified by the APO, such as laptop computers, cellular telephones, personal digital assistants, cameras, and lenses. Nonexpendable property is property such as furniture, office equipment, and information technology equipment, which is complete in itself, does not lose its identity or becomes a component part of another system when used, and is of durable nature with an anticipated useful life of over 2 years. (Note: 14 FAM 425, "Control of Nonexpendable Property," also provides the same definition for nonexpendable personal property.)

[4] As of August 2008, the Department had fully deployed ILMS to 14 of 277 overseas posts to replace the Nonexpendable Property Application and various post-developed property inventory systems.

- 14 FAM 423, "Responsibilities," defines the following positions:

    - o The Managing Director of Program Management and Policy, A/LM, is the designated Property Management Officer for the Department and is responsible for establishing policy for management and control of the Department's personal property; reviewing property management program operations; developing and implementing property management regulations and procedures; and providing guidance in areas of receipt, storage property accountability, inventory management, property utilization, and disposal.

    - o The APO accounts for property and ensures that all transactions affecting personal property on hand, received, and disposed of within the APO's accountable area are properly documented. The APO must also ensure that property management responsibilities are included in the job and work requirements of those employees having property duties. Finally, the APO must ensure that Principal Custodial Officer (PCO) and Area Custodial Officer (ACO) responsibilities have been established in writing at the local level and that written procedures are in place.

    - o The ACO has responsibility for the care and proper utilization of property assigned to a specific custodial area. However, the PCO has supervisory responsibility for property located in several custodial areas, directs and coordinates the duties of the ACOs, and maintains the accountable property records.

- 14 FAM 426.1, "Physical Inventory and Reconciliation," requires that physical inventories of accountable personal property be taken annually and the results immediately reconciled with the property records. Upon completion of the reconciliation and appropriate approval of any records adjustment resulting from inventory discrepancies, the PCO must prepare Part A of Form DS-1875, Certification of Inventory Reconciliation. When discrepancies are found between the physical inventory count and the property records, immediate action must be taken to resolve the discrepancies. Inventory overages must be documented to the property records. Inventory overages do not offset inventory shortages.

- 14 FAM 427.1(a)(b)(c)(d)(f),"Nonexpendable Property," requires the ACO to report unneeded property to the PCO, including any property not reassigned for further use. Such property is to be reported on the ILMS Asset Management application as "excess." The office must use the appropriate forms, including the ILMS Asset Management Excess Property Report and DS-586, Turn-In Property Inspection Certification (if needed), and the office must then place a U.S. Department of Agriculture (USDA) Centralized Excess Property Operations (CEPO) number on Form DS 586 or DS-1882, Domestic Property Excess, as described in the Foreign Affairs Handbook (FAH), 14-FAH-1 H-721, "Reporting to the Principal Custodial Officer." The Property Management staff forwards the ILMS Asset Management Excess Property Report to USDA's CEPO to request pickup of the property.

- 14 FAM 427.1(h), "Nonexpendable Property," states, "Unclassified computer hardware, declared as excess property that can no longer be used within the Department should be donated to schools or educational nonprofit organizations, especially in Federal empowerment zones and enterprise communities, in accordance with the Computer for Learning Program, Executive Order 12999." The FAM further states, "The controlling Department bureau or domestic field office must attempt to identify an appropriate donee, prior to following routine disposal procedures."

- 14 FAM 428 (a)(b), "Reporting Property Loss or Damage," requires the ACO to report missing, damaged, or destroyed accountable property to the APO through the PCO within 15 calendar days of discovering the loss or damage. The APO or the property survey board will act on reported instances of missing, damaged, or destroyed U.S. Government-owned personal property.

- 14 FAM 429, "Reporting Requirements," states that Form DS-1875, Property Management Report, is prepared by the ACO and the PCO, who must sign and submit it to the Property Management Branch (A/LM/PMP/BA/PM) by March 15 each year. The original form should be kept in the Inventory and Reconciliation file, and a copy should be scanned and submitted electronically to the Property Management Branch.

OBJECTIVE, SCOPE, AND METHODOLOGY

The Department of State's OIG conducted an audit of the Department's laptop computer security in the Washington, DC, area. The initial objective was to determine whether the Department has adequate security controls in place to protect national security and otherwise sensitive information stored, processed, and communicated on laptop computers. The audit was subsequently modified to limit the scope to a review of (1) property accountability related to the inventory control over Department-owned laptop computers, (2) the implementation of required encryption, and (3) security awareness training.

For this limited scope audit, OIG did not"

- Review all bureau-generated inventory records, including those relating to acquisition, maintenance, and third-party documents, such as invoices and CEPO forms, for the bureaus and samples selected for this audit to determine whether the information contained on the records was correctly recorded in ILMS Asset Management;

- Compare and analyze the supporting documentation for the 2005 and 2006 Department-prepared physical inventories conducted by the Department or an external contractor to determine discrepancies and reconciliations with ILMS Asset Management;

- Review the effectiveness of security controls applied to laptop computers or determine whether these controls protected the information stored, processed, and transmitted; or

- Review the content stored, processed, or transmitted on the laptop computers or make any determinations about the sensitivity or security level of such content.

To determine the universe of the Department's laptop computers assigned to domestic locations, OIG contacted A/LM and obtained a listing from the ILMS Asset Management module as of September 30, 2007. This listing identified 4,097 domestic laptop computers assigned to 31 bureaus and offices and undistributed in warehouses. The inventory is itemized in Appendix B.

To identify a sample of bureaus to review, OIG selected three bureaus with the largest number of laptop computers located domestically: the Bureau of Diplomatic Security (DS), IRM, and the Bureau of Overseas Buildings Operations (OBO). The Department's CIO is the head of IRM. OIG also selected INR because it processes intelligence information and had previously reported one classified laptop computer as lost in 2000. Collectively, these four bureaus had 1,679,[5] or 41 percent, of the domestic laptop computers. Of those 1,679 laptops, 1,612, or 39 percent, were located in the Washington, DC, area (includes nearby locations in Maryland and Virginia) as of September 30, 2007.

To determine a sample of laptop computers to review for these four bureaus, OIG randomly selected 341 of the 1,612 laptop computers (100 each with DS, IRM, and OBO and all 41 within INR). To determine the existence of these laptops, OIG requested that each bureau collect the laptops in a central review area where OIG conducted a physical inventory check to verify the inventory asset tag number, serial number, and model. While conducting this physical inventory verification, OIG also performed a visual inspection of all laptop computers that were located to determine whether each had been encrypted, as required by OMB mandates for all laptop computers. In instances where a laptop computer in the sample could not be located, OIG requested the required supporting documentation for the disposition of each one that was missing. The physical inventory verification and the review of disposition documentation were used by OIG to confirm the accuracy of information in ILMS Asset Management.

OIG also requested a listing of classified laptop computers from A/LM to determine, on a sample basis, whether proper labeling and encryption were implemented in accordance with Department policy. However, A/LM could not provide OIG with this listing because ILMS Asset Management did not contain an indicator to identify whether a laptop computer was classified or unclassified. Accordingly, the Department did not have an inventory of classified laptop computers in the Washington, DC, area. As an alternative approach, OIG sent a data call on October 3, 2007, to the executive directors for all Department bureaus and offices and requested each to provide a listing of its classified laptop computers located in the Washington, DC, area. To identify discrepancies, OIG compared the information received with the ILMS domestic inventory listing for all Department organizations, including the four bureaus selected for the audit. In addition, OIG conducted a physical verification for the existence, labeling, and encryption for all classified laptop computers identified in the data call responses for the four bureaus reviewed, whether or not they had been selected for the sample group, to determine compliance with Department policy.

[5] The total universe of laptop computers for the four bureaus is 582 for DS, 41 for INR, 656 for IRM, and 400 for OBO.

Because of the sensitive nature of information that may be stored on classified laptop computers, which are designated to process Secret data, OIG also identified other classified laptops for each of the four bureaus that were collocated in the review areas where the sampled laptops were held and labeled "Secret." The additional laptop computers discovered were compared with those identified on the ILMS list to determine whether any were also included in OIG's sample group. OIG also conducted a physical inspection of all classified laptops found in these storage areas that were not included in the sample group to determine whether each was properly encrypted in accordance with Department policy.

OIG also identified required training related to laptop computer security awareness and reviewed relevant records available for DS, OBO, and IRM to determine how participation in this training was tracked. OIG was not able to obtain complete training records for any of the four bureaus audited.

OIG analyzed relevant laws, regulations, and standards; Department policies and procedures; and existing inventory, purchasing, maintenance, disposal, and laptop security awareness and training records. OIG interviewed bureau officials responsible for managing and maintaining the laptop computers, applicable records, and inventory and acquisition systems. Specifically, OIG reviewed applicable guidance issued by OMB and the National Institute of Standards and Technology (NIST) to include memoranda and Federal Information Processing Standards (FIPS). OIG also reviewed reports issued by the Government Accountability Office and the Departments of Justice, the Treasury, and Veterans Affairs.

OIG conducted a survey to obtain laptop computer information from April to September 2007 and performed fieldwork from October 2007 to July 2008 in the Washington, DC, area, primarily at A/LM, DS, IRM, INR, and OBO. OIG accepted updated inventory information from each bureau until October 30, 2008, as each responded to OIG's notification of the initial missing laptop computers, but OIG did not verify the outcome of the searches for this equipment beyond this date.

OIG conducted this audit in accordance with generally accepted government auditing standards. OIG did not have an exit conference with Department officials, but it considered their comments and incorporated them into the report as appropriate. On October 10, 2008, OIG announced a follow-on audit of property accountability and compliance with security requirements for the Department's laptop computers at overseas posts.

AUDIT RESULTS

Department Did Not Fully Control Laptop Computer Inventory or Implement Encryption Requirements for Selected Bureaus

The Department does not have an accurate accounting for and has not encrypted all of its classified and unclassified laptop computers in the Washington, DC, area for the four bureaus included in OIG's audit. Three of the four bureaus were not able to fully account for each of the laptop computers in the sample. Contrary to the Department's official ILMS inventory records, OIG was unable to inspect 119 laptop computers in its sample size of 334[6] because they were either missing (27); were not physically located in the Washington, DC, area or were otherwise unable to be physically inspected (35); or had been disposed of (57). Of the 215 laptops that were physically inspected, 172 were not encrypted and 43 were encrypted.

Included in the sample of 334 were 14 classified laptop computers that were labeled "Secret," all of which were located and physically inspected. However, OIG's verification found that there was no encryption software installed on nine of these classified laptop computers. Although the Department had issued a series of mandates regarding responsibilities for protecting unclassified and SBU laptop computers, including encryption requirements, it had not done so for the more security-sensitive classified laptop computers.

Table 1 summarizes OIG's final verification results of its audit of accountability and encryption for the sample of 334 laptop computers assigned to DS, IRM, INR, and OBO. (This table is also presented in the Executive Summary section of this report.)

[6] OIG's original sample size totaled 341; however, during fieldwork, this number was reduced to 334 because OIG found seven items in the ILMS sample that were miscoded and were not laptop computers.

Table 1. Results of Testing for Inventory and Encryption of 334 Laptop Computers Included in Sample Group

LAPTOP COMPUTERS IN SAMPLE GROUP									
Bureau	Number and Type of Laptops			Results of Inventory and Encryption Testing					
	Unclassified and SBU	Classified	Total Sample Group	Missing	Encrypted	Not Encrypted	Located but Unable to Test for Encryption	Disposed	Total Sample Group
DS	97	0	97	6	13	45	7	26	97
INR	31	8	39	0	0	39	0	0	39
IRM	95	3	98	18	14	26	19	21	98
OBO	97	3	100	3	16	62	9	10	100
Total	320	14	334	27	43	172	35	57	334
% of Total	96%	4%	100%	8.0%	13.0%	52%	10%	17.0%	100%

Note: Percentages adjusted for rounding.

OIG also determined that there was no requirement to identify computers designated as "classified" in ILMS. Because ILMS is not capturing identifiers for laptop computers such as those labeled "Secret," it is not a viable resource, thereby making inventory accountability and visibility over this security-sensitive equipment fractured. Furthermore, procedures to remove property from ILMS are not being utilized, thereby misstating the active inventory. Although security awareness training is required for laptop computer users, it is not centrally tracked so that the Department is assured that all individuals are appropriately trained.

Department Did Not Properly Account for All Laptop Computers

As of October 31, 2008, 27 laptop computers were missing from OIG's sample group for three of four bureaus and therefore were not available for OIG to verify. While Department officials have stated that the disposition of four of the 27 items was determined and produced informal documentation, proper asset tracking documentation was not available to support these claims. As a result, OIG could not verify the location of those four items, and none had been properly removed from the official inventory system. Department officials said that, "to the best of [their] knowledge," none of the missing laptop computers were classified as "Secret." The estimated cost of the missing laptop computers is about $55,000.

In February 2008, at the conclusion of its initial verification, OIG alerted Department senior leadership that 83 laptop computers in its sample group could not be accounted for. Because of the potential for unprotected information contained on the laptops to be at risk for unauthorized exposure, OIG provided Department officials with an opportunity to locate the missing laptop computers. After a concentrated search, 56 were found and made available for OIG to inspect either physically or via acceptable documentation if not located locally. OIG used an alternative method whereby it accepted, from a designated official, legible photographs of the laptop computers that clearly showed the official serial and asset tag numbers affixed to the laptop computer itself or documentation showing that the laptop computer was legitimate, such as a nonexpendable property transfer form for DS.

Regarding the 27 laptop computers still missing, Department officials could not determine the disposition of 23 of them. Officials stated that three of the remaining four laptop computers were returned to the vendor and that one was destroyed in a fire, but they could not provide proper asset tracking documentation to support these events. As a result, OIG could not verify the locations of those four items, and none had been properly removed from the official inventory system. After several attempts by OIG, Department officials provided proper documentation to change the classification for only one of the 27 laptop computers to "missing" by the end of its verification. Documentation for 18 of the 27 missing laptops was prepared after OIG had completed its verification.

According to Department officials in IRM and DS, the information that may be contained on the hard drive of the missing 27 laptop computers was unknown, but, "to the best of [their] knowledge," none of the laptops contained PII or classified information. OBO officials responded for one of their missing laptop computers, stating that the computer did not contain PII or classified information. However, none of the officials for these bureaus could provide documentation to OIG to support their statements that the hard drives of the missing laptop computers did not contain PII or classified information. Because the content and the encryption status of the missing laptop computers are unknown, there is a risk that PII and other sensitive Department information may be susceptible to unauthorized access and use. Details on the missing laptop computers are presented in Table 2.

Table 2. Missing Unclassified and SBU Laptop Computers

MISSING LAPTOP COMPUTERS					
Bureau	With Proper Missing Equipment Documentation	Without Proper Disposition Documentation	Destroyed in Fire (No Supporting Documentation)	Returned to Vendor (No Supporting Documentation)	Total Missing
DS	0	4	0	2	6
INR	0	0	0	0	0
IRM	0	16	1	1	18
OBO	1	2	0	0	3
Total	1	22	1	3	27
Percentage	4%	81%	4%	11%	100%

When a property item is missing, damaged, or destroyed, Form DS-310, U.S. Department of State, Property Survey Report, is to be prepared in accordance with 14 FAM 425.3, "Property Utilization." In the case of a laptop computer, the ACO for each office must submit, to the PCO (usually in the executive office), a Form DS-310 with an explanation as to why the laptop is missing. When the Form DS-310 is received, the PCO forwards it to the APO. After the APO determines that all efforts have been made to recover the laptop, the APO will sign the Form DS-310 and send a copy back to the PCO, who then deletes the item from ILMS. This procedure was not performed for the 27 items OIG determined to be missing. The risk that a laptop computer could unknowingly become missing and not be reported also increases the risk that the information it contains could become compromised. OIG's results also indicate that ILMS was not being updated for missing laptop computers to reflect an accurate current inventory.

Urgent Action Sought To Locate Missing Laptops

On February 6, 2008, the Department's Senior Assessment Team[7] discussed the preliminary results of OIG's audit and whether the creation of a significant defi-

[7] The Senior Assessment Team (SAT) was established in 2005 to provide oversight of the annual assurance assessment on the effectiveness of internal control over financial reporting required under OMB Circular A-123, Appendix A, Management's Responsibilities for Internal Control. The SAT reports the assessment status and identified weaknesses to the Department's MCSC. The Inspector General is a nonvoting member.

ciency should be recommended to the Department's Management Control Steering Committee (MCSC)[8] in terms of protecting PII, an action that was supported by representatives of both the CIO and OIG. OIG also reported this potential for lost laptop computers to the MCSC at its February 21, 2008, meeting. During this meeting, the early indications that laptop computers may be lost and unencrypted was discussed as a potential significant deficiency, and OIG strongly encouraged all MCSC members to request that their respective executive directors find the missing laptops.

Because of the unknown sensitivity of information that these missing laptop computers may have contained and the urgent need to act upon the potential risk of lost and unprotected information, on February 29, 2008, OIG formally notified senior executives of each of the respective bureaus of their specific missing inventory to provide Department officials with an immediate opportunity to locate the laptop computers. In response, Department officials requested an extension of OIG's fieldwork to allow them to locate the missing laptop computers, and OIG agreed to verify the existence of those laptops found. As laptops were found or were otherwise accounted for with proper documentation, the bureaus brought them to a central location for verification by OIG. The last physical verification of laptop computers that were subsequently found or had been properly disposed of was completed by OIG in September 2008. Subsequently, the Department continued to provide periodic updates as additional laptops were either located or accounted for by some other disposition action. The final accounting as of October 23, 2008, showed that 27 laptop computers from OIG's sample were still missing.

Given the government-wide importance and attention placed on protecting PII and sensitive agency information, more aggressive and consistent action is needed by A/LM, DS, INR, IRM, and OBO to enforce the various internal and federal requirements relating to laptop computer inventory responsibilities, including protecting PII. Furthermore, Department policy requires that notification of missing laptop computers[9] or breaches to PII[10] be made to designated internal and external entities, such as to OIG; DS' Computer Incident Response Team (CIRT); or the United States Computer Emergency Readiness Team (US-CERT), which is a partnership between the Department of Homeland Security and the public and private sectors.

[8] The MCSC was established by the Under Secretary for Management to oversee all aspects of the Federal Managers' Financial Integrity Act process for the Department. The purpose of the MCSC is to set management control policy, determine management control objectives, and oversee management control processes for the Department. The duties of MCSC members include supporting the resolution and closing of OIG audit recommendations when appropriate to advance management control objectives. The Inspector General is a nonvoting member.

[9] 12 FAM 592.4, "Reporting Cyber Security Incidents."

[10] Personally Identifiable Breach Response Policy, prepared by the Bureau of Administration, in draft form as of May 2008.

Recommendation 1: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a thorough search is made to locate its missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain personally identifiable information or other sensitive agency information, appropriate notifications should be made.

Bureau Response and OIG Reply

In its response to the draft report, DS did not address the recommendation; therefore, the recommendation is unresolved.

Recommendation 2: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a thorough search is made to locate its missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain personally identifiable information or other sensitive agency information, appropriate notifications should be made.

Bureau Response and OIG Reply

In its response to the draft report, OBO stated that it had conducted "a thorough inventory of OBO laptops" between November 2007 and April 2008 and had made "an extensive analysis" of all OBO property records during that time. OBO further stated that "continued efforts" found that two laptops were unaccounted for from OBO's inventory. The last known recipient of one laptop was the Director of the Cost Management Division, who indicated that the laptop contained unclassified value engineering data while it was in her possession, that she had returned the laptop to OBO/IRM [formerly OBO/IM] through a subordinate, and that the information was deleted before the laptop was returned. OBO stated that it was "impossible to confirm this" because of the "lack of appropriate [standard operating procedures] under the prior IRM management" but that "[c]urrent management controls prevent this from occurring." OBO said that the other missing laptop, which was new, "had last been documented during its move from the warehouse where it had been initially received to imaging in preparation for its eventual deployment."

OBO said that it found, "[a]fter an additional inquiry," that a third laptop was missing; that the laptop was "believed to be in the field;" and that its status would be verified at the end of the OBO laptop recall, which was scheduled for June 1, 2009. OBO further stated that "PII is expressly prohibited on any OBO laptops as exemplified in the Laptop Security Briefing and administered by the Information Systems Security Officer (ISSO) and/or the laptop administrator" and that there was "no indication that any PII or SBU [Sensitive but Unclassified] data was compromised with the loss of these 3 laptops."

On the basis of OBO's response, OIG considers the recommendation resolved. Although OBO has identified the last known actions for two of its three missing laptop computers, it cannot verify their current locations. The recommendation can be closed when OIG receives documentation (a) verifying that the third laptop is actually assigned to a user in the field and contains no PII, SBU, or classified information; (b) declaring all laptops that cannot be located or verified as lost or missing; and (c) verifying that proper accountability documentation has been prepared and submitted to update the inventory status of all three laptop computers in ILMS.

Recommendation 3: OIG recommends that the Chief Information Officer ensure that a thorough search is made to locate the Bureau of Information Resource Management's missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain personally identifiable information or other sensitive agency information, appropriate notifications should be made.

Bureau Response and OIG Reply

In its response to the draft report, IRM did not address the recommendation; therefore, the recommendation is unresolved.

Recommendation 4: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

Bureau Response and OIG Reply

In its response to the draft report, DS did not address the recommendation; therefore, the recommendation is unresolved.

Recommendation 5: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

Bureau Response and OIG Reply

In its response to the draft report, OBO stated that it has "no evidence that PII or sensitive Department data has been lost as a result of the 3 missing laptops." OBO also stated that it had not yet determined whether the laptops had been reissued without proper administrative tracking but that there was "currently no evidence of theft or tampering."

OBO reiterated its plans for a June 1, 2009, exercise to recall all laptop computers for this quarter and to require "the entire OBO community" to deliver the laptops in their possession to OBO/RM/EX/IRM [the Office of Resource Management, Office of the Executive Director, Office of Information Resource Management] for replacement, update, and/or service." OBO further stated that at the end of the exercise, it plans to have "a complete accounting of its entire laptop inventory, and will be in a position to report the status of each, and if an incident exists."

Based on OBO's response, OIG considers the recommendation resolved. The recommendation can be closed when OIG receives documentation that provides a complete accounting of OBO's three missing laptop computers and confirms whether potential or actual incidents have occurred and, if so, that proper notification was made as warranted.

Recommendation 6: OIG recommends that the Chief Information Officer ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

Bureau Response and OIG Reply

In its response to the draft report, IRM did not address the recommendation; therefore, the recommendation is unresolved.

Recommendation 7: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

Bureau Response and OIG Reply

In its response to the draft report, DS did not address the recommendation; therefore, the recommendation is unresolved.

Recommendation 8: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

Bureau Response and OIG Reply

In its response to the draft report, OBO stated that "fundamental errors" had been made in the administration of the laptop program "under previous OBO/IM management." OBO further stated that "proper controls were not in place to track and monitor [laptop computer] usage" and that "the task of laptop administration was moved from person to person within the Division without regard for the responsibility as identified in the FAM." OBO said that the laptop program management function was moved under the purview of the ISSO in January 2008 and that today it is "rigorously controlled and reviewed." According to OBO, excess inventory is being reduced to a manageable level, the laptop request and distribution process has been revised to use standard property accountability forms, a new laptop standard operating policy and procedure has been released, and management controls have been reintroduced.

On the basis of OBO's response, OIG considers the recommendation resolved. The recommendation can be closed when OIG receives a copy of the new laptop standard operating policy and procedure and verification that the new policy and procedure have been implemented in accordance with applicable sections of the FAM and other Department of State directives, to include telegrams.

Recommendation 9: OIG recommends that the Chief Information Officer ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

Bureau Response and OIG Reply

In its response to the draft report, IRM did not address the recommendation; therefore, the recommendation is unresolved.

Department Did Not Encrypt All Laptop Computers

OIG was unable to inspect 119 laptop computers in its sample size of 334 because they were either missing (27); were not physically located in the Washington, DC, area or were otherwise unable to be physically inspected (35); or had been disposed of (57). Of the 215 laptops that were physically inspected, 172 were not encrypted and 43 were encrypted. There is the risk that the count for unencrypted laptops may be higher because OIG could not test 119 laptop computers.

Through a series of internal notices, the Department had mandated that all Department-owned unclassified and SBU laptop computers be encrypted by September 30, 2007, for older[11] laptops and by July 1, 2008, for all laptop computers. A comprehensive listing of these notices is in Appendix A. Although referred to in a March 2008 notice,[12] the Department had not issued an encryption requirement for the more security-sensitive classified laptop computers. According to one of DS' Special Assistants to the Senior Coordinator for Security Infrastructure, no telegram was issued to address classified laptop computers. The Special Assistant stated:

[11] In 07 State 058726 All Diplomatic and Consular Posts (ALDAC) telegram, issued on May 1, 2007, entitled "Protection of Personally Identifiable Information (PII) on Laptops," the Department defined older laptop computers as those that were currently in operation and not using Vista operating software.

[12] 08 State 032537 ALDAC telegram, issued on March 28, 2008, entitled "Unclassified and Sensitive But Unclassified Laptop Inventory and Encryption Responsibilities," includes the statement, "Responsibilities for classified laptops will follow septel [septel refers to a separate telegram]."

> [T]he telegram died on the vine, recognizing that the encryption requirement only exists for the protection of PII and that the cost associated with the encryption software to meet the classified standard for a classified laptop is more than 3K a copy versus the risk that 1) PII would be stored on a classified laptop and more importantly 2) a classified laptop would be removed from the building; noting the fact that a classified laptop must only [be] removed from classified facility to a classified facility and must be double-wrapped for transport and not be unattended during travel.

Because the content on these laptop computers is unknown, OIG does not agree that the risk would necessarily be low or that a classified laptop computer would not contain PII or other sensitive agency information. Furthermore, OMB's requirement makes no exceptions for classified laptops on the basis of cost or content. Additionally, while IRM has identified specific procedures in place for handling classified material, to include handling classified laptop computers, these do not supersede the OMB requirement to encrypt all laptop computers.

Therefore, OIG does not agree with this interpretation of encryption requirements relating to classified laptop computers. Specifically, according to OMB requirements,[13] the Department must develop policies and procedures to address sensitive agency information on mobile devices, such as laptop computers. Furthermore, the Department had begun drafting guidance for portable computers, which includes laptop computers, to be contained in 12 FAM 684,[14] but it has not finalized or implemented the guidance. The February 26, 2008, version of the draft guidance that OIG obtained contains a requirement that all Department-owned classified portable computer hard drives should be encrypted.

As Tables 3 and 4 indicate, most of the 334 laptop computers in the sample group that OIG was able to test were not encrypted—64 percent of the classified and 51 percent of the unclassified and SBU laptop computers.

[13] OMB Memoranda M-06-16 and M-07-16. (These memoranda are listed in the Background section of this report.)

[14] 12 FAM 684.2-5(e), "Department-Owned Classified Portable Computers," draft document dated February 26, 2008.

Table 3. Results of Testing for Encryption on Classified Laptop Computers

CLASSIFIED LAPTOP COMPUTERS						
Tested for Encryption			Not Tested			
Bureau	Number Encrypted	Number Not Encrypted	Number Located but Unable To Be Tested	Number Disposed	Number Missing	Total
DS	0	0	0	0	0	0
INR	0	8	0	0	0	8
IRM	2	1	0	0	0	3
OBO	2	0	1	0	0	3
Total	**4**	**9**	**1**	**0**	**0**	**14**
Percentage	29%	64%	7%	0%	0%	100%

Table 4. Results of Testing for Encryption on Unclassified and Sensitive but Unclassified Laptop Computers

UNCLASSIFIED AND SENSITIVE BUT UNCLASSIFIED LAPTOP COMPUTERS						
Tested for Encryption			Not Tested			
Bureau	Number Encrypted	Number Not Encrypted	Number Located but Unable To Be Tested	Number Disposed	Number Missing	Total
DS	13	45	7	26	6	97
INR	0	31	0	0	0	31
IRM	12	25	19	21	18	95
OBO	14	62	8	10	3	97
Total	**39**	**163**	**34**	**57**	**27**	**320**
Percentage	12%	51%	11%	18%	8%	100%

Department officials for the four bureaus provided OIG with several reasons why they had not met the encryption requirements as follows:

- The Deputy Division Chief for the Cyber Threat Analysis Division for DS and the ISSO for OBO said that both bureaus were in the process of encrypting their laptop computers but that neither had finished and neither could provide OIG with an implementation methodology or schedule.

- The Executive Director for INR acknowledged the mandates but said that INR did not encrypt its unclassified laptop computers because they are used only for word processing or presentation purposes and sensitive information is prohibited from being saved on those laptop computers. The Executive Director interpreted the mandates as applicable only to laptop computers that processed sensitive and/or classified information.

- By February 2008, IRM had completed its schedule for encrypting its laptop computers. However, IRM officials said that they could ensure only that the laptop computers contained in their "known" universe, which had been turned in, were encrypted. They did not believe that their inventory recorded in ILMS was accurate or complete.

From a Department-wide perspective, OIG discussed the lack of compliance with encryption requirements with the Department's Chief Information Security Officer (CISO) and his staff. According to these officials, the Department first needed to determine its inventory of laptop computers and whether available licenses for one type of encryption software, SecureDoc Disk Encryption, could be used. IRM sent Department-wide guidance[15] mandating encryption using the existing licenses for SecureDoc encryption software. According to the CIO, the Department recognized that it would probably have to purchase additional licenses, which was a resource issue, but it was coupled with the need to identify viable technical software solutions for encryption. By January 18, 2008, the CISO wanted to initiate coordination with DS and the rest of the Department to have a coordinated and consolidated approach to encrypt laptop computers worldwide. The CISO began by scheduling encryption for IRM's laptop computers, meanwhile negotiating with vendors to come up with reasonable and systematic options for purchasing other encryption software. After the decision was reached regarding using additional SafeNet Protect Drive encryption software (Safenet), on March 28, 2008, the CISO sent out worldwide guidance mandating encryption.[16]

By January 10, 2008, IRM had acquired 55,700 licenses for SafeNet encryption software, which was certified by NIST and approved by the Department's Information Technology Configuration Control Board for Department-wide implementation on March 19, 2008. According to the CISO, these licenses were received with a bundle of Public Key Infrastructure maintenance licenses at no additional charge from the vendor and will be used on Department desktop and laptop computers. However, based on discussions with Department officials and review of the encryption process, OIG believes that the success of this encryption implementation will be dependent upon the Department's ability to identify and track its universe of laptop computers.

[15] 07 State 0167072 ALDAC telegram, issued on December 14, 2007, entitled "Protecting Sensitive Department Information on Mobile Computing Devices and Media."
[16] 08 State 032537 ALDAC telegram, issued on March 28, 2008.

Unable To Test for Encryption on All Laptops in Sample

OIG was unable to test whether encryption software had been installed on 35 laptop computers for several reasons. For instance, some computers were not physically available locally in the Washington, DC, area. To verify their existence remotely, OIG used an alternative method whereby it accepted, from a designated official, legible photographs of the laptop computers that clearly showed the official serial and asset tag numbers affixed to the laptop computer itself or documentation showing that the laptop computer was legitimate, such as a nonexpendable property transfer form for DS. Other laptop computers could not be tested because they were inoperative in that either the hard drive or the power cord was not available. Therefore, the number of unencrypted laptops could potentially be higher. The details for the laptops that OIG was unable to test are provided in Table 5.

Table 5. Laptop Computers That Were Located but Unable To Be Tested for Encryption

CLASSIFIED LAPTOP COMPUTERS						
	Remote Inventory Verification Only		**Inoperative and Other**			
Bureau	Located Overseas	Located Domestically Outside DC Metro Area	Without Hard Drive	Without Power Cord	Other: In Use – Not Available	Total
DS	0	0	0	0	0	0
INR	0	0	0	0	0	0
IRM	0	0	0	0	0	0
OBO	0	0	0	0	1	1
Total	**0**	**0**	**0**	**0**	**1**	**1**
UNCLASSIFIED AND SENSITIVE BUT UNCLASSIFIED LAPTOP COMPUTERS						
	Remote Inventory Verification Only		**Inoperative and Other**			
Bureau	Located Overseas	Located Domestically Outside DC Metro Area	Without Hard Drive	Without Power Cord	Other: In Use – Not Available	Total
DS	0	1	3	1	2	7
INR	0	0	0	0	0	0
IRM	0	1	18	0	0	19
OBO	0	1	0	4	3	8
Total	0	3	21	5	5	34

TOTAL LAPTOP COMPUTERS						
	Remote Inventory Verification Only		**Inoperative and Other**			
Bureau	Located Overseas	Located Domestically Outside DC Metro Area	Without Hard Drive	Without Power Cord	Other: In Use – Not Available	Total
DS	0	1	3	1	2	7
INR	0	0	0	0	0	0
IRM	0	1	18	0	0	19
OBO	0	2	0	4	3	9
Grand Total	0	4	21	5	5	35
Percentage	0%	12%	60%	14%	14%	100%

Note: Percentages adjusted for rounding.

Additional Classified Laptops Discovered and Tested for Encryption

Apart from the classified laptop computers included in the sample group that OIG identified through the data call and manually, an additional 67 classified laptops were discovered during the on-site searches, including 28 that belonged to bureaus not included in OIG's sample group. Because of the sensitive nature of information that may be stored on classified laptop computers, OIG also tested the additional 39 laptops associated with the four bureaus in its sample group to determine whether each had been recorded in ILMS and installed with encryption software. Of the 39 laptops, 33 were not recorded in ILMS. Only five (or 12 percent) of the 39 had been encrypted, as illustrated in Table 6. Of the 39, OIG found that 31 had been reported in response to its data call.

Table 6. Results of Inventory and Encryption Verification of Classified Laptop Computers Not Included in ILMS Sample Group

ADDITIONAL CLASSIFIED LAPTOP COMPUTERS FOUND							
Method Discovered				**Results of Inventory and Encryption Testing**			
Bureau	Number Identified by All Bureaus in Data Call	Number Identified Manually	Total	Number Encrypted	Number Not Encrypted	Number Located but Unable to Test for Encryption	Total
DS	21	1	22	2	18	2	22
INR	7	0	7	0	6	1	7
IRM	2	0	2	1	1	0	2
OBO	1	7	8	2	0	6	8
Subtotal That Was Tested	**31**	**8**	**39**	**5**	**25**	**9**	**39**
Percentage	79%	21%	100%	13%	64%	23%	100%
Other Bureaus Not in Sample Group*	28	n/a	28				
Total Additional Classified Laptops Found	**59**	**8**	**67**				

*No testing was performed for the laptop computers with bureaus that were not included in the sample group.

Without visibility of the classified laptop computers in a centralized inventory system, such as ILMS, proper security safeguards are less likely to be implemented on a routine basis.

Recommendation 10: OIG recommends that the Assistant Secretary for Diplomatic Security, in coordination with the Chief Information Officer, ensure that 12 FAM 684, "Portable Computers" (or other numbering sequence), is finalized and published.

Recommendation 11: OIG recommends that the Chief Information Officer, in coordination with the Assistant Secretary for Diplomatic Security, issue a Department of State-wide mandate requiring that appropriate encryption be acquired and installed on all classified laptop computers, in accordance with specified Department policy, as soon as possible but no later than September 30, 2009.

Bureau Response and OIG Reply

In its response to the draft report, IRM said that DS "owns 12 FAM, therefore, IRM suggests that this action [the recommendation] be directed to DS."

OIG acknowledges that DS is responsible for coordinating the drafting, vetting, and publishing of 12 FAM. However, the primary intent of the recommendation is for the issuance of a Department-wide mandate to require appropriate encryption for classified laptop computers, an action that can be implemented once a policy is put in place. As contained in 12 FAM 615, "Department Responsibilities," IRM has joint responsibility with DS to develop and implement a comprehensive, technically current, and cost-effective Automated Information System security program for the Department. Therefore, in recognizing the collaboration needed by both IRM and DS, OIG has distinguished the responsibilities for this action. First, OIG has revised recommendation 10 and specified that DS is responsible for the action concerning completing and publishing the guidance being developed in draft 12 FAM 684, "Portable Computers." Second, OIG has specified that IRM is responsible for the action regarding mandating the installation of appropriate encryption because the CIO has issued prior Department Notices and ALDACs mandating encryption on laptop computers. As a result of these clarifications, recommendations 10 and 11 are unresolved for DS and IRM, respectively.

Recommendation 12: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that all of its Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Bureau Response and OIG Reply

In its response to the draft report, DS did not agree with "OIG's interpretation that OMB mandated encryption of classified laptops," and it questioned the validity of the recommendation. DS said that both OMB M-06-16 and M-07-17 address only NIST standards but that NIST does not have governing authority over standards for national security systems, such as for classified laptops. DS further stated that the Committee for National Security Systems (CNSS), which is the governing body for policy relating to national security systems, does not require encryption but that if encryption is used, CNSS requires that the encryption be approved by the National Security Agency (NSA). DS stated that the "only currently available NSA approved encryption product for use with a laptop is an external, in-line [Communication Security] COMSEC device," and it provided its explanation as to why CNSS policy does not require encryption. DS also provided illustrations of specific provisions of OMB M-06-16 and OMB M-07-16 to support its position. According to DS, "The lack of CNSS standards in [OMB Memoranda M-06-16 and M-07-17] indicate that OMB never intended to address the protection of PII on classified systems."

DS stated that OIG , "[b]y its own admission . . . in the subject draft report, *'did not review the effectiveness of security controls applied to laptop computers to determine whether these controls protected the information stored, processed and transmitted….'"* DS further stated, "As the Department already has in place physical security controls for classified information and equipment, including laptops, when the information is removed from, the agency location, does not allow accessed from outside, and CNSS is the governing authority for the protection of national security systems, DS does not consider this recommendation to be valid. Therefore, DS requests that all mention of encryption for classified laptops be removed from this report."

Regarding the additional classified laptop computers that OIG found during its audit, DS stated, "OIG found encryption software on some classified laptops that were inspected, which DS considers a classified information security issue as encryption for classified systems require additional COMSEC equipment, i.e., hardware that is keyed with COMSEC material/keys, not software installation."

Other than questioning the validity of the recommendation regarding classified laptop computers, DS did not fully address the entire recommendation in its response. Specifically, DS did not address its concurrence or nonconcurrence with requirements to physically inspect and encrypt unclassified and SBU laptop computers, which are specifically required for Department-owned laptop computers as mandated in various Department-wide notices and ALDACs (see Appendix A).

Regarding the validity of the recommendation pertaining to the encryption of classified laptop computers, OIG concedes that the method and technology for encryption may be more prescriptive than the installation of encryption software such as SecureDoc and Safenet. As such, OIG has modified all such recommendations to replace the term "proper encryption software" with "appropriate encryption." However, OIG disagrees that classified laptop computers should not be encrypted. In the details of its response, DS also referred to the encryption requirement contained in OMB M-07-16, section C, "Security Requirements." However, DS seems to have taken away only the portion of this requirement that describes "encryption" in terms of NIST requirements. More specifically, this provision does not exclude other governing laws and policies, such as those prescribed for national security systems. OMB M-07-16, section C, which DS illustrated, states:

> **While agencies continue to be responsible for implementing all requirements of law and policy** [emphasis added], below are five requirements agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, e.g., law enforcement information, etc.
>
> - Encryption. Encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing.

The requirement for the use of NSA-approved encryption products is applicable government-wide and is found in CNSS Policy No. 15, Fact Sheet No.1, "National Policy on the Use of Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information," June 2003. Specifically, this policy states:

> Scope
>
> (4) This policy is applicable to all U.S. Government Departments or Agencies that are considering the acquisition or use of products incorporating the Advanced Encryption Standard (AES) to satisfy Information Assurance (IA) requirements associated with the protection of national security systems and/or national security information.

Policy

> (5) NSA-approved cryptography[17] is required to protect (i.e., to provide confidentiality, authentication, non-repudiation, integrity, or to ensure system availability) national security systems and national security information at all classification levels.

Given this government-wide CNSS policy, OIG disagrees with DS that CNSS has not specifically issued guidance addressing encrypting classified laptop computers. Furthermore, based on its own action, OIG believes that DS was embracing this security measure by drafting new policy in 12 FAM 684 that will require encryption for classified laptop computers. Specifically, the draft 12 FAM 684.2-5(e), "Department-Owned Classified Portable Computers," states:

> The system manager must encrypt all Department-owned classified portable computer hard drives with Type 1 encryption products endorsed by the National Security agency (NSA). In addition, the user must encrypt all associated media (e.g. CDs, flash drives) with Type 1 encryption products endorsed by the NSA.

In its response, DS identified the use of NSA-approved encryption products, such as a COMSEC device, as the approved method for encrypting classified systems, and it stated that because OIG had determined that encryption software had been found on DS' classified laptops instead of COMSEC equipment, a security issue had been identified.

Because OIG found that some classified laptop computers had encryption software installed, OIG does not agree with DS that it did not intend to encrypt its classified laptop computers by making the argument that the encryption software was not in compliance with COMSEC equipment encryption requirements. To the contrary, OIG believes that DS needs to clarify and issue encryption requirements for classified laptop computers by finalizing and publishing 12 FAM 684, "Portable Computers," as discussed in recommendation 10 of this report.

Therefore, OIG considers this recommendation unresolved. It can be resolved and closed when OIG receives documentation to support DS' implementation of this recommendation to physically inspect and have proper encryption technology installed on all of the DS-owned classified, unclassified, and SBU laptop computers. Documentation such as an encryption installation completion report that itemizes each laptop computer would fulfill the intent of this verification.

[17] NSA-approved cryptography consists of an approved algorithm; an implementation that has been approved for the protection of classified information in a particular environment; and a supporting key management infrastructure.

Recommendation 13: OIG recommends that the Assistant Secretary for Intelligence and Research ensure that all of its Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Bureau Response and OIG Reply

In its response to the draft report, INR clarified that it did have an accurate accounting for its laptops. INR further stated that since the end of OIG's audit, it had physically inspected and installed proper encryption software on all INR-owned laptop computers that are assigned to users.

On the basis of INR's response, OIG considers the recommendation resolved. The recommendation can be closed when OIG receives documentation to support INR's implementation of this recommendation to physically inspect and have proper encryption technology installed on all of the INR classified, unclassified, and SBU laptops. Documentation such as an encryption installation completion report that itemizes each laptop computer would fulfill the intent of this verification.

Recommendation 14: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that all of its Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Bureau Response and OIG Reply

In its response to the draft report, OBO reiterated, as it did in its response for recommendation 5, plans for a June 1, 2009, exercise to recall all laptop computers for this quarter and to require "the entire OBO community" to deliver the laptops in their possession to OBO/RM/EX/IRM "for replacement, update, and/or service." OBO further stated that at the end of the exercise, it "anticipates having a complete accounting of its entire laptop inventory" and will then "be in a position to report the status of each laptop in its inventory."

On the basis of OBO's response, OIG considers the recommendation resolved. The recommendation can be closed when OIG receives documentation to support OBO's implementation of this recommendation to physically inspect and have proper encryption technology installed on all of the OBO classified, unclassified, and SBU laptops. Documentation such as an encryption installation completion report that itemizes each laptop computer would fulfill the intent of this verification.

Recommendation 15: OIG recommends that the Chief Information Officer ensure that all of the Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers within the Bureau of Information Resource Management are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Bureau Response and OIG Reply

In its response to the draft report, IRM did not address this recommendation; therefore, the recommendation is unresolved.

Recommendation 16: OIG recommends that the Chief Information Officer ensure that a Department of State-wide process is developed and implemented so that newly acquired laptop computers are not issued to users until appropriate encryption is installed in accordance with the sensitivity and security level for the use of each laptop computer.

Bureau Response and OIG Reply

In its response to the draft report, IRM stated that the laptops purchased through the IRM Laptop Program are encrypted before they are used and that "Department-wide Notices and IRM Notices have been issued over the past two years reiterating this requirement."

In OIG's review of various Department-wide and IRM notices, as listed in Appendix A, only one referred to the IRM Laptop Program. According to IRM Notice 2008-11, the IRM Laptop Program became effective as of April 14, 2008, and requires that all laptops purchased through the IRM Laptop Program be encrypted before use. However, OIG did not identify a similar notice specifying that the IRM Laptop Program or the encryption provisions thereof were applicable to all Department organizations.

OIG considers this recommendation resolved. However, OIG requests a copy of any Department-wide notification that clarifies that the intended recipients of IRM Notice 2008-11 or another publication regarding the IRM Laptop Program are all Department organizations. This recommendation can be closed when IRM provides OIG with documentation verifying that the implementation of the encryption provision of the Laptop Program has been applied Department-wide.

ILMS Is Not Accurate or Effectively Utilized

OIG was able to verify the inventory status of 307 (92 percent) of the 334 laptop computers in its sample group. Specifically, 250 (about 75 percent) were located both within and outside the Washington, DC, area, as supported by physical verification or acceptable documentation, and Department officials provided OIG with proper documentation for the disposal of 57 laptop computers. However, in conducting its audit, OIG determined that ILMS was not being used effectively to easily identify specific laptop computer property items, to code laptop computers designated as classified, to reconcile annual physical inventory results, or to update current inventory for missing or disposed of property.

Too Many Asset Coding Options Available

OIG identified the universe of 4,097 domestically located laptop computers listed in ILMS as of September 30, 2007, through discussions with Department officials and review of the ILMS inventory as of September 30, 2007. OIG ascertained that 30 different asset codes were used in ILMS purportedly to identify laptop computers. OIG found nine of these codes in its sample to identify laptop computer equipment, as described in Table 7, but the only correct laptop computer code was 25108. OIG identified this universe by screening these codes and other descriptive information in ILMS to identify actual laptop computers. At that time, OIG also found that seven ILMS items were incorrectly coded as laptop computers—namely, three printers, one case, one console, one workstation, and one computer monitor. Therefore, the original sample was reduced from 341 to 334. However, OIG reverted to the original sample of 341 to perform an analysis of the frequency with which the correct coding was used, as detailed in Table 8.

As Table 7 illustrates, the nine codes corresponded to several different types of computer equipment. One frequently used code, 25104, was associated with the Department's predecessor inventory system to ILMS, Non-Expendable Property Application (NEPA), which was used to identify laptop computers.

Table 7. Property Asset Codes Used in ILMS for Sample of Laptop Computers

ILMS Asset Class Code	Description
25108	CPU, LAPTOP/NOTEBOOK
25104	CPU, PORTABLE
23000	Communications Equipment
25000	ADP and Word Processing Equipment
25100	CPU (Central Processing Unit)
25103	CPU, MICRO
25250	DISPLAY, CRT, Computer
25990	ADP/AP Equipment, Other
A0505	Computer Accessories

Table 8 demonstrates that the correct code, 25108, was used only 40 percent of the time to identify a laptop computer.

Table 8. Asset Class Coding for Sample Group of Laptop Computers

Bureaus	Correct Asset Code Used	Incorrect Asset Codes Used	Total
DS	24	76	100
IRM	26	74	100
OBO	73	27	100
INR	13	28	41
Total	136	205	341
Percentage	40%	60%	100%

According to Department officials, asset class codes for laptop computers in ILMS were incorrect because (1) the prior asset class code from NEPA was transferred and retained when the Department converted to ILMS in September 2005, (2) data entry personnel did not consistently choose the new asset class code for laptop computers in ILMS, and (3) updates were not made to ILMS as a result of physical inventory reconciliations.

OIG found that PCOs entered data into ILMS Asset Management and queried the application for the appropriate asset class code but that they did not consistently choose the correct asset class code for laptop computers. Of the 205 incorrectly coded items in OIG's sample, 171 were identified with the old NEPA code 25104. The PCO should complete an ILMS training course before access is granted to ILMS Asset Management and may attend ILMS refresher training thereafter. The training does not include guidance on which specific codes to use for which property, but it does show how to find the information. Department officials were unable to provide documentation to OIG to show that the PCOs had successfully completed the training. OIG identified no other guidance issued to staff on how to determine the correct asset class code to use for laptop computers.

Annual Inventory Not Reconciled to ILMS

The Department is required to conduct an annual physical inventory of its property, including laptop computers. However, the ACOs were not providing the PCOs with data to update ILMS Asset Management after the annual physical inventory had been conducted. OIG did not compare or analyze the supporting documentation for the annual physical inventories conducted by the Department in 2005 and 2006 with the inventory information recorded in ILMS to determine whether discrepancies existed or reconciliations were conducted. However, OIG did review the 2007 annual physical inventory documents for the four bureaus audited and found that several of the laptop computers that the bureaus had identified as missing were also missing in OIG's sample but had not been recorded as such in ILMS. During its physical verification of laptop computers, OIG found four laptop computers that the bureaus had listed as missing in their 2007 annual inventories. These four laptops were also in OIG's sample group.

Classified Laptop Description Not Captured in ILMS

OIG determined that there was no requirement or code used to identify computers designated as "classified" in ILMS. Because ILMS was not a feasible source to identify classified laptop computers, OIG sent a data call on October 3, 2007, to the executive directors for all Department bureaus and offices and requested each to provide a listing of its classified laptop computers located in the Washington, DC, area. To identify discrepancies, OIG compared the information received with the ILMS domestic inventory listing for all Department organizations, including the four bureaus selected for the audit. For each of the four bureaus, OIG physically verified laptops located by Department officials and brought to a central review area. OIG also discovered more by manually inspecting other laptops labeled "Secret" that were located in the review areas. Table 9 summarizes the methods used to identify the classified laptops included in the sample group.

Table 9. Methods Used to Identify Classified Laptops Included in Sample Group

CLASSIFIED LAPTOP COMPUTERS				
Bureau	Identified From ILMS Listing	Identified by Bureau in Data Call	Identified by OIG During Manual Search	Total
DS	0	0	0	0
INR	0	8	0	8
IRM	0	1	2	3
OBO	0	0	3	3
Total	**0**	**9**	**5**	**14**
Percentage	0%	64%	36%	100%

OIG received varying responses from Department officials about why the laptop classification designation was not being captured in ILMS. For example, INR officials stated that they do not record information for their classified laptop computers into ILMS Asset Management because INR considers the information to be classified. Instead, INR keeps separate internal records and an inventory of its classified laptop computers. OIG did not test these internal records. Because ILMS is not being used at all or to capture identifiers for classified laptop computers, inventory accountability and visibility over this security-sensitive equipment are fractured.

Property Not Removed From Official Inventory

OIG's verification determined that 57 (17 percent) of the 334 laptop computers had been disposed of. The laptops were either transferred to excess property or donated to schools. None of the 57 were identified by Department officials as a classified laptop. Table 10 summarizes the results of OIG's verification of documentation required for laptop disposals.

Table 10. Disposed of Unclassified and SBU Laptop Computers

DISPOSED LAPTOP COMPUTERS			
Bureau	Number Excessed per Forms DS-1882 and CEPO-1	Number Donated to Schools per Forms DS-584* and DS-1882	Total
DS	26	0	26
INR	0	0	0
IRM	21	0	21
OBO	4	6	10
Total	**51**	**6**	**57**
Percentage	89%	11%	100%

*This form, Nonexpendable Property Transaction, is used to transfer property for another use, such as transferring it to a field office or transferring it as a donation to a school. This form is not used to report excess property, which is listed on Form DS-1882, Domestic Property Excess. The PCOs use the Centralized Excess Property Operations (CEPO-1) form to update the bureaus' property records after verification is performed.

The Department has established procedures to process disposable property and to update ILMS. The ACO must report unneeded property to the PCO. If only one custodial officer has been designated, the property is reported to the APO. Any property not reassigned for further utilization is reported on the ILMS Asset Management application as "excess" and, as such, is available for screening/transfer within the Department for a 10-day period before being reported to the Property Management (PM) staff within A/LM. Certain types of property[18] must be inspected for classified material before removal, and Form DS-586, Turn-In Property Inspection Certificate, must be signed by the employee to whom the property is assigned. The ACO, unit security officer, or ISSO also inspects the equipment and signs Form DS-586. To dispose of excess property, the ACO must complete Form DS-1882, U.S. Department of State, Domestic Property Excess, and forward it to the PCO.[19] After Form DS-1882 has been completed, the PCO faxes a copy to the PM staff. Upon receipt of the form, the PM staff assigns a USDA CEPO number to Form DS-1882 and notifies the bureau contact person and the PCO of this number via e-mail.

The USDA acquires and transfers title of federal excess personal property to certain eligible institutions in support of research, educational, technical, and scientific activities or for related programs. After ensuring the completeness and accuracy of DS-1882, the PM staff completes USDA Form CEPO-1, Report of Excess Property, and attaches it to Form DS-1882. These documents are submitted to USDA to report excess property. CEPO personnel from USDA sign Form CEPO-1 at the time the property is picked up and leave a signed copy with the dock manager. PCOs should retrieve a copy of this form to update their records. The PCOs update ILMS with the information about the excess property.

Federal agencies may donate computer equipment that is no longer needed to educational organizations. Unclassified computer hardware declared as excess property that can no longer be used within the Department should be donated to schools or educational nonprofit organizations in accordance with the Computer for Learning

[18] According to 14 FAH-1 H-721, 1(a), "Classified Material Inspection," this property includes data or word processing and ADP equipment, which must be cleared of any sensitive information stored in memory.

[19] Excess property that is removed by USDA personnel is listed on Form DS-1882 rather than Form DS-584, Nonexpendable Property Transaction.

Program, Executive Order 12999. The controlling Department bureau or domestic field office must attempt to identify an appropriate donee prior to following routine disposal procedures.

Department officials provided the proper documentation to support the disposition of all 57 laptop computers that OIG had reviewed and had determined to be acceptable. This documentation had been properly prepared prior to OIG's final verification. However, these items had not been properly removed from ILMS at the time of OIG's inventory sample selection and initial verification, thereby misstating the active inventory. Better enforcement of these requirements would improve the accuracy of the status of ILMS' inventory.

Recommendation 17: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Bureau Response and OIG Reply

In its response to the draft report, DS requested that OIG modify the recommendation to include additional requirements that the inventory process should also include provisions to capture equipment when "received, excessed, or moved" on an ongoing basis.

OIG believes that the recommendation as stated covers incidents of excessed or moved equipment as changes to record during the annual inventory. Current ILMS inventory guidance stated in 14 FAM 426-428 already requires that changes to inventory be made as they occur, but OIG did not find bureau-level processes to implement that requirement. Furthermore, OIG did not review equipment acquisitions and, as such, does not have an opinion or recommendation regarding the receipt of equipment. Therefore, OIG did not modify this recommendation.

On the basis of DS' inferred concurrence with this recommendation, OIG considers the recommendation resolved. The recommendation can be closed when OIG receives documentation from DS documenting inventory process improvements implemented to address the requirements of the recommendation.

Recommendation 18: OIG recommends that the Assistant Secretary for Intelligence and Research ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Bureau Response and OIG Reply

In its response to the draft report, INR stated, for recommendations 16-19, that it believes that the A Bureau is "the best entity to 'develop a policy and process to validate and verify that ILMS is updated when the inventory changes after an annual physical inventory is conducted.'" INR further stated, "This would ensure that a Department-wide policy and process is put in place that would ensure uniform treatment of inventory changes."

OIG encourages INR to coordinate with the A Bureau to address this recommendation. Current ILMS inventory guidance contained in 14 FAM 425-428 already requires that changes to inventory be made as they occur, but OIG did not find bureau-level processes to implement that requirement. On the basis of INR's response, OIG considers the recommendation unresolved. The recommendation can be resolved when INR identifies actions it will take to address this recommendation and closed when OIG receives documentation from INR documenting inventory process improvements implemented to address the requirements of the recommendation.

Recommendation 19: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Bureau Response and OIG Reply

In its response to the draft report, OBO stated that the distribution and recovery process is now "rigorously managed and maintained by the ISSO" and that the process uses "the DOS [Department of State] standard Mobile Computing form set, DS-7642 for tracking and management." According to the response, the form set includes "the DS-584 'Nonexpendable Property Transaction' form," which it says is for "recording distributions and turn-ins." OBO also included a copy of its "rewritten Standard Operating Procedures for its laptop loan program," stating that it had reissued the document on December 30, 2008.

On the basis of OBO's response, including its revised Standard Operating Procedures (SOP), OIG considers this recommendation resolved. However, in reviewing OBO's SOP, OIG noted that while the SOP addresses OBO's laptop loan program and encryption configuration requirements, it does not address updating ILMS after the annual physical inventory is conducted or when laptop computers are identified as missing or lost. This recommendation can be closed when OIG receives a description of the ISSO's responsibilities and a copy of the OBO process that has been implemented to validate and verify that ILMS is updated on an ongoing basis when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Recommendation 20: OIG recommends that the Bureau of Administration, in coordination with the Chief Information Officer, ensure, at the Bureau of Information Resource Management, that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Bureau Response and OIG Reply

In its response to the draft report, IRM requested that the recommendation be modified to also be directed to the A Bureau. IRM also stated that ILMS "may not necessarily be the best or proper system for recording and tracking laptop computers." IRM "suggests" that the recommendation be modified to add an alternative system to ILMS.

OIG encourages IRM to coordinate with the A Bureau to address this recommendation. On the basis of IRM's response, OIG considers this recommendation unresolved. Current annual physical inventory and reconciliation guidance contained in 14 FAM 429 requires bureaus to report the results of the inventories to A/LM on the annual inventory certifications. Therefore, OIG has revised the recommendation and redirected responsibility to the A Bureau, in coordination with the CIO, for developing a process to validate and verify that ILMS is updated when the inventory changes after the annual physical inventory, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment. OIG is addressing its recommendation only with respect to ILMS, the official inventory system, and obtained no information regarding an alternative system during the audit.

The recommendation can be resolved when IRM and the A Bureau identify actions they will take to address the requirements of the recommendation and can be closed when IRM and the A Bureau provide OIG with documentation of the process developed to update the inventory after the annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Recommendation 21: OIG recommends that the Assistant Secretary for Administration ensure that the Office of Logistics Management develops standard asset codes for the Integrated Logistics Management System to specifically identify classified, unclassified, and sensitive but unclassified laptop computers; disseminates these codes prior to the next Department of State-wide annual inventory; and defines or eliminates existing codes that are ambiguous.

Bureaus' Responses and OIG Reply

In its response to the draft report, the A Bureau concurred with the recommendation and stated that A/LM had completed the analysis on the numerous asset classes associated with notebooks/laptops in ILMS Asset Management. The A Bureau included a copy of the ILMS Change Request Form (see the Exhibit to Appendix E) with its response, stating that the form had been submitted to update the ILMS Notebook/Laptop Asset Classes in accordance with the recommendation specifically to identify asset codes for classified, unclassified, and SBU laptop computers.

OIG considers the actions taken by the A Bureau to be responsive to this recommendation, and on the basis of its response, OIG considers the recommendation resolved. The Change Request Form provided four "Detailed Requirements of Change:" renaming asset class 25108 (from "'CPU, Notebook/Laptop' to 'CPU, Notebook/ Laptop, Unclassified;'" adding two new asset classes for Classified and Sensitive But Unclassified Laptops; mapping six existing asset classes to asset class 25108; and removing these six asset classes from the asset class table.

The recommendation can be closed when OIG receives verification that the A Bureau has received approval for this Change Request and has disseminated these asset code changes prior to the next Department of State-wide annual inventory.

In its response to the draft report, INR did not agree with this recommendation, stating that it is "uncomfortable identifying classified equipment in an unclassified inventory system resident on an open network." OIG encourages INR to discuss its concerns with the A Bureau for an alternative mitigating control to fulfill the intent of this recommendation to capture an accurate and official inventory of all laptop computers.

Recommendation 22: OIG recommends that the Chief Information Officer issue a Department of State-wide notice to remind personnel of laptop inventory accountability responsibilities and requirements.

Bureau Response and OIG Reply

In its response to the draft report, IRM did not address this recommendation; therefore, the recommendation is unresolved.

Laptop Computer Security Awareness Training Not Centrally Tracked

According to documentation provided to OIG, DS has conducted biweekly Unclassified/SBU Laptop Cyber Security Awareness Briefings since July 2007 to address laptop computer security responsibilities for users. These briefings cover the requirements for protecting Department-owned laptop computers and the data stored on them. However, the Department did not have a centralized tracking system to record those individuals who had taken the briefings. Officials with each of the four bureaus included in this audit stated that the respective bureaus maintained their own training participation records. In a separate 2008 review of the Department's overall security awareness training program as it relates to the Federal Information Security Management Act,[20] OIG noted this same decentralized condition. Without centralized tracking for all forms of information security training, including for laptop computer users, the Department cannot ensure that all personnel are receiving required training, thus obtaining a comprehensive awareness of individual security responsibilities. This increases the risk of unauthorized access, use, disruption, disclosure, modification, or destruction of information.

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, dated November 30, 2000, requires that each agency ensure that all indi-

[20] Review of the Information Security Program at the Department of State (AUD/IT-08-36, Oct. 2008).

viduals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. It states:

> Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.

In addition, NIST SP 800-18, revision 1, "Guide for Developing Security Plans for Federal Information Systems," section 1.8, "Rules of Behavior," issued in February 2006, states that rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. It states:

> The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior. Electronic signatures are acceptable for use in acknowledging the rules of behavior. . .
>
> When developing the rules of behavior . . . the intent is to make all users accountable for their actions by acknowledging that they have read, understand, and agree to abide by the rules of behavior.

All users are required to have the Unclassified/SBU Laptop Cyber Security Awareness Briefing before being issued a laptop computer, which includes information on identifying the risks inherent in information systems, including laptop computers. Although this briefing is mandatory, the Department did not have a centralized tracking mechanism to determine whether the user had taken the briefing. Furthermore, OIG was not able to obtain complete training records for any of the four bureaus audited. For example, officials in the ISSO's office in INR stated that it was the employees' responsibility to complete and document the required training.

OIG discussed the security briefing process with officials in the CISO's office, who stated that the Department did not have a centralized tracking system for those individuals who had taken the briefings. OIG also discussed how participation and completion of this briefing are tracked with other bureau officials, such as the OBO ISSO and officials within the Chief Technology Office in DS and in INR. These officials also stated that there was no central tracking mechanism and that each bureau kept its own records. The briefing acknowledgement forms that the users sign stated that individuals are responsible for keeping a copy for their records and for providing a copy of the signed form to their ISSO as confirmation that they had attended the session. The form is signed by the briefer (usually a DS employee) and the employee.

Department officials were aware of the requirement that laptop computer users were required to receive a briefing, including the guidance contained in 08 State Telegram 032537, ALDAC, dated March 28, 2008, for the posts' laptop computer inventory personnel that explained requirements such as the one that employees needed to take the briefings. The guidance told the posts to maintain records of those individuals who took the briefings, but it did not require the Department to track the information centrally because it delegated this responsibility to each post (and bureau or office). OIG reviewed the records of the laptop cyber security awareness training for two bureaus, DS and OBO, but was unable to obtain a complete list of training for any of the four bureaus audited. Bureau officials advised us that they did not keep complete records of those employees who had taken the training. Because the lists were incomplete, Department employees may not have received guidance issued by NIST and OMB apprising them of their responsibilities when using a laptop computer. Not having the guidance increases the risk of unauthorized access, use, disruption, disclosure, modification, or destruction of information.

Recommendation 23: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that the Office of Computer Security develops a Department of State-wide centralized method to track participation in the Unclassified/SBU Laptop Cyber Security Awareness Briefing.

Bureau Response and OIG Reply

In its response to the draft report, DS requested that OIG modify the report to show the specific title of the laptop training to Laptop Cyber Security Awareness Briefings and that it conducts this briefing biweekly rather than quarterly. DS also stated that DS/SI/CS keeps records of all users who received the laptop briefing given by its Enterprise Technology Policy & Awareness Division. Further, DS stated that the recommendation "incorrectly references a finding relating to the Annual Cyber Security Awareness Training, which is not a part of this audit" and that the recommendation should be changed to "reflect the tracking of the 'Laptop Computer Security Awareness Briefing.'"

On the basis of DS's response, OIG has modified the recommendation to correct the title of the laptop briefing covered in this audit. OIG considers DS' response that DS/SI/CS retains participation records as responsive to the recommendation. Therefore, OIG considers the recommendation resolved and will close it when DS provides documentation to support that the centralization of participation records Department-wide resides with DS/SI/CS.

Additionally, OIG has modified the final report to address the frequency with which DS conducts its briefings. During the audit, OIG was provided with documentation by DS to support that biweekly briefings were held. OIG misstated in its draft report that the briefings were held quarterly and not biweekly based on the quarterly issuance of the briefing schedule rather than the biweekly briefing sessions. Therefore, OIG has modified the final report accordingly.

In its response to the draft report, IRM also stated that DS/SI/CS keeps the attendance records on users who receive the laptop security briefing. However, during the audit, OIG was informed by IRM's Chief for the Desktop Systems Support Division (now Desktop Support Services division) that the records for IRM users who take the briefing were maintained by IRM. OIG encourages IRM to coordinate and verify with DS where the laptop security briefing participation records should be maintained.

LIST OF RECOMMENDATIONS

Recommendation 1: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a thorough search is made to locate its missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain personally identifiable information or other sensitive agency information, appropriate notifications should be made.

Recommendation 2: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a thorough search is made to locate its missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain personally identifiable information or other sensitive agency information, appropriate notifications should be made.

Recommendation 3: OIG recommends that the Chief Information Officer ensure that a thorough search is made to locate the Bureau of Information Resource Management's missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain personally identifiable information or other sensitive agency information, appropriate notifications should be made.

Recommendation 4: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

Recommendation 5: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

Recommendation 6: OIG recommends that the Chief Information Officer ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

Recommendation 7: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

Recommendation 8: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

Recommendation 9: OIG recommends that the Chief Information Officer ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

Recommendation 10: OIG recommends that the Assistant Secretary for Diplomatic Security, in coordination with the Chief Information Officer, ensure that 12 FAM 684, "Portable Computers" (or other numbering sequence), is finalized and published.

Recommendation 11: OIG recommends that the Chief Information Officer, in coordination with the Assistant Secretary for Diplomatic Security, issue a Department of State-wide mandate requiring that appropriate encryption be acquired and installed on all classified laptop computers, in accordance with specified Department policy, as soon as possible but no later than September 30, 2009.

Recommendation 12: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that all of its Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Recommendation 13: OIG recommends that the Assistant Secretary for Intelligence and Research ensure that all of its Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Recommendation 14: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that all of its Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Recommendation 15: OIG recommends that the Chief Information Officer ensure that all of the Department of State-owned classified, unclassified, and sensitive but unclassified laptop computers within the Bureau of Information Resource Management are physically inspected and have appropriate encryption installed as soon as possible but no later than September 30, 2009.

Recommendation 16: OIG recommends that the Chief Information Officer ensure that a Department of State-wide process is developed and implemented so that newly acquired laptop computers are not issued to users until appropriate encryption is installed in accordance with the sensitivity and security level for the use of each laptop computer.

Recommendation 17: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Recommendation 18: OIG recommends that the Assistant Secretary for Intelligence and Research ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Recommendation 19: OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Recommendation 20: OIG recommends that the Bureau of Administration, in coordination with the Chief Information Officer, ensure, at the Bureau of Information Resource Management, that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

Recommendation 21: OIG recommends that the Assistant Secretary for Administration ensure that the Office of Logistics Management develops standard asset codes for the Integrated Logistics Management System to specifically identify classified, unclassified, and sensitive but unclassified laptop computers; disseminates these codes prior to the next Department of State-wide annual inventory; and defines or eliminates existing codes that are ambiguous.

Recommendation 22: OIG recommends that the Chief Information Officer issue a Department of State-wide notice to remind personnel of laptop inventory accountability responsibilities and requirements.

Recommendation 23: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that the Office of Computer Security develops a Department of State-wide centralized method to track participation in the Unclassified/SBU Laptop Cyber Security Awareness Briefing.

ABBREVIATIONS

A Bureau	Bureau of Administration
ACO	Area Custodial Officer
AES	Advanced Encryption Standard
A/LM	Bureau of Administration, Office of Logistics Management
A/LM/PMP/BA/PM	Property Management Branch
ALDAC	All Diplomatic and Consular Posts
APO	Accountable Property Officer
CEPO	Centralized Excess Property Operations
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CNSS	Committee for National Security Systems
COMSEC	Communication Security
Department	Department of State
DoD	Department of Defense
DS	Bureau of Diplomatic Security
DS/SI/CS	Office of Computer Security
FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
FIPS	Federal Information Processing Standards
ILMS	Integrated Logistics Management System
INR	Bureau of Intelligence and Research
IRM	Bureau of Information Resource Management
ISSO	Information Systems Security Officer
MCSC	Management Control Steering Committee

NEPA	Nonexpendable Property Application
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OBO	Bureau of Overseas Buildings Operations
OBO/RM/EX/IRM	Office of Resource Management, Office of the Executive Director, Information Resource Management Division
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCO	Principal Custodial Officer
PII	Personally identifiable information
PM	Property Management
SAT	Senior Assessment Team
SOP	Standard Operating Procedure
SBU	Sensitive but Unclassified
US-CERT	United States Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture

APPENDIX A

Department Mandates for Implementing Inventory and Security Controls Over Department Laptop Computers

The Department of State issued directives in 2007 and 2008 regarding the safeguarding of information on laptop computers, including requirements for encrypting hard drives. This guidance was issued in the form of Department telegrams to “All Diplomatic and Consular” posts, also known as an ALDAC; memoranda; and other notices. This information is summarized in Table 1 of this appendix.

Table 1. Telegrams, Memoranda, and Other Notices for Implementing Inventory and Security Controls.

07 State Telegram 058726 to All Diplomatic and Consular Posts Collective “Protection of Personally Identifiable Information (PII) on Laptops”	05/01/07	This ALDAC is to mandate that all Department laptop hard disks be encrypted. This action is necessitated by a number of events and activities concerning the protection of Personally Identifiable Information (PII)…and other sensitive agency data. This guidance will be one of a series of notices on responsibilities related to handling PII and other sensitive agency data on other media. References: OMB Memoranda M-06-19, M-06-16, and M-06-15	Multiple technical solutions are available for encrypting laptop hard disks so this policy change can be readily implemented based on the timelines set forth below. Solutions refer to: a) Older Laptops (SecureDoc/available), b) New Laptops (Vista encryption as standard feature/needs user activation), and c) New and Old Laptops (pending solution for “data at rest”).

Document Number and Title	Document Date	Purpose/Summary	Action Required
Action Memorandum for All Executive Officers "Protection of Sensitive Information on Laptops"	05/04/07	Effective immediately, all Department laptop hard disks must be encrypted to ensure the security of PII and other sensitive agency data. Attachment, "Laptop Encryption Solutions." References: OMB Memorandum M-06-19 and State 058726 ALDAC	Older laptop solution: SecureDoc Disk Encryption should be in place by bureaus and posts by the end of the current fiscal year (09/30/07) unless adopting one of the other solutions. New laptop solution: Users should consider Vista's encryption feature [which requires user activation] immediately. New and old laptop solution (pending): When available, information will be provided for protecting "data at rest," including multiple tools for encrypting laptop hard drives.
Department Notice – (recurring) "Unclassified/SBU Laptop Cyber Security Awareness Briefings" These notices were reissued every 2 or 3 months with updated briefing schedules to remind employees of the briefing schedule, i.e., July, September, and October 2007 and January and April 2008.	07/13/07 and recurring	All Department users who have been issued a Department unclassified/ SBU laptop must attend a laptop briefing to ensure that they are aware of their cyber security responsibilities. Given that there are new laptop requirements, all laptop users who had previously been briefed are required to attend.	The briefings cover the requirements for protecting Department-owned laptops, as well as requirements for protecting Department data stored on personally owned laptops.

Document Number and Title	Document Date	Purpose/Summary	Action Required
IRM Notice Number 2007-04 “Protecting Sensitive Information on Mobile Computing Devices” Note: This notice is applicable only to the Bureau of Information Resource Management	11/06/07	This notice defines procedures for requesting, obtaining, using, securing, and returning a government laptop issued by IRM to protect Department information. All employees must understand their responsibilities as a laptop user, including incident response, by attending the DS Unclassified/SBU Laptop Cyber Security Awareness Briefing. Reference: OMB Memorandum M-07-16	Guidance is provided relating to: • Incidents • Disposal • Encryption • Responsibilities • General Guidance • Inventory & Inspection • Custody and Handling of Laptops
07 State Telegram 167072 to All Diplomatic and Consular Posts Collective and Department Notice Number 2007_12_091 “Protecting Sensitive Department Information on Mobile Computing Devices and Media”	12/14/07 12/17/07	Describes mandatory procedures for protecting sensitive Department information on all existing Department of State mobile computing devices and media. Reference: OMB Memorandum M-07-16	Guidance is provided for the following actions that are to be taken to comply with OMB M-07-16: • Inventory Management • Encryption • Awareness • Mobile Computing Device and Media Tracking

Document Number and Title	Document Date	Purpose/Summary	Action Required
08 State Telegram 032537 to All Diplomatic and Consular Posts Collective “Unclassified and Sensitive But Unclassified Laptop Inventory and Encryption Responsibilities”	03/28/08	This ALDAC is for distribution to all holders of State Department owned unclassified and sensitive but unclassified laptops. In order to protect unclassified, PII, and sensitive data on Department-owned laptops, Information Management Officers (IMO) have responsibility for inventory and security of all unclassified and SBU laptops at their site. This is an action ALDAC that provides instructions for IMOs and information systems security officers (ISSO) regarding laptop inventory and encryption activities.	All posts are required to take the actions listed in this ALDAC regarding: • Review and validation of site inventory of existing laptops • Record and report missing, lost, stolen, excessed or destroyed laptops • Reduce number of laptops to minimum necessary to accomplish mission • Keep records of the names of individual laptop users who receive the required annual DS Unclassified/SBU Laptop Cyber Security Awareness Briefing • Laptop users must immediately report to IMO or ISSO if they suspect theft/loss, loss, loss of control, loss of media, tampering, abnormal functionality, or any other suspicious activity • Laptop users must immediately report all suspected or confirmed PII loss or theft to CIRT • All laptops must be encrypted according to Department guidance

Document Number and Title	Document Date	Purpose/Summary	Action Required
08 State Telegram 034472 to All Diplomatic and Consular Posts Collective "Department Support of ProtectDrive: Encryption for Laptops"	04/3/08	SafeNet's ProtectDrive encryption software is now available for download. It is authorized for use only on mobile devices owned by the Department of State. This cable focuses on encrypting data on laptops. The use of other FIPS 140-2 compliant encryption software, such as SecureDocs, is authorized. IRM strongly encourages the use of ProtectDrive, which is centrally purchased, rather than renewing licenses or purchasing new licenses for alternative encryption software. IRM will provide technical assistance only for ProtectDrive. References: 08 State Telegram 032537, 07 State Telegram 033298 ("Hard Drive Destruction-Computer Security Policy," 03/15/07), 07 State Telegram 058726, and 07 State Telegram 167072	Availability of encryption software solution. This software will encrypt laptops in accordance with 08 State Telegram 032537 and 07 State Telegram 167072.
IRM Notice Number 2008-11 Subject: IRM Laptop Program Note: This notice is applicable only to the Bureau of Information Resource Management	04/14/08	The Mobile Computing Branch of IRM's Messaging Systems Office's Email Division will assume responsibility for consolidation and management of IRM's Laptop Program. Users are asked to coordinate all laptop activities with the Mobile Computing (MC) Branch. MC will maintain a pool of laptops that can be checked out for use by users. The objective of this Program will be to maintain up-to-date Security, Accountability and Traceability for IRM's laptops. All laptops must be encrypted. Reference: 07 State Telegram 058726	Effective April 14, 2008, for all IRM employees. All laptops older than 3 years are not eligible for this program and must be excessed in accordance with existing excess property guidance.

Document Number and Title	Document Date	Purpose/Summary	Action Required
Action Memorandum for Assistant Secretaries "Laptop Protection Responsibilities"	04/21/08	Recent thefts and losses of federal government laptops lacking adequate protection have garnered Congressional attention. In addition to PII, Department-owned laptops are likely to contain other sensitive data. Central to the protection of information on the Department's laptops are careful control of the laptop inventory, laptop user awareness training, and encryption of the laptop. References: 07 State Telegram 58726, 07 State Telegram 167072, 08 State Telegram 032537, and 08 State Telegram 034472	Remind of prior ALDACs issued and restates the actions required under 08 State Telegram 032537 for all unclassified and SBU Department-owned laptops. Confirmation of full compliance due by May 31, 2008.
08 State Telegram 064226 to All Diplomatic and Consular Posts Collective "Reminder: Unclassified and Sensitive But Unclassified Laptop Encryption Responsibilities"	06/13/08	The ALDAC is a reminder to bureaus and posts that all Department-owned unclassified and sensitive but unclassified laptops must be encrypted. References: 08 State Telegram 032537, 08 State Telegram 034472, 07 State Telegram 0001771 (regarding the procedure for requesting exceptions to cyber security policy, 01/08/07), and Department Notice 2007_01_024, 01/08/07)	IMOs and ISSOs requested to ensure that all Department-owned laptops are encrypted and compliance reported by July 1, 2008, to a designated IRM laptop survey web site.

APPENDIX B

Domestic Laptop Computers on ILMS Asset Management Report as of September 30, 2007

Bureau/Office	Total	Percentage
Bureau of Information Resource Management (IRM)	656	16.01%
Office of the Under Secretary for Management, Foreign Service Institute (M/FSI)	623	15.21%
Bureau of Diplomatic Security (DS)[a]	582	14.21%
Bureau of Overseas Buildings Operations (OBO)[b]	400	9.76%
Bureau of Human Resources (HR)	358	8.74%
Office of the Secretary, Executive Secretariat (S/ES)	271	6.61%
Bureau of Consular Affairs (CA)	264	6.44%
Bureau of Administration (ADM)	188	4.59%
Bureau of Resource Management (RM)	68	1.66%
Bureau of European and Eurasian Affairs (EUR)	64	1.56%
Bureau of East Asian and Pacific Affairs (EAP)	63	1.54%
Florida Regional Center in Fort Lauderdale (FRCFL)[c]	62	1.51%
Bureau of Public Affairs (PA)	61	1.49%
Charleston Financial Service Center (CFSC)[d]	50	1.22%
Office of International Security and Nonproliferation[e]	48	1.17%
Office of Inspector General (OIG)	43	1.05%
Bureau of Intelligence and Research (INR)	41	1.00%
Bureau of International Narcotics and Law Enforcement Affairs (INL)	36	0.88%
Bureau of Economic and Business Affairs (EB)[f]	31	0.76%
Bureau of Oceans and International Environmental Affairs (OES)	31	0.76%
Bureau of International Security and Nonproliferation (NEA)	29	0.71%
Office of Legal Adviser (L)	26	0.63%
Bureau of Political-Military Affairs (PRM)	22	0.54%
Bureau of International Organization Affairs (IOA)	19	0.46%

Office of the U.S. Representative to the United Nations, New York (USUNY)	14	0.34%
Bureau of African Affairs (AF)	13	0.32%
International Joint Commission (IJC)	10	0.24%
In Warehouses (undistributed inventory, located in Springfield, VA)	8	0.20%
Bureau of Public Affairs, Office of Strategic Communications and Planning (PA/SCP)	6	0.15%
International Boundary Commission (IBWC)	5	0.12%
Bureau of Western Hemisphere Affairs (WHA)	4	0.10%
Office of Medical Services (MED)	1	0.02%
TOTAL LAPTOP COMPUTERS PER ILMS	**4,097**	**100.00%**
Laptop computers for the four bureaus/offices in OIG's audit (DS, IRM, INR, OBO)	1,679	40.98%
Laptop computers in the Washington, DC, metropolitan area for the four bureaus/offices in OIG's audit (DS, IRM, INR, OBO)	1,612	39.27%

a Includes 67 items for DS located outside the Washington, DC, area not included in OIG's sample.

b Includes 17 items for the business unit OBO and 383 items for the business unit OBO/IM.

c Now the Florida Regional Information Management Center, Fort Lauderdale (RIMC).

d Now the Global Financial Services (GFS) in Charleston.

e Now the Bureau of International Security and Nonproliferation (ISN).

f Now the Bureau of Economic, Energy, and Business Affairs (EEB).

APPENDIX C

Sensitive But Unclassified

DS Comments to Office of the Inspector General Report AUD/SI-09-15

Title:

DS Comments to DRAFT Report for Audit of Property Accountability Inventory Controls and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington DC Metropolitan Area

Comments & Technical Corrections

1. "The Department does not have an accurate accounting for and has not encrypted all of its classified and unclassified laptop computers in the Washington, DC, area for the four bureaus included in OIG's audit." [Page 1]

DS Comment: DS does not agree with the OIG's interpretation that OMB mandated encryption of classified laptops. Both OMB M-06-16 and M-07-16 address only NIST Standards; however NIST does not have governing authority over standards for national security systems, i.e. classified laptops.

The Committee for National Security Systems (CNSS) is the governing body for policy relating to national security systems. CNSS does not require encryption. However, if encryption is used then CNSS requires that the encryption be NSA approved. The only currently available NSA approved encryption product for use with a laptop is an external, in-line COMSEC device. CNSS policy not requiring encryption is based in part on the use of alternative physical protection measures, e.g., storage in classified containers, shipment via classified pouch, and requirements to only process classified information in approved, secure facilities. This same philosophy is reflected in CNSS's most current draft CNSS No. 1253 on Security Controls, i.e., "At the discretion of the information owner the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical protection measures." The lack of CNSS standards in both documents indicate that OMB never intended to address the protection of PII on classified systems.

This is illustrated by language in :

1) OMB M-06-16 which states:

"The National Institute of Standards and Technology (NIST) provided a checklist for the protection of remote information. The intent of implementing the checklist is to compensate for the lack of physical security controls when the information is removed from, or accessed from outside the agency location. In addition to the checklist I am recommending encrypting all data on mobile computers…,"

2) OMB M07-16. Page 7 is where the encryption requirement is derived. It states:

"While agencies continue to be responsible for implementing all requirements of law and policy, below are five requirements agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, e.g., law enforcement information, etc.

Encryption. Encrypt using NIST certified crypto logical modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or senior-level individual he/she may designate in writing."

By its own admission on page 6 of the subject draft report, the OIG "did not review the effectiveness of security controls applied to laptop computers to determine whether these controls protected the information stored, processed and transmitted…." As the Department already has in place physical security controls for classified information and equipment, including laptops, when the information is removed from, the agency location, does not allow accessed from outside, and CNSS is the governing authority for the protection of national security systems, DS does not consider this recommendation to be valid. Therefore, DS requests that all mention of encryption for classified laptops be removed from this report.

2. *"Apart from the classified laptop computers included in the sample group that OIG identified through the data call and manually, an additional 67 classified laptops were discovered during the on-site searches, including 28 that belonged to bureaus not included in OIG's sample group. Due to the sensitive nature of information that may be stored on classified laptop computers, OIG also tested the additional 39 laptops associated with the four bureaus in its sample group to determine whether each had been recorded in ILMS and installed with encryption software. Of the 39 laptops, 33 were not recorded in ILMS. Only five (or 12 percent) of the 39 had been encrypted, as illustrated in Table 6. Of the 39, OIG found that 31 had been reported in response to its data call. " [Page17]*

DS Comment: The report states that OIG found encryption software on some classified laptops that were inspected, which DS considers a classified information security issue as encryption for classified systems require additional COMSEC equipment, i.e. hardware that is keyed with COMSEC material/keys, not software installation.

3. *“Since July 2007, DS has conducted quarterly Unclassified/SBU Laptop Cyber Security Awareness Briefings to address laptop computer security responsibilities for users, including reporting a missing, lost, or stolen laptop. These briefings cover the requirements for protecting Department-owned laptop computers and the data stored on them. However, the Department did not have a centralized tracking system to record those individuals who had taken the briefings. Officials in each of the four bureaus included in this audit said that the respective bureaus maintained their own training participation records.” [Page 2]*

DS Comment: Since DS conducts Laptop Cyber Security Awareness Briefings bi-weekly, not quarterly. DS asks that the word “quarterly” be replaced with “bi-weekly” at the bottom of page 2 of the subject draft report, which would then read: “Since July 2007, DS has conducted bi-weekly Unclassified/SBU Laptop Cyber Security Awareness Briefings to address laptop computer security responsibilities for users, including reporting a missing, lost, or stolen laptop.” Additionally on page 23 of the subject draft report DS asks that the word “quarterly” be replaced with the word “biweekly”, which would then read: “Since July 2007, DS has conducted bi-weekly Unclassified/SBU Laptop Cyber Security Awareness Briefings to address laptop computer security responsibilities for users.”

4. *“14 FAM 427.1, “Nonexpendable Property,” requires the ACO to report unneeded property to the PCO, including any property not reassigned for further use. Such property is to be reported on the ILMS Asset Management application as “excess.” The office must use the appropriate forms, including the ILMS Asset Management Excess Property Report and DS-586, Turn-In Property Inspection Certification (if needed), and the office must then place a U.S. Department of Agriculture (USDA) Centralized Excess Property Operations (CEPO) number on Form DS 586 or DS-1882, Domestic Property Excess, as described in the Foreign Affairs Handbook (FAH), 14–FAH-1, H-721, “Reporting to the Principal Custodial Officer.” The Property Management staff forwards the ILMS Asset Management Excess Property Report to USDA’s CEPO to request pickup of the property.” [Page 5]*

DS Comment: On page 5 of the subject draft report is a citation of Property Management requirements, especially 14 FAM 427.1. Implication is that excess laptops are subject to being donated, etc. DS believes it would be worthwhile for the OIG to include the following citation, as it regards hard drives, to put this information into perspective.

14 FAM 427.1.h. Nonexpendable Property. Unclassified computer hardware, declared as excess property that can no longer be used within the Department should be donated to schools or educational nonprofit organizations, especially in Federal empowerment zones and enterprise communities, in accordance with the Computer for Learning Program, Executive Order 12999. The controlling Department bureau or domestic field office must attempt to identify an appropriate donee, prior to following routine disposal procedures. (Contact A/LM/PMP/BA/PM staff for current procedures.) Nonvolatile memory (e.g., hard drives, portable computer hard drives) that has been used to process Department data must not be donated. Per NIST SP 800-88, these drives must be degaussed or destroyed before being released from the Department's control.

5. *"OIG also identified required training related to laptop computer security awareness and reviewed relevant records available for DS, OBO, and IRM to determine how participation in this training was tracked. OIG was not able to obtain complete training records for any of the four bureaus audited." [Page 7]*

DS Comment: DS/SI/CS keeps records on all users who received the laptop briefing given by its Awareness branch.

6. *"Given the government-wide importance and attention placed on protecting PII and sensitive agency information, more aggressive and consistent action is needed by DS, INR, IRM, and OBO to enforce the various internal and federal requirements relating to laptop computer inventory and encryption responsibilities. " [Page 3]*

DS Comment: We ask that you add "A/LM" to the phrase "more aggressive and consistent action is needed by A/LM, DS, INR, IRM…….to enforce inventory and encryption responsibilities……"

7. *"According to DS's Special Assistant to the Senior Coordinator for Security Infrastructure, there was no telegram issued to address classified laptop computers. The Special Assistant stated: " [Page 13]*

DS Comment: Please note that the Senior Coordinator for Security Infrastructure for Diplomatic Security has two Special Assistants. Please change the sentence to read: "According to one of DS's Special Assistants to the Senior Coordinator for Security Infrastructure……"

8. *"Recommendation 22: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that the Office of Computer Security develops a Department of State-wide centralized method to track participation in the annual cyber security awareness training." [Page 25]*

DS Comment: Recommendation 22 incorrectly references a finding relating to the Annual Cyber Security Awareness Training, which is not a part of this audit and should be changed to reflect the tracking of the "Laptop Computer Security Awareness Briefing," i.e., "OIG recommends that the Assistant Secretary for Diplomatic Security ensure that the Office of Computer Security develops a Department of State-wide centralized method to track participation in the annual cyber security awareness training Laptop Computer Security Awareness Briefing."

9. *Recommendation 16: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment." [Page 22]*

DS Comment: Please add the language "on an on-going basis when equipment is received, excessed or moved and" after the phrase "OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated "

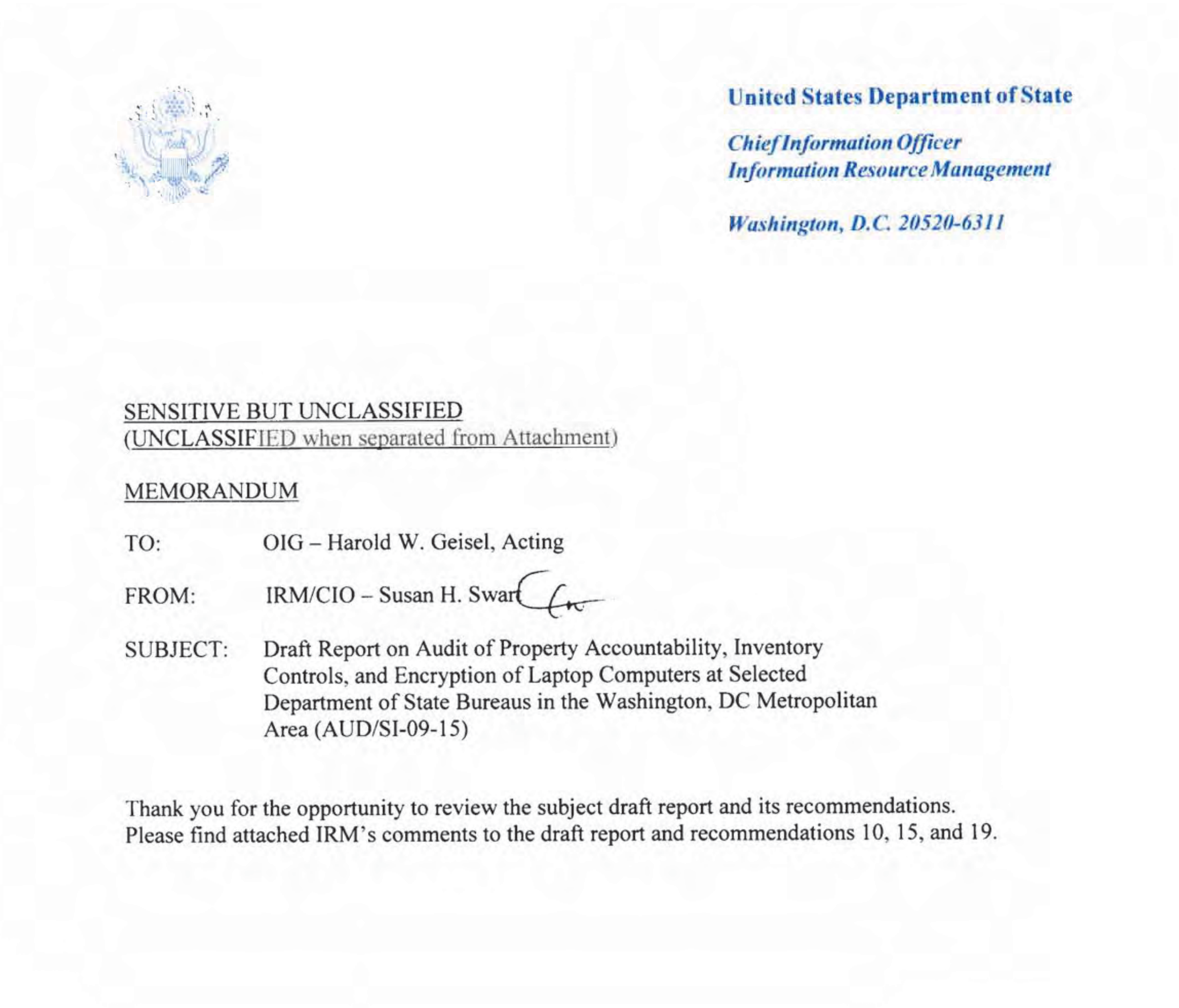
The new Recommendation 16 would then read:

"*Recommendation 16: OIG recommends that the Assistant Secretary for Diplomatic Security ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated on an on-going basis when equipment is received, excessed or moved and when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.*"

Drafted: DS/EX/MGT/PPD - David Winser
04/29/2009 - ext. 52746

Cleared:	DS/EX/PPD - Linda Watts	04/30/09	(OK)
	DS/SI – Don Reid/by Frank Wilkins	04/24/09	(OK)
	DS/EX- David Elswick	04/23/09	(OK)
	DS/EX/MGT - Ross Deal	04/23/09	(OK)
	DS/EX/CTO - Brian Jablon by J. Clynch	04/24/09	(OK)
	DS/DSS/TIA - Elizabeth Miller	04/22/09	(OK)
	DS/C/ST - Michael Vera	04/24/09	(OK)

APPENDIX D



United States Department of State

Chief Information Officer
Information Resource Management

Washington, D.C. 20520-6311

SENSITIVE BUT UNCLASSIFIED
(UNCLASSIFIED when separated from Attachment)

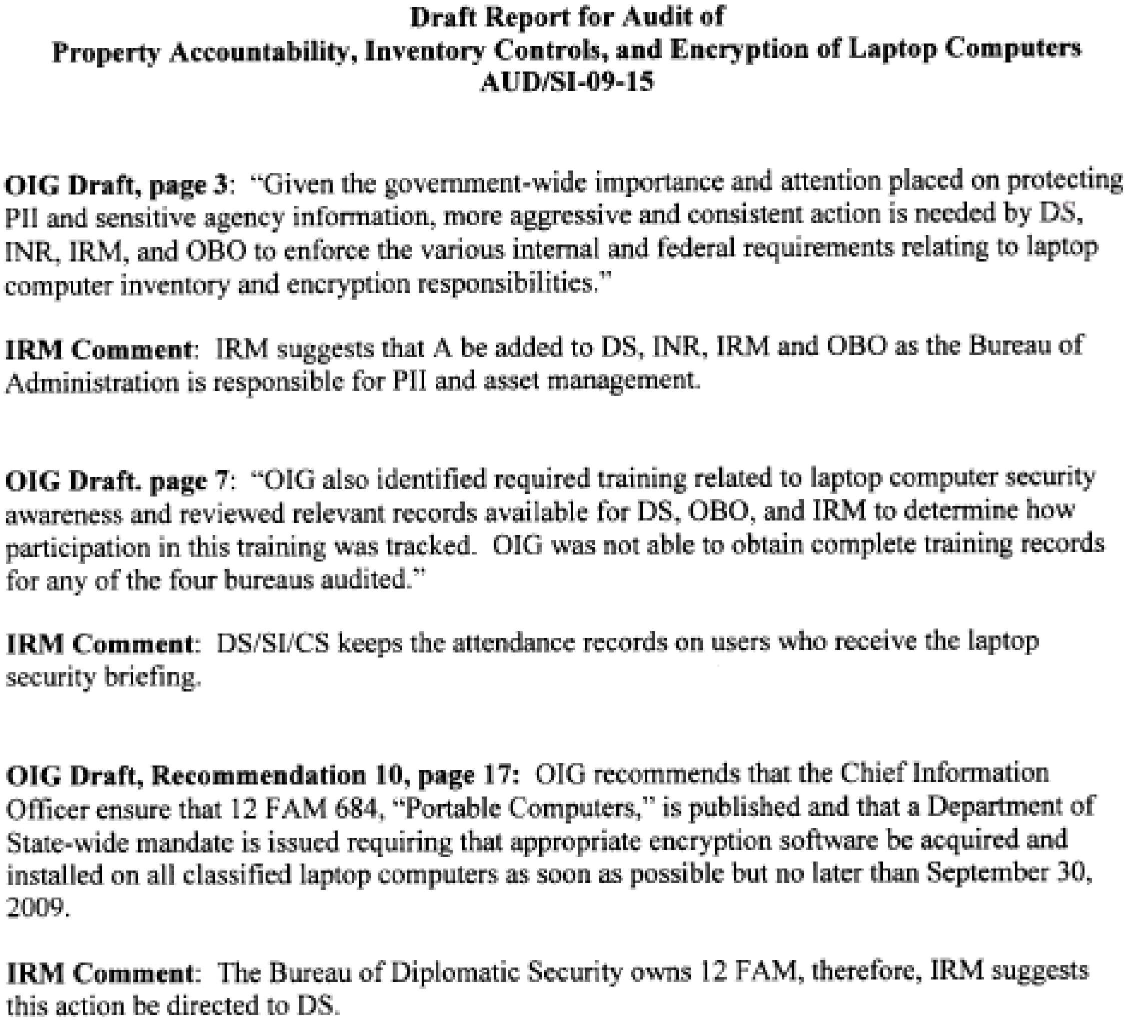
MEMORANDUM

TO: OIG – Harold W. Geisel, Acting

FROM: IRM/CIO – Susan H. Swart

SUBJECT: Draft Report on Audit of Property Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, DC Metropolitan Area (AUD/SI-09-15)

Thank you for the opportunity to review the subject draft report and its recommendations. Please find attached IRM's comments to the draft report and recommendations 10, 15, and 19.



Draft Report for Audit of
Property Accountability, Inventory Controls, and Encryption of Laptop Computers
AUD/SI-09-15

OIG Draft, page 3: "Given the government-wide importance and attention placed on protecting PII and sensitive agency information, more aggressive and consistent action is needed by DS, INR, IRM, and OBO to enforce the various internal and federal requirements relating to laptop computer inventory and encryption responsibilities."

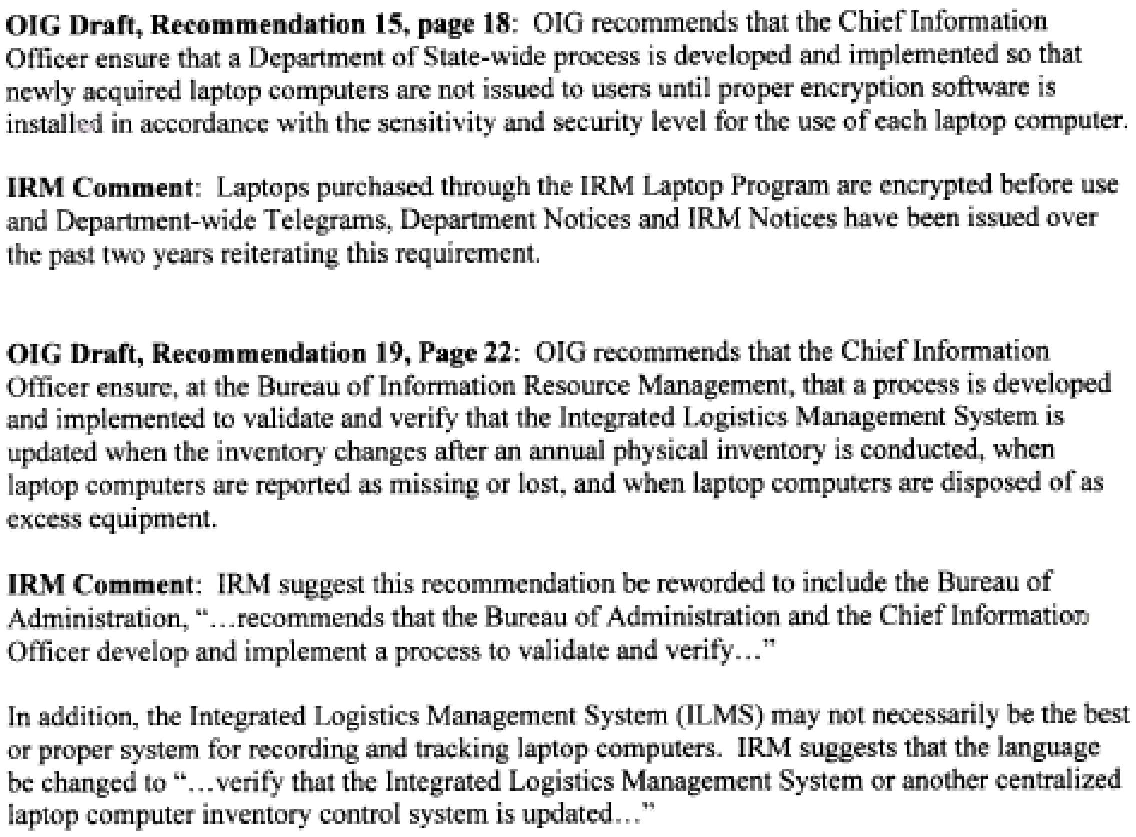
IRM Comment: IRM suggests that A be added to DS, INR, IRM and OBO as the Bureau of Administration is responsible for PII and asset management.

OIG Draft. page 7: "OIG also identified required training related to laptop computer security awareness and reviewed relevant records available for DS, OBO, and IRM to determine how participation in this training was tracked. OIG was not able to obtain complete training records for any of the four bureaus audited."

IRM Comment: DS/SI/CS keeps the attendance records on users who receive the laptop security briefing.

OIG Draft, Recommendation 10, page 17: OIG recommends that the Chief Information Officer ensure that 12 FAM 684, "Portable Computers," is published and that a Department of State-wide mandate is issued requiring that appropriate encryption software be acquired and installed on all classified laptop computers as soon as possible but no later than September 30, 2009.

IRM Comment: The Bureau of Diplomatic Security owns 12 FAM, therefore, IRM suggests this action be directed to DS.



OIG Draft, Recommendation 15, page 18: OIG recommends that the Chief Information Officer ensure that a Department of State-wide process is developed and implemented so that newly acquired laptop computers are not issued to users until proper encryption software is installed in accordance with the sensitivity and security level for the use of each laptop computer.

IRM Comment: Laptops purchased through the IRM Laptop Program are encrypted before use and Department-wide Telegrams, Department Notices and IRM Notices have been issued over the past two years reiterating this requirement.

OIG Draft, Recommendation 19, Page 22: OIG recommends that the Chief Information Officer ensure, at the Bureau of Information Resource Management, that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

IRM Comment: IRM suggest this recommendation be reworded to include the Bureau of Administration, "…recommends that the Bureau of Administration and the Chief Information Officer develop and implement a process to validate and verify…"

In addition, the Integrated Logistics Management System (ILMS) may not necessarily be the best or proper system for recording and tracking laptop computers. IRM suggests that the language be changed to "…verify that the Integrated Logistics Management System or another centralized laptop computer inventory control system is updated…"

APPENDIX E

Bureau of Administration Response

[OIG Note: *In an April 27 e-mail to the Office of Inspector General, the Bureau of Administration provided its response.*]

Recommendation 20: OIG recommends that the Assistant Secretary for Administration ensure that the Office of Logistics Management develop standard codes for the Integrated Logistics Management System to specifically identify classified, unclassified, and sensitive but unclassified laptop computers; disseminates these codes prior to the next Department of State –wide annual inventory; and defines or eliminates existing codes that are ambiguous.

Response: The Office of Logistics Management has completed the analysis on the numerous Asset Classes associated with Notebooks/Laptops in ILMS Asset Management. A change request (attached) has been submitted to update the ILMS Notebook/Laptop Asset Classes in accordance to the OIG's Recommendation and to specifically identify classified, unclassified, and sensitive but unclassified laptop computers.

[OIG Note: *The Bureau's ILMS Change Request Form is included as an exhibit to the appendix.*]

Section A – To be completed by Initiator (ALL fields required)

1. Change Request Title: Update Notebook/Laptop Asset Classes in ILMS Asset Management

15. CR Number:

2. Functional Area: Property Management

16. Date:

3. Initiator: Ron Tate

4. Phone No.:703-875-6093

5. ILMS Modules Affected: Asset Management

6a. Scope/Description of Change: Update the Notebook/Laptop Asset Classes in accordance to the OIG Recommendation 20, and to specifically identify classified, unclassified, and sensitive but unclassified laptop computers.

6b. Detailed Requirements of Change:

1. Rename Asset Class 25108 from “CPU, NOTEBOOK/LAPTOP” to “CPU, NOTEBOOK/LAPTOP,UNCLASSIFIED”
2. Add the following Asset Classes:
   a. 25109 CPU, NOTEBOOK/LAPTOP,CLASSIFIED
   b. 25110 CPU, NOTEBOOK/LAPTOP,SEN-BUT-UNCLASS
3. MAP Asset Classes - A5020, A5040, EP5200, 25102, 25103 and 25104 to 25108
4. Remove Asset Classes - A5020, A5040, EP5200, 25102, 25103 and 25104 from the Asset Class Table

7. Justification/Reason (Cost/Benefit): ***Taken from “OIG Laptop Inspection Report*** “- **Recommendation 20:** OIG recommends that the Assistant Secretary for Administration ensure that the Office of Logistics Management develop standard codes for the Integrated Logistics Management System to specifically identify classified, unclassified, and sensitive but unclassified laptop computers; disseminates these codes prior to the next Department of State –wide annual inventory; and defines or eliminates existing codes that are ambiguous.

Section B – To be completed by Production Support (ALL fields required)

8. Alternatives Considered and Rejected:

9. Related CR(s):

10. Impact: Technical Schedule Cost Quality Risk Database Structure EDW

11. Functional Area(s) Impacted by change:

12. Discuss Impacts Indicated Above and Any Security Risks:

13. Change Request as Production Support (CRPS): Yes No

14. Estimated Hours/Cost:	Hours	Cost
Functional Design		
Detailed Design		
Development		
Unit Test		
System Test		
UAT		
O&M		
Training		
Estimated Total		

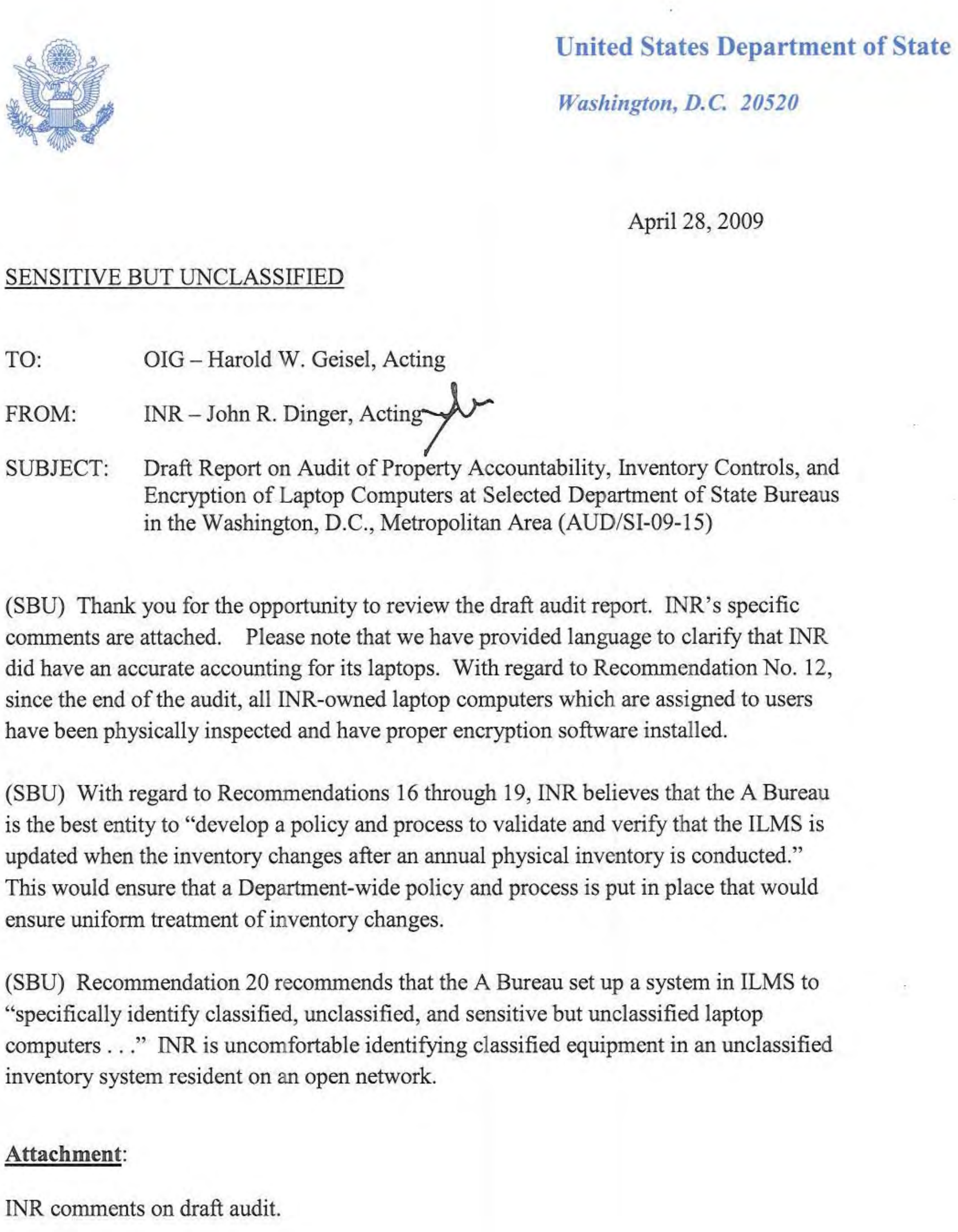
Section C – To be completed by Change Librarian

INSTRUCTIONS FOR COMPLETING A CHANGE REQUEST

Field Titles	*Field Descriptions*
1. Change Request Title	A brief title describing the Change Request
2. Functional Area	Identify the functional area affected by the change
3. Initiator	Name of the CR initiator
4. Phone No	Telephone number of the CR initiator
5. ILMS Modules Affected	Areas of the ILMS system affected by the change (Distribution, Transportation, etc.)
6a. Scope/Description of Change	Provide a description of the change and its complexity
6b. Detailed Requirements of Change	Provide a detailed list of the business and technical requirements for this change
7. Justification/Reason	Summarize why the change is important with clear business and/or technical requirements. What is the cost vs. benefit for making this change?
8. Alternatives Considered and Rejected	Identify methods pursued to resolve issue before initiating a CR
9. Related CR(s)	List any related change requests
10. Impact	Check the areas that will be impacted by the CR
11. Functional Area(s) Impacted	List functional area(s) impacted (i.e. DPM, AM, Ariba, Momentum, Transportation, etc.)
12. Discuss Impacts Indicated Above	Provide a detailed description of how the indicated areas will be affected by the CR. Include a description of security risks introduced by making the change -or- the security risks associated with not making the change.
13. Change Request as Production Support	Does the CR meet the requirements to be considered for CRPS
14. Estimated Hours/Cost	A rough order of magnitude (ROM) hours/cost to complete the change
15. CR Number	Change request number assigned and entered by the Change Librarian
16. Date	Date the initial CR was received by the Change Librarian
17. Impact Analysis	Check the box if an impact analysis has been performed and is attached
18. TRB Recommendation	TRB Outcome
19. CCB Decision	CCB Outcome

- Initiators complete fields 1-7.
- The ILMS prime contractor completes fields 8-14.
- The Change Librarian completes shaded fields 15-19.

APPENDIX F



United States Department of State

Washington, D.C. 20520

April 28, 2009

SENSITIVE BUT UNCLASSIFIED

TO: OIG – Harold W. Geisel, Acting

FROM: INR – John R. Dinger, Acting

SUBJECT: Draft Report on Audit of Property Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, D.C., Metropolitan Area (AUD/SI-09-15)

(SBU) Thank you for the opportunity to review the draft audit report. INR's specific comments are attached. Please note that we have provided language to clarify that INR did have an accurate accounting for its laptops. With regard to Recommendation No. 12, since the end of the audit, all INR-owned laptop computers which are assigned to users have been physically inspected and have proper encryption software installed.

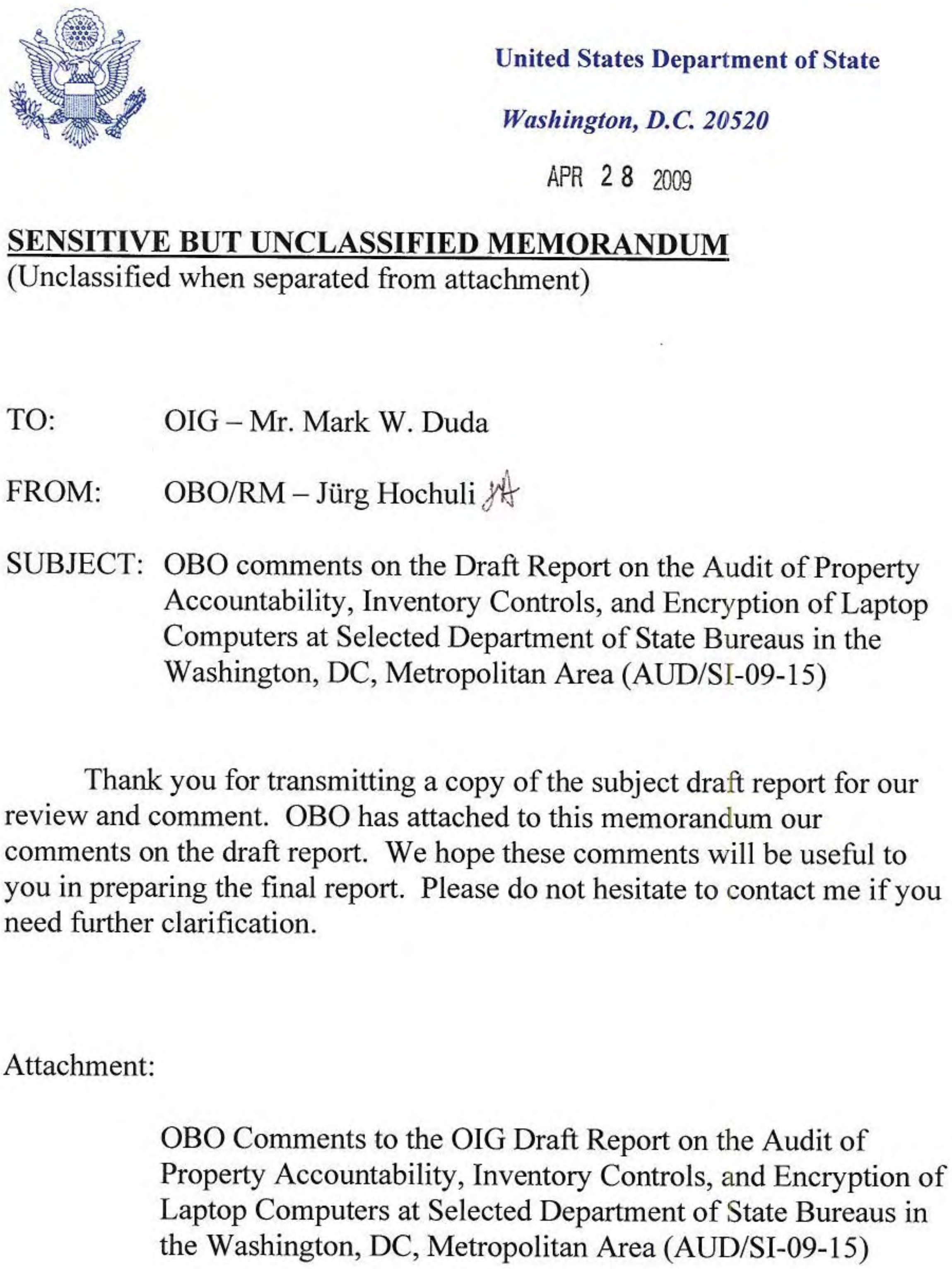
(SBU) With regard to Recommendations 16 through 19, INR believes that the A Bureau is the best entity to "develop a policy and process to validate and verify that the ILMS is updated when the inventory changes after an annual physical inventory is conducted." This would ensure that a Department-wide policy and process is put in place that would ensure uniform treatment of inventory changes.

(SBU) Recommendation 20 recommends that the A Bureau set up a system in ILMS to "specifically identify classified, unclassified, and sensitive but unclassified laptop computers . . ." INR is uncomfortable identifying classified equipment in an unclassified inventory system resident on an open network.

Attachment:

INR comments on draft audit.

APPENDIX G



United States Department of State

Washington, D.C. 20520

APR 28 2009

SENSITIVE BUT UNCLASSIFIED MEMORANDUM
(Unclassified when separated from attachment)

TO: OIG – Mr. Mark W. Duda

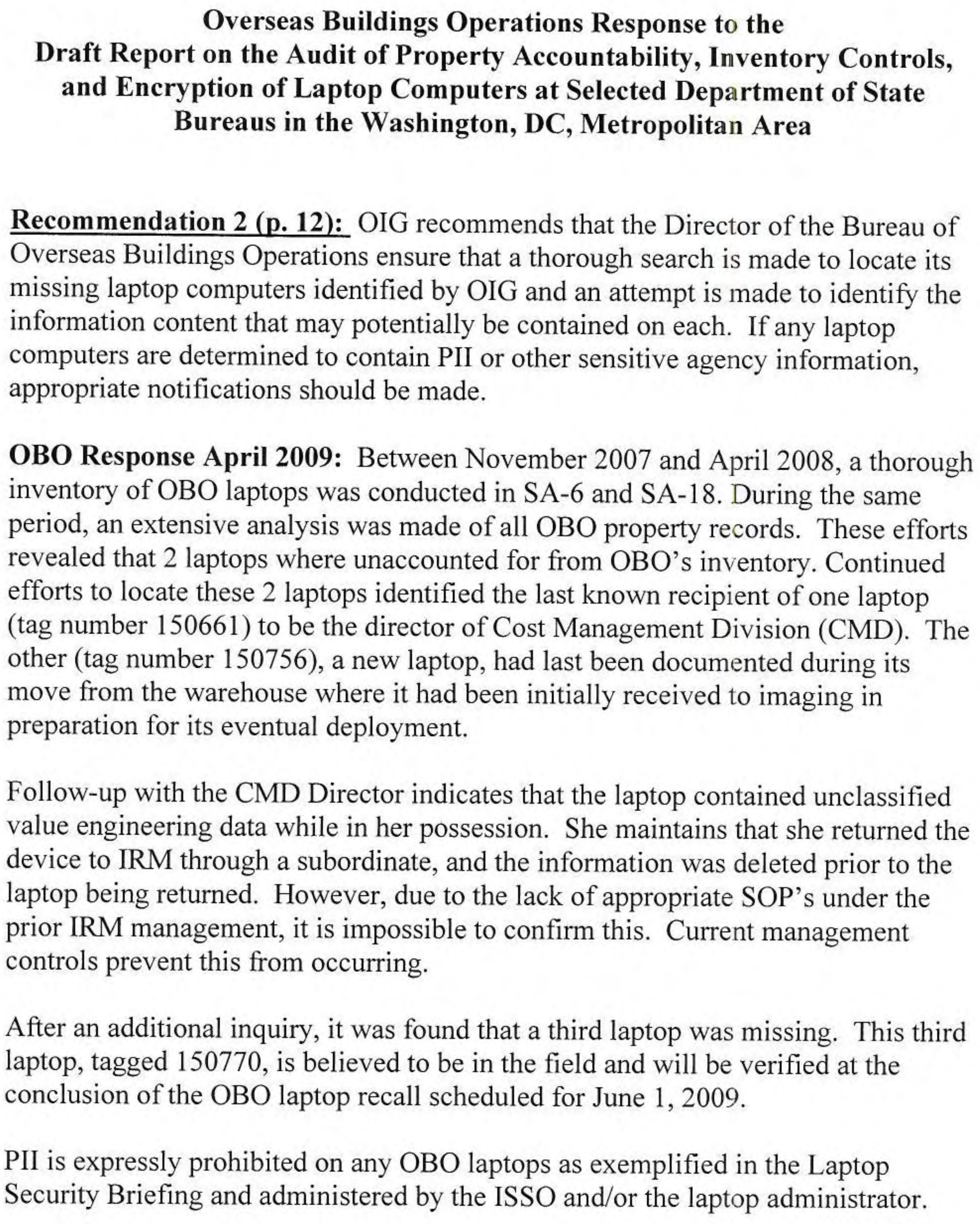
FROM: OBO/RM – Jürg Hochuli

SUBJECT: OBO comments on the Draft Report on the Audit of Property Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, DC, Metropolitan Area (AUD/SI-09-15)

Thank you for transmitting a copy of the subject draft report for our review and comment. OBO has attached to this memorandum our comments on the draft report. We hope these comments will be useful to you in preparing the final report. Please do not hesitate to contact me if you need further clarification.

Attachment:

OBO Comments to the OIG Draft Report on the Audit of Property Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, DC, Metropolitan Area (AUD/SI-09-15)



Overseas Buildings Operations Response to the Draft Report on the Audit of Property Accountability, Inventory Controls, and Encryption of Laptop Computers at Selected Department of State Bureaus in the Washington, DC, Metropolitan Area

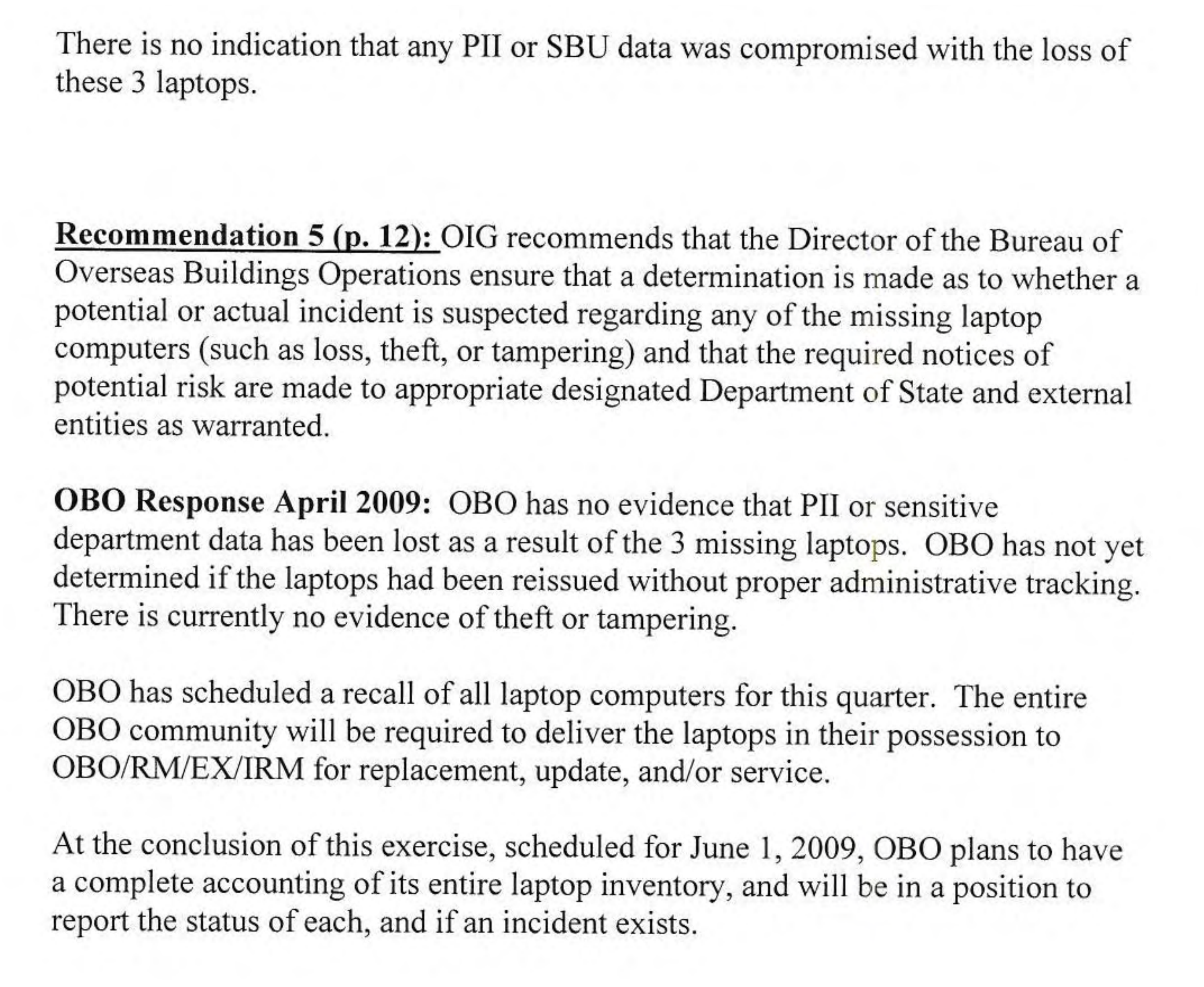
Recommendation 2 (p. 12): OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a thorough search is made to locate its missing laptop computers identified by OIG and an attempt is made to identify the information content that may potentially be contained on each. If any laptop computers are determined to contain PII or other sensitive agency information, appropriate notifications should be made.

OBO Response April 2009: Between November 2007 and April 2008, a thorough inventory of OBO laptops was conducted in SA-6 and SA-18. During the same period, an extensive analysis was made of all OBO property records. These efforts revealed that 2 laptops where unaccounted for from OBO's inventory. Continued efforts to locate these 2 laptops identified the last known recipient of one laptop (tag number 150661) to be the director of Cost Management Division (CMD). The other (tag number 150756), a new laptop, had last been documented during its move from the warehouse where it had been initially received to imaging in preparation for its eventual deployment.

Follow-up with the CMD Director indicates that the laptop contained unclassified value engineering data while in her possession. She maintains that she returned the device to IRM through a subordinate, and the information was deleted prior to the laptop being returned. However, due to the lack of appropriate SOP's under the prior IRM management, it is impossible to confirm this. Current management controls prevent this from occurring.

After an additional inquiry, it was found that a third laptop was missing. This third laptop, tagged 150770, is believed to be in the field and will be verified at the conclusion of the OBO laptop recall scheduled for June 1, 2009.

PII is expressly prohibited on any OBO laptops as exemplified in the Laptop Security Briefing and administered by the ISSO and/or the laptop administrator.



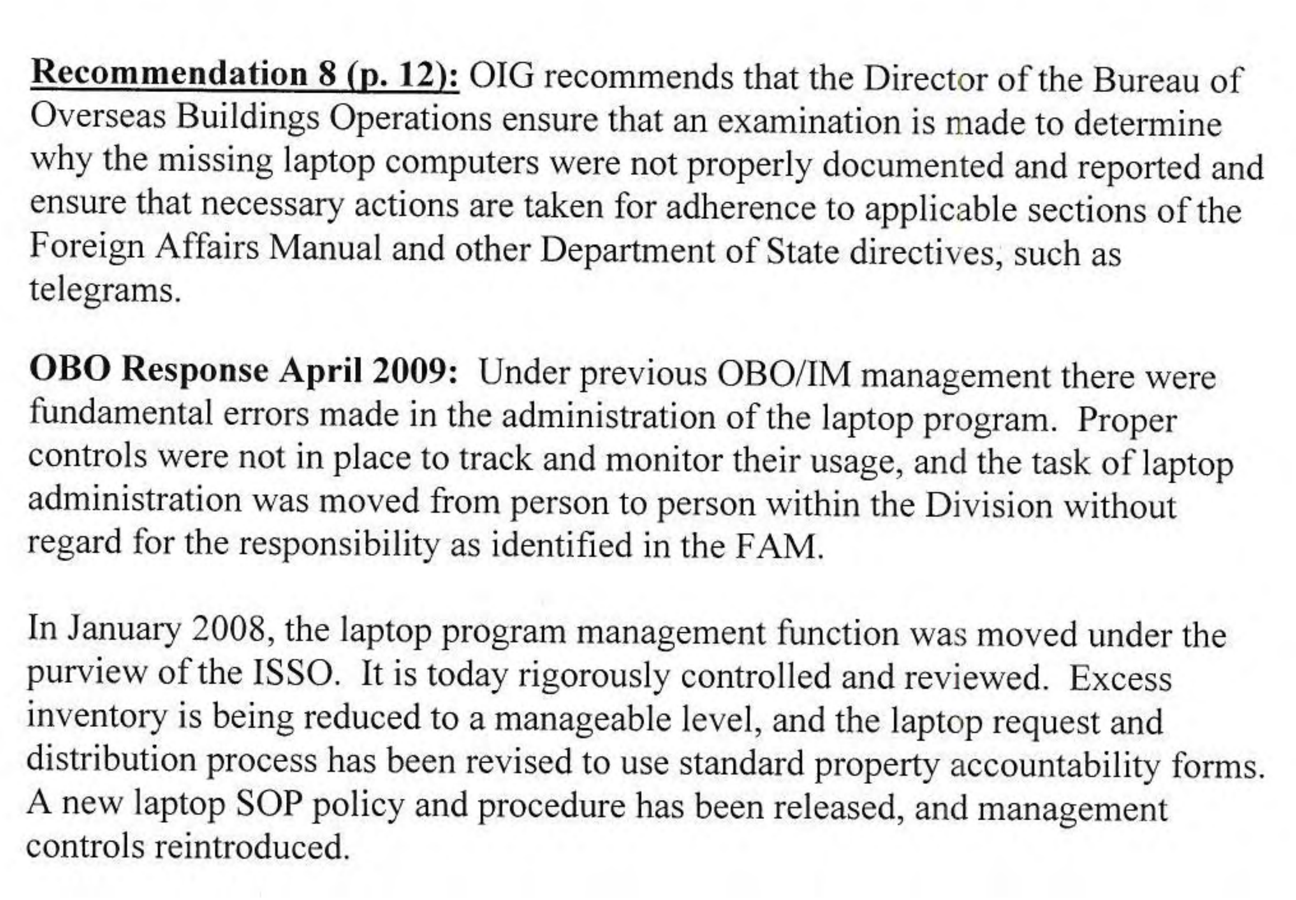
There is no indication that any PII or SBU data was compromised with the loss of these 3 laptops.

Recommendation 5 (p. 12): OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a determination is made as to whether a potential or actual incident is suspected regarding any of the missing laptop computers (such as loss, theft, or tampering) and that the required notices of potential risk are made to appropriate designated Department of State and external entities as warranted.

OBO Response April 2009: OBO has no evidence that PII or sensitive department data has been lost as a result of the 3 missing laptops. OBO has not yet determined if the laptops had been reissued without proper administrative tracking. There is currently no evidence of theft or tampering.

OBO has scheduled a recall of all laptop computers for this quarter. The entire OBO community will be required to deliver the laptops in their possession to OBO/RM/EX/IRM for replacement, update, and/or service.

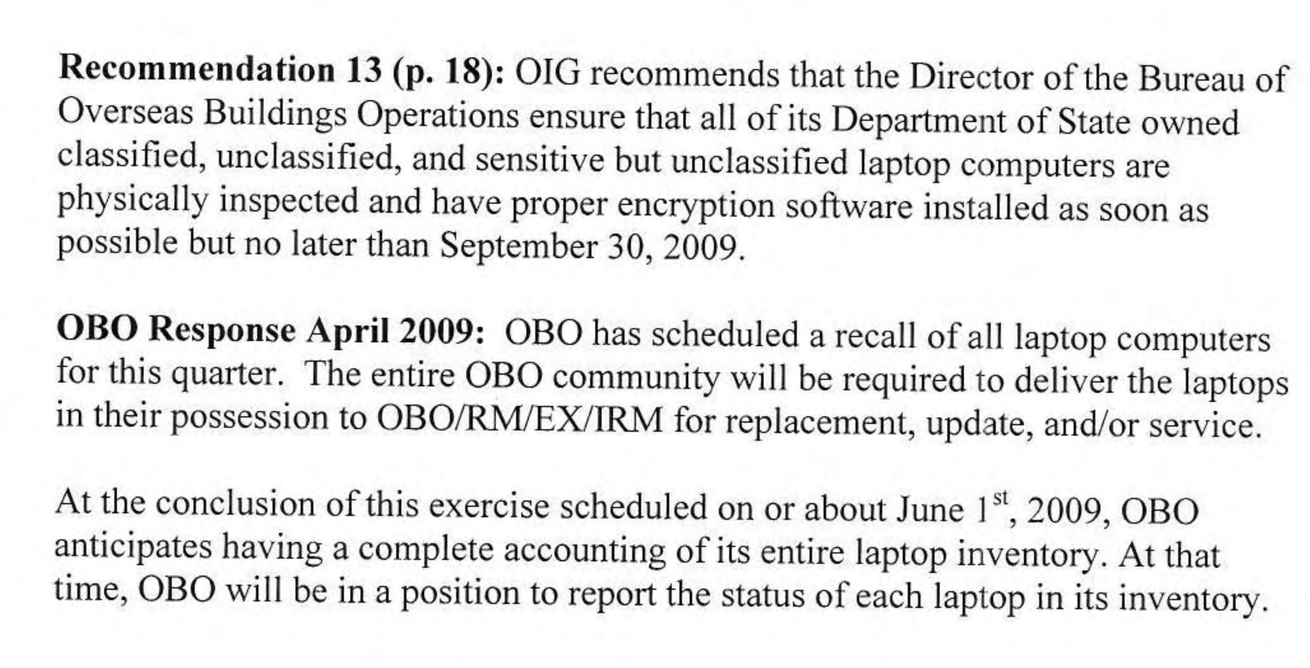
At the conclusion of this exercise, scheduled for June 1, 2009, OBO plans to have a complete accounting of its entire laptop inventory, and will be in a position to report the status of each, and if an incident exists.



Recommendation 8 (p. 12): OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that an examination is made to determine why the missing laptop computers were not properly documented and reported and ensure that necessary actions are taken for adherence to applicable sections of the Foreign Affairs Manual and other Department of State directives, such as telegrams.

OBO Response April 2009: Under previous OBO/IM management there were fundamental errors made in the administration of the laptop program. Proper controls were not in place to track and monitor their usage, and the task of laptop administration was moved from person to person within the Division without regard for the responsibility as identified in the FAM.

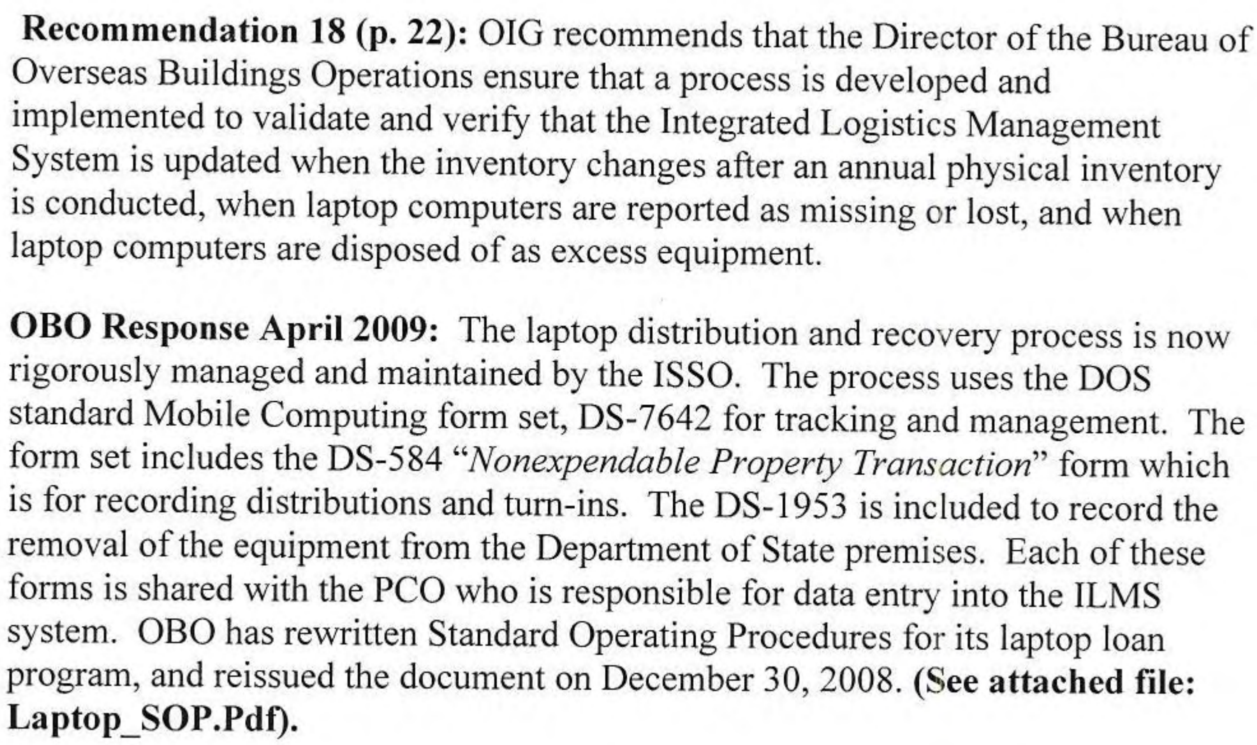
In January 2008, the laptop program management function was moved under the purview of the ISSO. It is today rigorously controlled and reviewed. Excess inventory is being reduced to a manageable level, and the laptop request and distribution process has been revised to use standard property accountability forms. A new laptop SOP policy and procedure has been released, and management controls reintroduced.



Recommendation 13 (p. 18): OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that all of its Department of State owned classified, unclassified, and sensitive but unclassified laptop computers are physically inspected and have proper encryption software installed as soon as possible but no later than September 30, 2009.

OBO Response April 2009: OBO has scheduled a recall of all laptop computers for this quarter. The entire OBO community will be required to deliver the laptops in their possession to OBO/RM/EX/IRM for replacement, update, and/or service.

At the conclusion of this exercise scheduled on or about June 1st, 2009, OBO anticipates having a complete accounting of its entire laptop inventory. At that time, OBO will be in a position to report the status of each laptop in its inventory.



Recommendation 18 (p. 22): OIG recommends that the Director of the Bureau of Overseas Buildings Operations ensure that a process is developed and implemented to validate and verify that the Integrated Logistics Management System is updated when the inventory changes after an annual physical inventory is conducted, when laptop computers are reported as missing or lost, and when laptop computers are disposed of as excess equipment.

OBO Response April 2009: The laptop distribution and recovery process is now rigorously managed and maintained by the ISSO. The process uses the DOS standard Mobile Computing form set, DS-7642 for tracking and management. The form set includes the DS-584 "*Nonexpendable Property Transaction*" form which is for recording distributions and turn-ins. The DS-1953 is included to record the removal of the equipment from the Department of State premises. Each of these forms is shared with the PCO who is responsible for data entry into the ILMS system. OBO has rewritten Standard Operating Procedures for its laptop loan program, and reissued the document on December 30, 2008. **(See attached file: Laptop_SOP.Pdf).**

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.