



UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS
OFFICE OF INSPECTOR GENERAL

AUD-IT-14-03

Office of Audits

November 2013

Audit of Department of State Information Security Program

~~**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

(U) PREFACE

(U) This report is being transmitted 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 as part of the Office of Inspector General's (OIG) responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

(U) In accordance with the Federal Information Security Management Act of 2002 (FISMA), OIG performed an audit of the Department of State Information Security Program for FY 2013. To perform this audit, OIG contracted with the independent public accountant Williams, Adley & Company, LLP. The audit report is based on interviews with employees and officials of the Department of State, direct observation, and a review of applicable documents.

(U) The independent public accountant identified areas in which improvements could be made, including the risk management program, plans of actions and milestones, continuous monitoring, configuration management, identity and access management, contingency planning, contractor systems, security training, and remote access management.

(U) OIG evaluated the nature, extent, and timing of the independent public accountant's work; monitored progress throughout the audit; reviewed supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with the findings, and the recommendations contained in the audit report were developed based on the best knowledge available and discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

(U) I express my appreciation to all of the individuals who contributed to the preparation of this report.

A handwritten signature in blue ink, appearing to read "Norman P. Brown".

Norman P. Brown
Acting Assistant Inspector General
for Audits



Audit of the Department of State Information Security Program

October 24, 2013

Office of Inspector General
U.S. Department of State
Washington, DC

Williams, Adley & Company-DC, LLP, has performed an audit of the Department of State Information Security Program. We audited the Department of State's compliance with the Federal Information Security Management Act, Office of Management and Budget requirements, and National Institute of Standards and Technology standards. We performed this audit under Contract No. SAQMMA10F2159. The audit was designed to meet the objectives described in the report.

We conducted this performance audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We communicated the results of our audit and the related findings and recommendations to the U.S. Department of State Office of Inspector General.

We appreciate the cooperation provided by the Department of State's personnel during the audit.

Williams, Adley & Company-DC, LLP
Williams, Adley & Company-DC, LLP

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1030 15th Street, NW, Suite 350 West • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

(U) Acronyms

(U) AD	Active Directory
(U) AIS	Automated Information System
(U) ALDAC	All Diplomatic and Consular Posts
(U) ARS	Action Request System
(U) ATO	Authority to Operate
(U) BEAP	Bureau Emergency Action Plan
(U) CGFS	Bureau of the Comptroller and Global Financial Services
(U) CIO	Chief Information Officer
(U) CS	Office of Computer Security
(U) Department	Department of State
(U) DHS	Department of Homeland Security
(U) DS	Bureau of Diplomatic Security
(U) EAC	Emergency Action Committee
(U) ENM	Enterprise Network Management
(U) FAM	Foreign Affairs Manual
(U) FISMA	Federal Information Security Management Act
(U) FSOT	Foreign Service Officer Test
(U) GAGAS	Generally Accepted Government Auditing Standards
(U) GAL	Global Address List
(U) GO	Global OpenNet
(U) IA	Information Assurance
(U) IRM	Information Resource Management
(U) ISCP	Information Security Contingency Plan
(U) ISSO	Information System Security Officer
(U) ISSC	Information Security Steering Committee
(U) ITAB	Information Technology Applications Baseline
(U) IT	Information Technology
(U) MCMS	Mobile Computing Management System
(U) NIST	National Institute of Standards and Technology
(U) OCIO	Office of the Chief Information Officer
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) ONE	OpenNet Everywhere
(U) OU	Organizational Unit
(U) PKI-BLADE	Public Key Infrastructure and BLADE
(U) POA&M	Plan of Action and Milestones
(U) SI	Security Infrastructure
(U) SP	Special Publication
(U) TOMIS	The Office of Foreign Missions Information System
(U) UII	Unique Investment Identifier

(U) Table of Contents

(U) Executive Summary 1

(U) Background 3

(U) Objective 3

(U) Results of Audit..... 4

 (U) Finding A. Risk Management Framework..... 4

 (U) Finding B. Plan of Action and Milestones 7

 (U) Finding C. Continuous Monitoring 13

 (U) Finding D. Configuration Management 14

 (U) Finding E. Identity and Access Management..... 18

 (U) Finding F. Contingency Planning..... 25

 (U) Finding G. Contractor Systems 28

 (U) Finding H. Security Training..... 32

 (U) Finding I. Remote Access Management..... 33

 (U) Finding J. Compliance With FISMA Requirements 35

(U) List of Current Year Recommendations..... 36

(U) Appendices

 (U) A. Scope and Methodology..... 41

 (U) B. Followup of Recommendations From the FY 2012 FISMA Report 45

 (U) C. End-to-End Configuration Management Process Needs Improvement..... 52

 (U) D. Sample Selection of Information Systems Listed in Information Technology Asset
 Baseline Used for FY 2013 Audit..... 53

 (U) E. Department of State Response..... 54

(U) Executive Summary

(U) In accordance with the Federal Information Security Management Act of 2002 (FISMA),¹ the Office of Inspector General (OIG) contracted with Williams, Adley & Company-DC, LLP (referred to as “we” in this report), to perform an independent audit of the Department of State (Department) information security program’s compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) for FY 2013. Additionally, the results are designed to assist OIG in providing responses to *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated November 30, 2012.

(U) The FY 2012 FISMA report² contained 31 recommendations intended to address security deficiencies, and the most significant of these deficiencies involved the Department’s risk management strategy and security authorizations, security configuration management, Plan of Action and Milestones (POA&M), and the continuous monitoring program. We reviewed the Department’s corrective actions to address weaknesses identified in OIG’s FY 2012 FISMA report. OIG closed 11 of the 31 recommendations in the FY 2012 report. The status of each recommendation from OIG’s FY 2012 report is presented in Appendix B of this report.

(U) Since FY 2012, the Department has taken the following steps to improve management controls:

- (U) Increased the security awareness training compliance rate in FY 2013.
- (U) Improved the management of Active Directory (AD) to limit the amount of accounts created without requiring a password or setting an expiration date on the accounts.
- (U) Established and published UNIX standard baselines.
- (U) Opened the Foreign Affairs Cybersecurity Center, thereby enhancing situational awareness and protecting against attacks and emerging threats.
- (U) Enhanced the Security Capital Planning process by tracking Department FISMA systems to their corresponding Information Technology (IT) investments for more accurate reporting on the Exhibit 300s.

(U) Overall, we found that the Department had implemented an information security program and had made progress during FY 2013, but we identified control weaknesses that significantly impacted the information security program. If these control weaknesses were exploited, the Department could experience security breaches.

[Redacted] (b) (5)

¹ (U) Pub. L. No. 107-347, tit. III.

² (U) *Audit of Department of State Information Security Program* (AUD-IT-13-03, Nov. 2012).

³ (U) OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept. 27, 2012.

[Redacted] (b) (5)

(U) This report contains 10 findings (identified as Findings A through J) and 29 recommendations to address security deficiencies identified in nine of 11 reportable areas. We believe the most significant security deficiencies are the first four findings:

- (U) The risk management framework remains unfinalized. (Finding A)
- (U) Plans of Action and Milestones (POA&M) remain ineffective. (Finding B)
- (U) An overall continuous monitoring strategy remains undocumented. (Finding C)

[Redacted] (b) (5)

(U) The following is a summary of our 10 findings:

- (U) In FY 2010,⁴ FY 2011,⁵ FY 2012, and FY 2013, OIG reported that the Department's risk management framework was not finalized. (Finding A)
- (U) In FY 2010, FY2011, FY 2012, and FY 2013, OIG found that the POA&M process was not effective. (Finding B)
- (U) In FY 2010, FY2011, FY 2012, and FY 2013, OIG found that the Office of the Chief Information Officer (OCIO) did not have an overall continuous monitoring strategy documented. (Finding C)

[Redacted] (b) (5)

- (U) Bureaus and/or offices within the Department did not identify an alternate processing site, an alternate storage site, and an alternate telecommunications services and/or conduct contingency testing. (Finding F)

[Redacted] (b) (5)

- (U) IT personnel with security responsibilities for the Department had not taken specialized role-based security training, and a tracking mechanism for role-based training had not been fully implemented. (Finding H)
- (U) The Department's policies were not updated to include the only approved remote access method, Global OpenNet (GO). (Finding I)

⁴ (U) *Review of Department of State Information Security Program* (AUD/IT-11-07, Nov. 2010).

⁵ (U) *Evaluation of Department of State Information Security Program* (AUD/IT-12-14, Nov. 2011).

- (U) The Department was in compliance with the Incident Response and Security Capital Planning requirements. (Finding J)

(U) In its October 22, 2013, response to the draft report (see Appendix E), the Department concurred with 19 recommendations but did not concur with 10 recommendations. Based on the response, OIG considers 17 recommendations resolved, pending further action, and 12 recommendations unresolved. Also based on the response, OIG revised four recommendations. These revisions are noted in management's response and OIG's analysis, which are presented after each recommendation.

(U) Background

(U) Through FISMA, Congress recognized the importance of information security to the economic and national security interests of the United States. According to FISMA, each Federal agency should develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including information and information systems provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

(U) FISMA assigns specific responsibilities to Federal agencies, NIST, OMB, and the Department of Homeland Security (DHS)⁶ in order to strengthen information system security. In particular, according to FISMA, the head of each agency should implement policies and procedures to cost effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, according to FISMA, agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS.

(U) On an annual basis, OMB, in coordination with DHS, provides guidance with reporting categories and questions for meeting the current year's reporting requirements.⁷ OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

(U) Objective

(U) The objective of this audit was to perform an independent evaluation of the Department's information security program and practices for FY 2013 and included testing the effectiveness of security controls for a subset of systems as required.

⁶ (U) OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security (DHS)*, July 6, 2010.

⁷ (U) OMB Memorandum M-12-20.

(U) Results of Audit

(U) Overall, we found that the Department had implemented an information security program, but we identified control weaknesses that significantly impacted the information security program. If these control weaknesses were exploited, the Department could experience security breaches. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, the Department needs to address the control weaknesses described.

(U) Finding A. Risk Management Framework

(U) OIG first identified Risk Management deficiencies in FY 2010, and many of these same deficiencies remained in FY 2013. NIST Special Publication (SP) 800-37, Revision 1,⁸ states the risk management framework is a process that:

(U) ...emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

(U) Furthermore, NIST SP 800-30, Revision 1,⁹ states:

(U) Risk assessments can be conducted at all three tiers in the risk management hierarchy—including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level). At Tiers 1 and 2, organizations use risk assessments to evaluate, for example, systemic information security-related risks associated with organizational governance and management activities, mission/business processes, enterprise architecture, or the funding of information security programs. At Tier 3, organizations use risk assessments to more effectively support the implementation of the Risk Management Framework (i.e., security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring).

(U) OMB M-10-15¹⁰ states, “For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB.”

⁸ (U) NIST SP 800-37, rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, sec. 1.1, Feb. 2010.

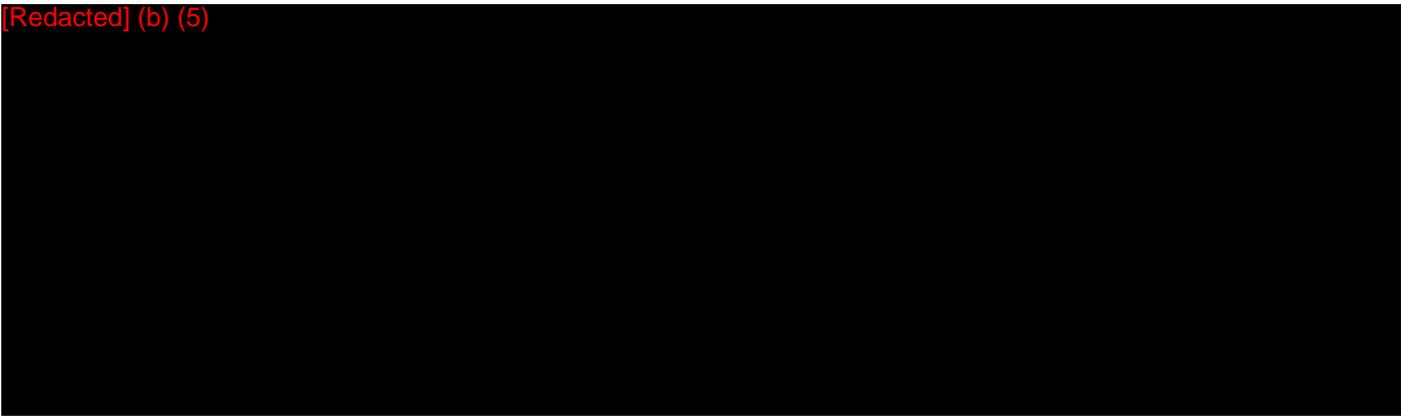
⁹ (U) NIST SP 800-30, rev. 1, *Guide for Conducting Risk Assessments*, Introduction, Sept. 2012.

(U) NIST SP 800-53, Revision 3,¹¹ states the organization:

- (U) Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;
- (U) Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
- (U) Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

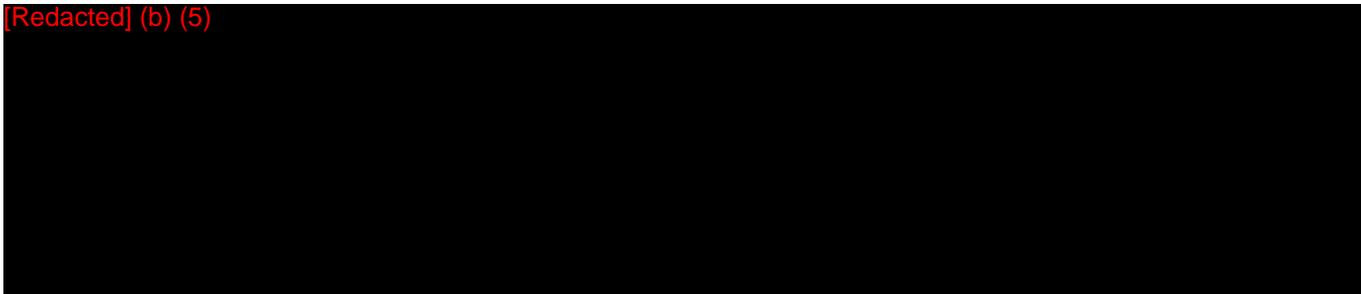
(U) At the organizational level, the Department did not formally develop or document a risk management framework or strategy addressing how the Department intends to assess, respond to, and monitor information security risk. In addition, OIG identified the following deficiencies:

[Redacted] (b) (5)



(U) The Chief Information Officer (CIO), in coordination with the Information Security Steering Committee (ISSC), did not prioritize tasks to ensure devoted resources identified, documented, and finalized a risk management framework for their information systems.

[Redacted] (b) (5)

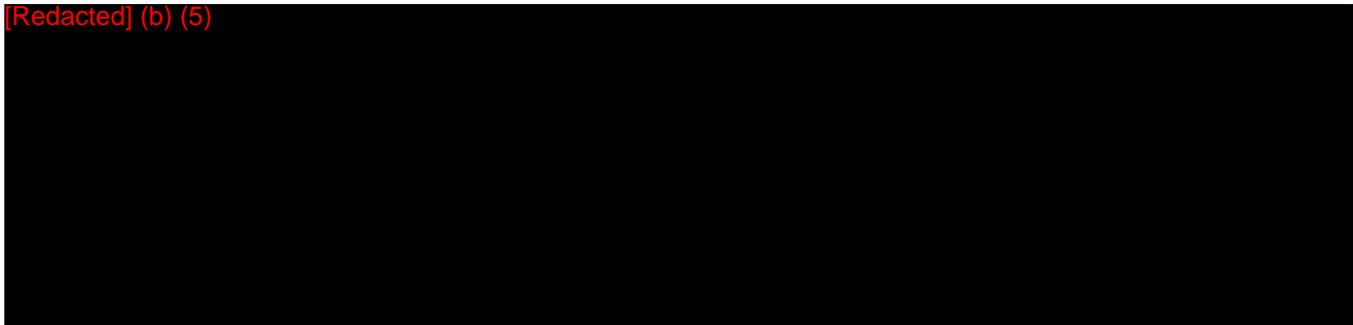


¹⁰ (U) OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, sec. NIST Standards and Guidelines, April 2010.

¹¹ (U) NIST SP 800-53, rev. 3, *Recommended Security Controls for Federal Information Systems*, CA-3 Information System Connections, Aug. 2009 (last updated May 2010).

¹² (U) *Ibid.*

[Redacted] (b) (5)



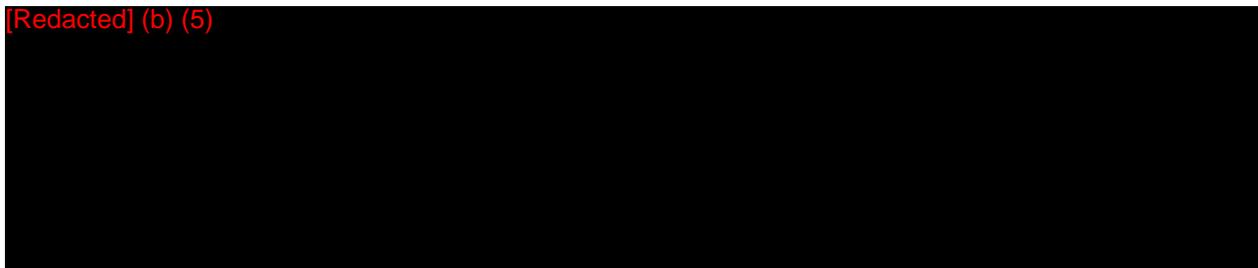
(U) Without a risk management program, the Department cannot prioritize, assess, respond to, and monitor information security risk, which leaves the Department vulnerable to attacks and threats. In addition, without a documented framework, the Department cannot transfer knowledge from senior-level management to the bureaus, resulting in the lack of a process to appropriately set Department boundaries, perform timely Certification and Accreditation activities, and authorize its systems.

(U) **Recommendation 1.** OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, prioritize tasks to ensure that devoted resources identify, document, and finalize a risk management framework for Department of State information systems in accordance with National Institute of Standards and Technology Special Publication 800-30, Revision 1.

(U) **Management Response:** IRM concurred with this recommendation.

(U) **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that a risk management framework for the Department's information systems has been identified, documented, and finalized in accordance with NIST SP 800-30, Revision 1.

[Redacted] (b) (5)



(U) **Management Response:** IRM concurred with this recommendation and noted that this work was in process.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation

[Redacted] (b) (5)



¹³ (U) NIST SP 800-53, rev. 3.

¹⁴ (U) NIST SP 800-53, rev. 2, *Recommended Security Controls for Federal Information Systems*, Dec. 2007.

[Redacted] (b) (5)

(U) Recommendation 3. OIG recommends that Bureau of Information Resource Management ensure system owners perform security impact analyses for all systems and applications in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3, and reauthorize the systems accordingly.

(U) Management Response: IRM did not concur with this recommendation, stating, “this is part of the IA Toolkit for A&A [Assessment and Authorization].”

(U) OIG Analysis: OIG considers the recommendation unresolved. OIG agrees that performing security impact analyses is required as part of the Information Assurance Toolkit but noted that ARS, TOMIS, and FSOT security impact analyses were performed with the outdated NIST SP 800-53, Revision 2, controls instead of the current NIST SP 800-53, Revision 3, controls. NIST SP 800-53, Revision 3, was first published in August 2009 and has been the baseline for security controls for more than four years; however, no evidence exists to show that the Bureau of Information Resource Management and system owners made efforts to implement the new controls. NIST SP 800-53, Revision 3, contains additional security controls and an additional security control family that NIST SP 800-53, Revision 2, does not contain. This recommendation can be closed when OIG reviews and accepts documentation showing that security impact analyses were performed in accordance with NIST SP 800-53, Revision 3, controls.

(U) Finding B. Plan of Action and Milestones

(U) OIG first identified POA&M deficiencies in FY 2010, and many of these same deficiencies remained in FY 2013. OMB Memorandum M-02-01¹⁵ states, “The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.” In addition, according to OMB Memorandum M-04-25,¹⁶ POA&Ms must be tied to the agency’s budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.

(U) The Department made progress in its POA&M process. However, the Department did not effectively manage the POA&M process to capture necessary elements for remediation and capital planning. The CIO could not mandate and/or require system owners to follow the Department’s policies. In addition, various bureau system owners failed to follow the Department’s policy of completing all the necessary elements of a POA&M. The Department entities involved included the Bureau of Consular Affairs; IRM; the Bureau of International Narcotics and Law Enforcement Affairs; the Bureau of Human Resources; the Foreign Service

¹⁵ (U) OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, sec. Preparing and Submitting Security Plans of Action and Milestones, Oct. 2001.

¹⁶ (U) OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, Aug. 2004.

Institute; the Bureau of the Comptroller and Global Financial Services (CGFS); DS; the Bureau of African Affairs; the Bureau of South and Central Asian Affairs; the Office of the Secretary; the Bureau of Arms Control, Verification and Compliance; and the Bureau of European and Eurasian Affairs. Specifically,

1. (U) For systems that resided on OpenNet:
 - a. (U) System owners and IRM, Office of Information Assurance (IA), closed POA&Ms without implementing the required remediation actions. From a sample of 25 POA&Ms, the evidence of the remediation efforts did not exist for 15 POA&Ms (60 percent). Further, of the 15 POA&Ms, one POA&M (7 percent) did not implement the stated remediation actions prior to closure.
 - b. (U) Although the Bureau of the Comptroller and Global Financial Services was recording and tracking identified security weaknesses, OIG noted the master POA&M database excluded findings identified in an FY 2012 financial statement audit report.¹⁷
 - c. (U) System owners did not record and track all identified security weaknesses. Specifically, the POA&M databases, provided by system owners to IRM/IA, excluded findings identified from DS vulnerability assessments.
 - d. (U) System owners did not adhere to established completion dates. Specifically, from a sample of 25 completed POA&Ms, nine POA&Ms (36 percent) exceeded 90 days or more from the scheduled completion date. Of those nine actions, three (33 percent) exceeded 365 days or more from the scheduled completion date.
 - e. (U) System owners did not provide realistic completion dates. Specifically, from the 25 POA&Ms sampled, the scheduled completion date for six POA&Ms (24 percent) exceeded 365 days from the creation date. Of those six POA&Ms, two POA&Ms (33 percent) exceeded 2,000 days from the POA&M creation date.
 - f. (U) System owners did not consistently update all POA&M fields. Specifically,
 - i. (U) Of 25 POA&Ms sampled, 24 (96 percent) did not have resources budgeted (that is, no data or zero in the action budget field).
 - ii. (U) For 365 (44 percent) of 832 actions completed in FY 2013 in the POA&M database, system owners did not consistently record Unique Investment Identifiers (UII).¹⁸ For example:

¹⁷ (U) Office of Audits, *Audit of Department of State FY 2012 Compliance With Improper Payments Requirements* (AUD-FM-13-23, Mar. 2013).

¹⁸ (U) A Unique Investment Identifier refers to a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years of an agency's investment portfolio.

- (U) 286 (78 percent) of 365 actions were reported as “N/A (OIG Report/Site Risk Scoring exceptions),”
 - (U) 41 (11 percent) of 365 actions were reported as “no Major investment,”
 - (U) 32 (9 percent) of 365 actions were reported as “not provided.”
- g. (U) In addition, our review of the capital planning process for sampled information technology investments found that the CIO did not integrate the POA&M information, including costs and resources for corrective actions, into the capital planning process. Furthermore, the Department did not cross-reference the POA&Ms to the budget submissions with a UII.
- h. (U) Bureaus and/or offices did not provide remediation plans to the Chief Information Security Officer to close outstanding POA&Ms. Specifically, for quarter one of FY 2013, 10 (50 percent) of 20 bureaus and/or offices did not provide complete plans of action (that is, not all posts for the bureau reported their plans) to close outstanding POA&Ms. For the second quarter of FY 2013, 5 (24 percent) of 21 bureaus and/or offices did not provide complete plans of action.
2. (U) For systems residing on ClassNet:
- a. (U) From a sample of 25 POA&Ms, system owners did not provide scheduled completion dates for 12 POA&Ms (48 percent) with corrective actions taken.
 - b. (U) System owners did not consistently update all POA&M fields. Specifically,
 - i. (U) Of 25 POA&Ms sampled, one action (4 percent) did not have resources budgeted.
 - ii. (U) Of 25 POA&Ms sampled, system owners did not consistently record UIIs for 23 POA&Ms (92 percent).
 - c. (U) System owners did not provide realistic scheduled completion dates based on Department policies for implementing patches. Specifically, the scheduled completion date for 7 (28 percent) of 25 POA&Ms sampled exceeded 200 or more days from the POA&M creation date.

(U) The Clinger Cohen Act¹⁹ states:

(U) The Chief Information Officer of an executive agency shall be responsible for (1) providing advice and other assistance to the head of the executive agency and

¹⁹ (U) The Clinger-Cohen Act, *Information Technology Management Reform*, sec. 5125, Agency Chief Information Officer, Feb. 1996. The Clinger-Cohen Act was formerly titled the Information Technology Management Reform Act.

other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with chapter 35 of title 44, United States Code, and the priorities established by the head of the executive agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.

(U) The *Foreign Affairs Manual* (FAM), 1 FAM 040,²⁰ states, “The head of IRM, when carrying out the functions of the Chief Information Officer as established by the Clinger-Cohen Act, reports directly to the Secretary.”

(U) OMB Memorandum M-11-33²¹ states, “While agencies are no longer required to follow the exact format prescribed in the POA&M examples in OMB Memorandum 04-25,²² they must still include all of the associated data elements in their POA&Ms. The required data elements are weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status.”

(U) Furthermore, the Department’s POA&M Toolkit states:

- (U) To Close a POA&M action all the fields for Remediation (Milestone 2) and Verification (Milestone 3) must be completed. The “Completed By” field is designated for the name of the individual who performs the Actual Remediation (e.g. System Administrator). It must then be verified by someone other than the person who performed the remediation (e.g. Information Systems Security Officer).²³
- (U) A POA&M is a mutual commitment made between remediators who promise management that the security weakness will be corrected by the due date and management who promise remediators that the specified resources will be provided.²⁴
- (U) Quarterly grade memos will be sent to Bureau Executives on the quality of the Bureau POA&M process implementation. The grade memos will cover:
 - (U) timely and complete identification of weaknesses,

²⁰ (U) 1 FAM 044.2a.4, *The Under Secretaries of State*, Jan. 2013.

²¹ (U) OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept. 2011.

²² (U) OMB Memorandum M-04-25.

²³ (U) *POA&M Toolkit*, sec. How does a Bureau (and its Information System Owners) record that POA&M actions are closed.

²⁴ (U) *POA&M Toolkit*, sec. Why is the process to manage POA&Ms and their actions important?.

- (U) development of remediation plans,
- (U) implementation of remediation, and management of weaknesses (including timely and complete quarterly updates of status).²⁵

(U) The CIO did not effectively execute his authority or exert influence, as a direct report to the Secretary, to ensure that Department bureaus complied with POA&M requirements. As a result, information system owners for the bureaus chose to focus on daily operations instead of devoting resources to

- (U) Consistently validate the accuracy of actions implemented prior to closure.
- (U) Take management action, as needed, to ensure work was completed on schedule.
- (U) Implement a process to enter UII data, including costs, that link POA&Ms to the agency's budget submission.
- (U) Consistently provide the plans of action to resolve open actions to IRM/IA.

(U) Although CGFS was recording, tracking, and communicating identified security weaknesses, IRM/IA did not include those findings within the POA&M database. In addition, IRM/IA and system owners did not have the resources to include the ongoing DS/Security Infrastructure (SI)/Office of Computer Security (CS) vulnerability assessment results within the quarterly updated POA&M database because of the biweekly frequency of the vulnerability assessments performed.

(U) If the CIO, in coordination with system owners, does not adequately identify, assess, prioritize, and monitor corrective actions on an enterprise basis, the most important actions (highest security risks) affecting the Department may not be fully funded or resolved within a timely manner, thus exposing the Department's sensitive data, systems, and hardware to unauthorized access and activities.

(U) Recommendation 4. OIG recommends that the Chief Information Officer exercise the authorities prescribed in the *Foreign Affairs Manual* (1 FAM 040) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plans of Action and Milestones (POA&M); ensure completion dates for corrective actions are adhered to and/or the remediation dates are updated as needed; implement processes and procedures to cross-reference POA&M information, including costs, to the capital planning budget process with a Unique Investment Identifier; and ensure that written responses for the *Quarterly Plan of Action & Milestones Grade* memorandums are provided to the Bureau of Information Resource Management, Office of Information Assurance.

(U) Management Response: IRM stated that it did “not concur in totality with this recommendation.” IRM further stated that the Department “has made and continues to

²⁵ (U) *POA&M Toolkit*, sec. How is the quality of the POA&M process monitored?.

make progress with tracking of POA&Ms” but that it “welcome[s] OIG recommendations on how to do this more effectively.”

(U) OIG Analysis: OIG considers the recommendation unresolved. OIG agrees that progress has been made regarding written responses from system owners for the *Quarterly Plan of Action & Milestones Grade* memorandums since FY 2012. However, many of the same POA&M deficiencies first identified in FY 2010 remained and the Department continued to not capture necessary POA&M elements for remediation and capital planning, which showed a lack of progress in the overall management of POA&Ms. This recommendation can be closed when OIG reviews and accepts documentation showing that POA&Ms are being tracked in accordance with Department policies.

(U) Recommendation 5. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, include the financial statement audit report findings, identified and communicated by the Bureau of Comptroller and Global Financial Services, within the Plan of Action and Milestone database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Management Response: IRM stated, “This recommendation is referred to the Bureau of the Comptroller and Global Financial Services.” IRM further stated that it “will acknowledge that IRM/IA is in receipt of both the report sought during the FISMA review, and the most recent audit report findings. CGFS annually posts the Agency Financial Report to the Department’s web site enabling bureaus and all employee access to this information.”

(U) OIG Analysis: OIG considers the recommendation resolved. OIG modified the recommendation to state that IRM/IA should include the financial statement audit report weaknesses that were identified and communicated by CGFS in the master POA&M database. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the weaknesses identified by CGFS are tracked within the master POA&M database.

(U) Recommendation 6. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify weaknesses resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, and include those weaknesses that are not immediately remediated in the Plan of Action and Milestone database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Management Response: IRM concurred with this recommendation.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IRM/IA, in coordination with system owners, has identified and included weaknesses resulting from

the vulnerability scans performed by DS/SI/CS in the POA&M database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Finding C. Continuous Monitoring

(U) OIG first identified deficiencies in the Department's continuous monitoring effort in FY 2010, and many of those same deficiencies remained in FY 2013. According to NIST SP 800-137,²⁶ information security continuous monitoring is "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

(U) In its FY 2010 report to Congress on FISMA, OMB²⁷ stated that "[a] well designed and well managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real time security status related information" to senior leaders. OMB further stated that senior leaders can use this information to take "appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system."

(U) Although the OCIO, in coordination with the ISSC, was in the process of implementing a continuous monitoring strategy, the Department did not document an overall continuous monitoring strategy.

(U) According to NIST SP 800-53, Revision 3,²⁸ an organization should establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process, security impact analysis, ongoing security control assessment, and reporting the security state of the system to appropriate organizational officials.

(U) Previous Department management did not have a continuous monitoring strategy in place. Although the current CIO, in coordination with the ISSC, was in the process of developing a continuous monitoring strategy, they did not document their envisioned strategy to assist system owners in evaluating various control deficiencies. According to the CIO, the Department was awaiting the implementation of DHS continuous monitoring tools prior to documenting their strategy, with the goal of inheriting DHS strategy.

(U) If a continuous monitoring strategy is not documented, the Department cannot transfer knowledge between rotating senior officials. In addition, a documented strategy will provide stakeholders, system owners, and personnel with a unified understanding of the information system security goals, allowing the Department to consistently monitor a dynamic

²⁶ (U) NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Executive Summary, Sept. 2011.

²⁷ (U) OMB, *Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*, sec. A., Continuous Monitoring and Remediation, Mar. 2010.

²⁸ (U) NIST SP 800-53, rev. 3, CA-7 Continuous Monitoring.

network environment with changing threats, vulnerabilities, technologies, missions, and business functions.

(U) Recommendation 7. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, document an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems and is consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) Management Response: IRM stated that it had provided documentation in 2012.

(U) OIG Analysis: OIG considers the recommendation unresolved. OIG is aware that documentation was provided in 2012, but the documentation provided was still in draft form and had not been formally approved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Chief Information Officer, in coordination with the Information Security Steering Committee, has documented and approved an overall continuous monitoring strategy.

(U) Finding D. Configuration Management

(U) OIG reported in FY 2011 and FY 2012 that the Department had patch management control and configuration management weaknesses. OIG found many of these same deficiencies in FY 2013. According to 5 FAM 1067,²⁹ the installation of critical patches on workstations and servers should be at an installation rate of 100 percent and 90 percent for non-critical patches. According to the Enterprise Patch Management Program Standard Operating Procedures,³⁰ critical patches must be installed within 3 business days, high-risk patches must be installed within 5 business days, medium-risk patches must be installed within 10 business days, and low-risk patches must be installed within 15 business days.

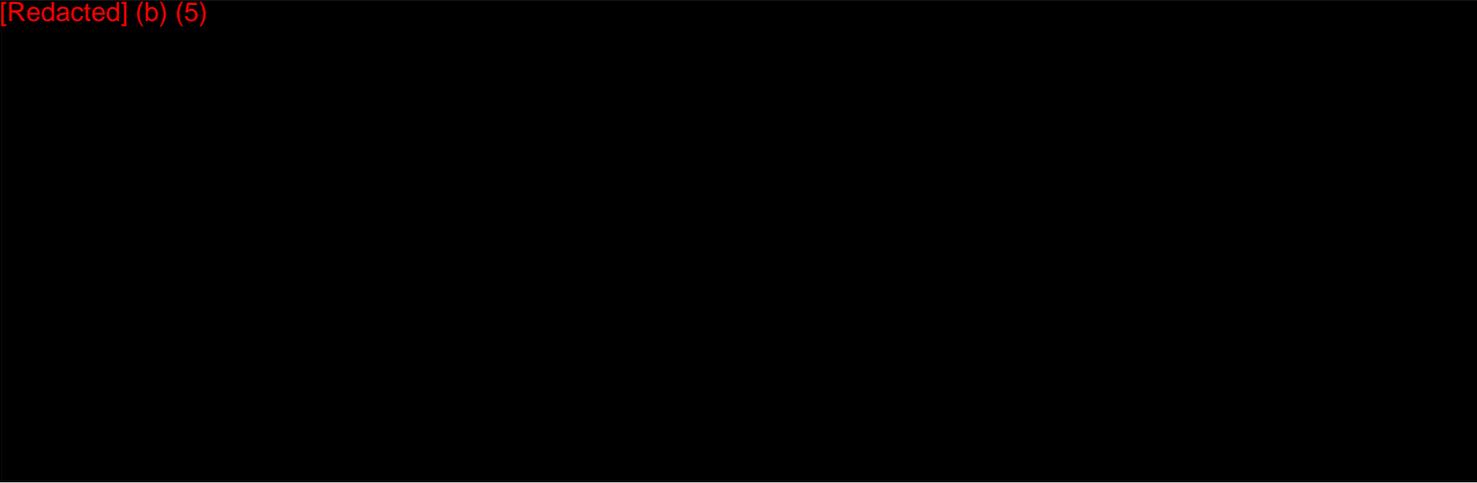
(U) In FY 2013, the CIO had not finalized and implemented the Cyber Security Architecture and initiative for end-to-end configuration management for all of its components. In addition, OIG noted that although the Department had developed and implemented periodic vulnerability and compliance scans using McAfee Vulnerability Management (including Foundstone) and Policy Auditor to address prior audit recommendations, various weaknesses still existed. Specifically,

[Redacted] (b) (5)

²⁹ (U) 5 FAM 1067.3b, *Information Assurance Management*, Jan. 2009.

³⁰ (U) *Enterprise Patch Management Program Standard Operating Procedures*, sec. 6, Delivery Process, Aug. 2007.

[Redacted] (b) (5)



(U) According to NIST SP 800-53, Revision 3,³¹ the organization identifies, reports, and corrects information system flaws.

(U) 5 FAM 866³² states, “Information Management Officers/Information Security Officers/system administrators must follow guidelines and procedures established by the Department’s Enterprise Patch Management Program and apply patches in an expeditious manner.”

(U) NIST SP 800-115³³ states that the organization’s information security assessment policy should identify the following:

- (U) Organizational requirements with which assessments must comply
- (U) Appropriate roles and responsibilities (at a minimum, for those individuals approving and executing assessments)
- (U) Adherence to established methodology
- (U) Assessment frequency
- (U) Documentation requirements, such as assessment plans and assessment results.

(U) According to 5 FAM 1067,³⁴ patch management compliance is:

- (U) (1) For critical patches: achieving and maintaining a patch installation rate of 100%, as designated by the IRM/Operations/Enterprise Network Management (ENM) Office;

³¹ (U) NIST SP 800-53, rev. 3, SI-2 Flaw Remediation.

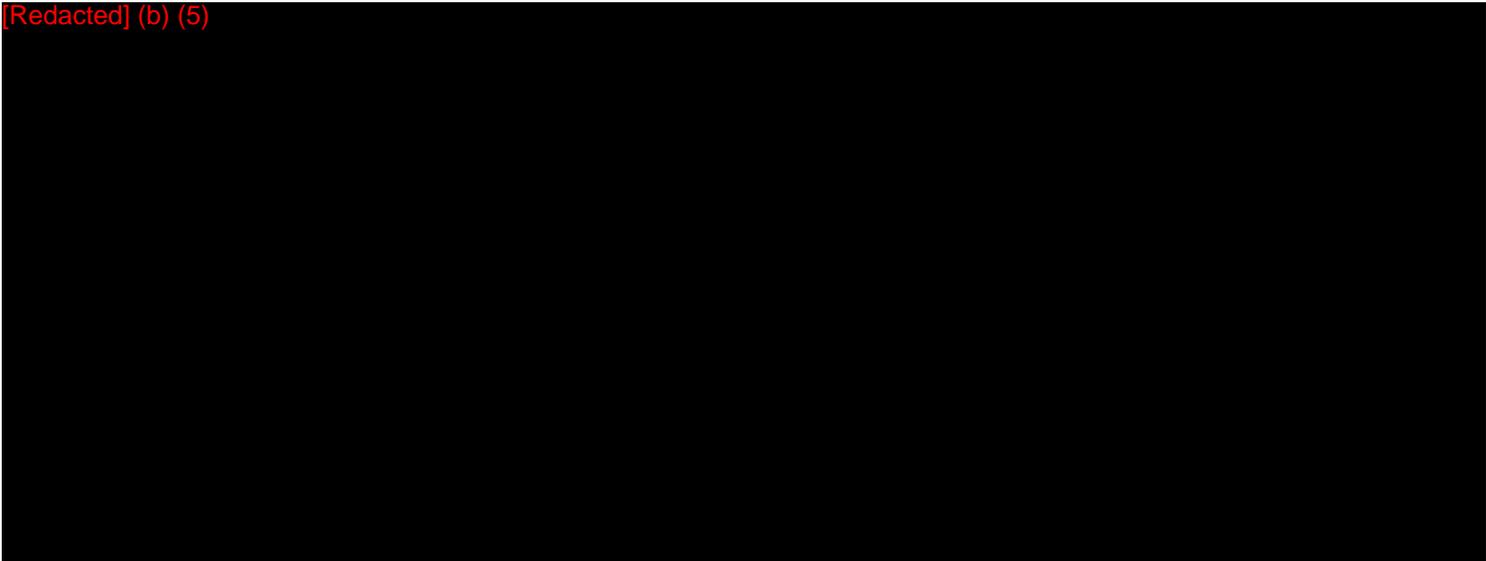
³² (U) 5 FAM 866c, *Hardware and Software Maintenance*, April 2009 (last updated July 2013).

³³ (U) NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, sec. 6.1, Developing a Security Assessment Policy, Sept. 2008.

³⁴ (U) 5 FAM 1067.3b.

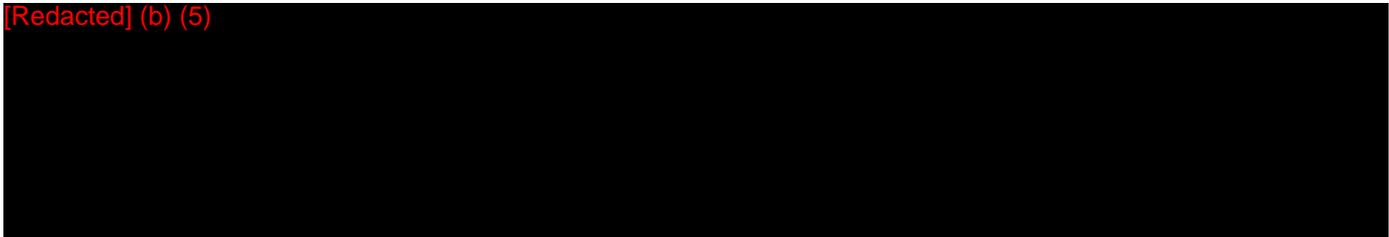
- (U) (2) For all workstations and servers on OpenNet and ClassNet: achieving and maintaining a patch installation rate 90% of all patches within 15 days after patch release.

[Redacted] (b) (5)



(U) Without detailed procedures that govern the performance of routine and critical processes and the awareness of new devices or applications connected to the network, the Department leaves its systems vulnerable to denial of service attacks, damage to the general support systems, and/or the potential introduction of security weaknesses.

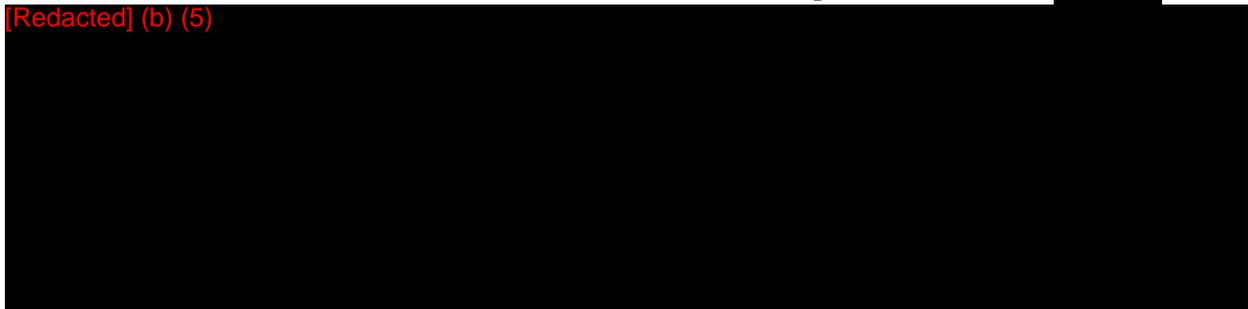
[Redacted] (b) (5)



~~(SBU)~~ **Management Response:** IRM concurred with this recommendation.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation

[Redacted] (b) (5)



³⁵ (U) NIST SP 800-115, sec. 6.1, Developing A Security Assessment Policy.

~~(SBU)~~ **Management Response:** IRM concurred with this recommendation.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation

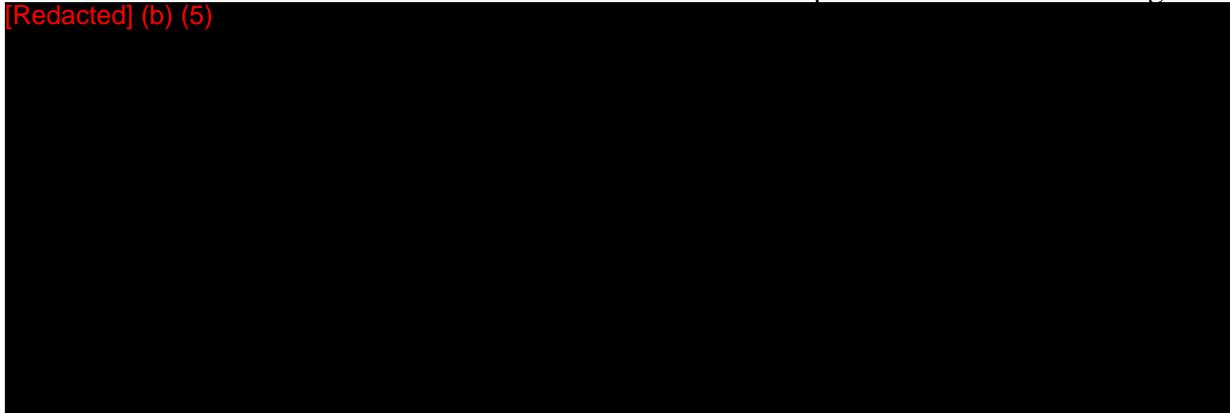
[Redacted] (b) (5)



~~(SBU)~~ **Management Response:** IRM stated that it and DS concurred with this recommendation.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing

[Redacted] (b) (5)



~~(SBU)~~ **Management Response:** IRM stated that it and DS concurred with this recommendation.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation

[Redacted] (b) (5)



~~(SBU)~~ **Management Response:** IRM stated that it and DS concurred with the recommendation [Redacted] (b) (5)

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. [Redacted] (b) (5)

This recommendation can be closed when OIG reviews and accepts documentation [Redacted] (b) (5)

[Redacted] (b) (5)

~~(SBU)~~ **Management Response:** IRM and DS concurred with the recommendation, stating to fully resolve the recommendation, [Redacted] (b) (5)

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation [Redacted] (b) (5)

(U) Finding E. Identity and Access Management

(U) OIG first identified deficiencies in identity and access management in FY 2010, and many of these deficiencies remained in FY 2013. 12 FAM 620³⁶ states that the Department

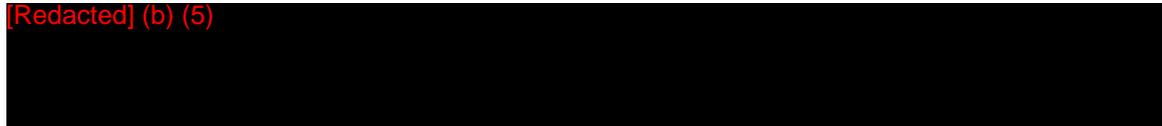
³⁶ (U) 12 FAM 621.1a, *Unclassified Automated Information Systems*, June 2000.

should “ensure that all personnel accessing Department automated information system (AIS) processing resources have:

- (U) (1) The required access levels and need-to-know;
- (U) (2) Appropriate supervision.”

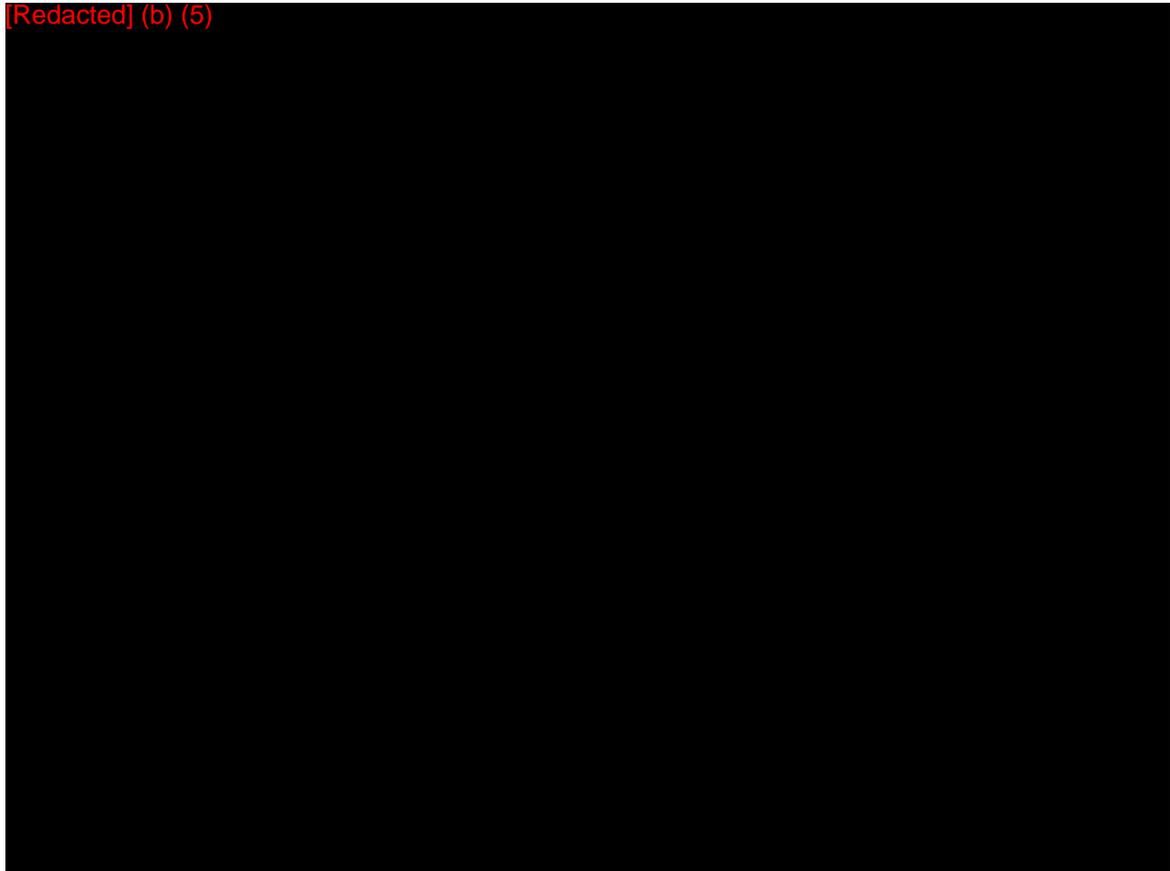
(U) Although OIG found that system owners, in coordination with IRM, improved certain components of monitoring account passwords, the Department did not have effective identity and access management of their information systems. Specifically,

[Redacted] (b) (5)



- 2. (U) System owners did not provision user accounts effectively for OpenNet and ClassNet AD accounts. 

[Redacted] (b) (5)



(U) 12 FAM 620,³⁹ in regard to obtaining administrative access, states:

(U) c. The form must include the user’s name, the applications involved, and the type of access required within each application. Whenever a user’s functional

³⁷ (U) Accounts include User, Service, and Mailbox accounts.

³⁸ (U) Ibid.

³⁹ (U) 12 FAM 629.2-1c-d.

responsibilities change and the user still requires system access, the user's current supervisor must complete a new system access request form for access privileges commensurate with the user's new responsibilities.

(U) d. The data center manager and the system manager must sign the access request form when the information provided is adequate, indicating approval for AIS access. The data center manager and the system manager retain all approved AIS access request forms for at least six months after the date of removal from the AIS.

(U) 12 FAM 620,⁴⁰ in regard to termination of accounts, states:

(U) Personnel officers must include the data center manager and the system manager on the bureau or post check-out list, to ensure notification of all employees (U.S. and non-U.S. citizen) and contractors who are transferred or terminated. The data center manager and the system manager, in conjunction with the ISSO, must revoke user access privileges for these personnel. Furthermore, "The data center manager and the system manager must immediately delete individual user IDs and passwords under the following conditions:

(U) (1) Whenever notified by a user's supervisor that the user no longer requires AIS access; or

(U) (2) Whenever notified by a proper authority, such as the human resources officer, that the user's employment has been terminated with the Department or has been transferred to another office or post."⁴¹

(U) Further, 12 FAM 620,⁴² states:

(U) The ISSO must review monthly the audit reports for potential security-related incidents such as:

(U) (1) Multiple logon failures;

(U) (2) Logons after-hours or at unusual times;

(U) (3) Failed attempts to execute programs or access files;

(U) (4) Addition, deletion, or modification of user or program access privileges; or

(U) (5) Changes in file access restrictions.

(U) 12 FAM 620,⁴³ in regard to obtaining access, states, "Supervisors must complete a system access request form for each staff member who requires AIS access."

⁴⁰ (U) 12 FAM 621.3-3.

⁴¹ (U) 12 FAM 622.1-3g.

⁴² (U) 12 FAM 629.2-7b.

⁴³ (U) 12 FAM 622.1-2b.

(U) NIST SP 800-53, Revision 3,⁴⁴ states, “The information system automatically disables inactive accounts after [Assignment: organization defined time period].”

(U) All Diplomatic and Consular Posts (ALDAC) Telegram 2008 STATE 8277⁴⁵ states, “...implement the following password requirements for users, local PC accounts and Active Directory service accounts”

(U) “...Maximum password age 60 days.”

(U) The AD Password Requirements Standard Operating Procedure⁴⁶ states, “All AD accounts are required to change the password every 60 days, per Department policy. This includes administrative, service, and mailbox accounts that manage various systems and applications.”

(U) 12 FAM 620,⁴⁷ in regard to password requirements, states, “The data center manager and the system manager must initially assign a unique user ID and password to each new authorized user. The data center manager and the system manager must ensure that all passwords are changed under the following conditions:

(U) (1) At least once every 60 days.”

(U) Further, “...The data center manager and the system manager must ensure that the following are the minimum required settings.

(U) (1) The maximum password age must be set to 60 days.”

(U) 12 FAM 630,⁴⁸ specific to classified systems, states, “The system administrator must ensure that accounts are temporarily disabled after 90 days of inactivity. Before reactivating the account, the user’s supervisor must recertify in writing, e.g., via email or memo that the user still requires the account.”

(U) The Active Directory and Global Address List (GAL) Standardization states:

- (U) “Secondary User Accounts must be located in the **Admin Accounts** Organizational Unit (OU) within the site’s OU structure.”⁴⁹
- (U) “Shared Mailbox Accounts must be located in a sub-OU of the Users OU within the site’s OU structure. The sub-OU must also be named **MAILBOXES.**”⁵⁰

⁴⁴ (U) NIST SP 800-53, rev. 3, AC-2 Control Enhancement 3.

⁴⁵ (U) ALDAC Telegram 2008 STATE 8277, *Change to Password Policy*, sec. 1, Jan. 2008.

⁴⁶ (U) *AD Password Requirements SOP*, sec. 2, Background, Feb. 2013.

⁴⁷ (U) 12 FAM 622.1-3a.

⁴⁸ (U) 12 FAM 632.1-3h, *Classified Automated Information Systems*, May 2013.

⁴⁹ (U) Active Directory and GAL Standardization, sec. 2.2.2, OU Location, Feb. 2012.

⁵⁰ (U) *Ibid.*

(U) ALDAC Telegram 2009 STATE 101353⁵¹ states, “IRM's Enterprise Network Management (IRM/OPS/ENM) and Information Assurance (IRM/IA) offices have documented the information that must be included in AD and created the 'Department of State Global Address List and Active Directory Standardization' document. This document provides the information needed to accurately manage user accounts in AD.”

(U) The Department used a decentralized process to manage the AD, which resulted in the mismanagement of user accounts by system owners. Specifically,

1. (U) System owners failed to comply with the documented policy, which caused them to require users to complete the appropriate access forms (that is, for new user access and elevated rights) inconsistently prior to granting access.
2. (U) IRM did not consistently provide termination reports to applicable system owners to ensure the timely removal of accounts for departing or transferring employees.
3. (U) Management did not consistently review the AD OU structuring, which aids account administration across the enterprise, to ensure alignment with the Department's Active Directory and GAL Standardization guidelines.

(U) In addition, 12 FAM 620 does not define a time period for disabling inactive accounts for unclassified systems. Further, 12 FAM 620 is ambiguous in that it does not define all the accounts (that is, user/service/mailbox) that must comply with account password requirements.

(U) Without effective identity and access management, the risk of unauthorized access is significantly increased. Unauthorized access may result in the submission of false transactions, improper access, dissemination of confidential data, and other malicious activities.

(U) **Recommendation 14.** OIG recommends system owners (bureaus and posts) follow the *Foreign Affairs Manual* (12 FAM 620) to have the supervisor complete the appropriate system access forms (for example, new user access and elevated rights) prior to granting access.

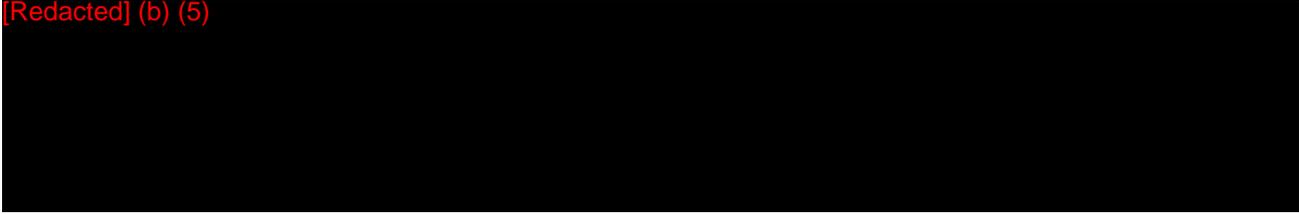
(U) **Management Response:** IRM stated that it and DS believe that this is a “prudent action and look to the OIG to audit these during their audit of bureaus and posts.”

(U) **OIG Analysis:** OIG considers the recommendation unresolved. The FAM requires supervisors to complete a system access request form for each new user and/or users who require elevated system access. Without proper approval, unauthorized access may result in the submission of false transactions, improper access, dissemination of confidential data, and other malicious activities. In addition, system owners are required to perform user provisioning functions and should not rely upon OIG to ensure that appropriate access was granted for authorized users. This recommendation can be closed when OIG

⁵¹ (U) ALDAC Telegram 2009 STATE 101353, *User Account Objects Standardization*, sec. 1 and 2, Sept. 2009.

reviews and accepts documentation showing that supervisors have completed appropriate system access forms prior to granting system access in accordance with 12 FAM 620.

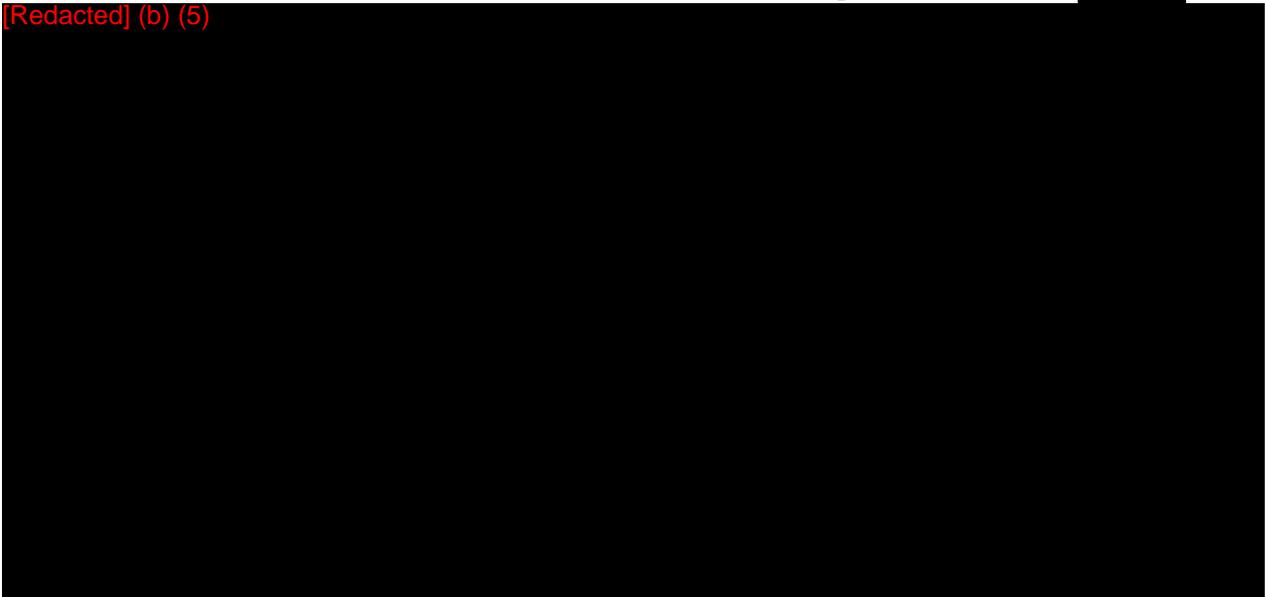
[Redacted] (b) (5)



~~(SBU)~~ **Management Response:** IRM concurred with this recommendation.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation

[Redacted] (b) (5)



~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation unresolved.

[Redacted] (b) (5)



This recommendation can be closed when OIG reviews and accepts documentation

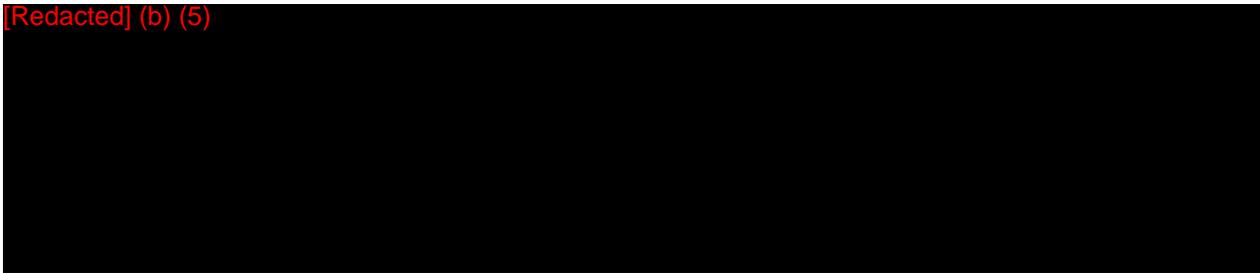
[Redacted] (b) (5)

(U) Recommendation 17. OIG recommends that management review their Active Directory Organizational Units structure and correct any Organizational Units that do not follow the guidance stated within the Active Directory and Global Address List Standardization.

(U) Management Response: IRM did not concur with this recommendation, stating that it believes “it is impractical in the Department’s environment and also suggest with the appropriate implementation of recommendations 14 and 15 the risk can be adequately managed.”

(U) OIG Analysis: OIG considers the recommendation unresolved. This recommendation is not impractical because IRM management already provided the Active Directory and Global Address List Standardization procedures to system owners and posts since 2009. In addition, following these standards will 1) ensure uniformity of AD user and computer account information across the Enterprise; 2) allow for accurate scoring with regard to AD user and computer account risk components; 3) aid ISSOs at sites to better track what users within their purview have taken the annually required CyberSecurity Awareness Training and those that have not; and 4) make searches on fields through Outlook on the Global Address List relevant when searching for employees and offices by job title, location, and in some cases, function. This recommendation can be closed when OIG reviews and accepts documentation showing that AD user account objects that are managed by the OU at posts and sites are standardized.

[Redacted] (b) (5)



~~(SBU)~~ **Management Response:** In its response, IRM provided DS’s response to the recommendation. DS stated that it “deems this recommendation resolved.”

[Redacted] (b) (5)



~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation

[Redacted] (b) (5)



(U) Finding F. Contingency Planning

(U) OIG first identified deficiencies in the contingency planning process in FY 2010, and many of these same deficiencies remained in FY 2013. NIST SP 800-34, Revision 1,⁵² states:

(U) ...contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.

(U) System owners, in coordination with IRM/IA, did not develop the information system contingency plans (ISCP) in accordance with 6 FAM 400,⁵³ NIST SP 800-34, Revision 1,⁵⁴ and NIST 800-53, Revision 3.⁵⁵ Specifically,

1. (U) Ten (63 percent) of 16 OpenNet systems had not conducted annual contingency plan testing.
2. (U) Thirteen (81 percent) of 16 OpenNet system contingency plans had not been approved.
3. (U) Six (38 percent) of 16 OpenNet system contingency plans had not identified an alternate processing site, alternate storage site, and alternate telecommunications services separate from the primary site.
4. (U) Ten (63 percent) of 16 OpenNet systems had not provided backup logs as evidence that a backup had been performed within a period of 6 months.
5. (U) For the 16 OpenNet systems, seven (88 percent) of eight Bureau Emergency Action Plans (BEAP) had not been reviewed, updated, and certified on an annual basis.

(U) NIST SP 800-34, Revision 1,⁵⁶ regarding ISCP approval, states:

(U) An up-to-date ISCP is essential for successful ISCP operations. As a general rule, the ISCP should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the ISCP, system, mission/business processes supported by the system, or resources used for recovery procedures. Deficiencies identified through testing should be addressed during plan maintenance. Elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently.

⁵² (U) NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, Executive Summary, May 2010.

⁵³ (U) 6 FAM 416.1-3a-3, *General Services and Domestic Emergency Management*, May 2012.

⁵⁴ (U) NIST SP 800-34, rev. 1, Appendix C bullet 13.

⁵⁵ (U) NIST SP 800-53, rev. 3, CP-2 Contingency Plan.

⁵⁶ (U) NIST SP 800-34, rev. 1, Appendix C bullet 13.

(U) 5 FAM 1064,⁵⁷ states:

(U) a. System owners and non-Department entities (i.e., organizations, individuals, or other agencies) that process Federal information on behalf of the Department must:

(U) (1) Develop and maintain contingency plans for the major applications and general support systems under their control that process, store, or transmit Federal information;

(U) (2) Use the Department's Contingency Plan (CP) template to prepare the contingency plan (see the Contingency Plan template available on the Information Assurance IRM/IA Web site);

(U) (3) For purposes of inspection, retain copies of the contingency plan and test results for the life of the system;

(U) (4) Update and test the contingency plan when the major application or general support system has undergone a major change to its operational baseline configuration; and

(U) (5) For moderate and high impact systems, test the contingency plan at least annually to verify the entities' ability to recover and/or restore the application or system to operation in the event of a system or application failure.

(U) b. IRM/IA will assess system security, contingency planning, and continuity of operations efforts, and assist system owners in correcting deficiencies.

(U) NIST SP 800-53, Revision 3,⁵⁸ states, "the contingency plan is reviewed and approved by designated officials within the organization."

(U) The *FAM*, 6 FAM 400⁵⁹ states that the Bureau Emergency Action Committee (EAC) responsibilities include "(3) coordinating with the EAC Chairperson to ensure the BEAP is exercised and certified on an annual basis."

(U) 12 FAM 620⁶⁰ states, "The data center manager and the system manager must ensure that a system operations log is maintained for all AISs. The log must contain a record of all normal daily operations, system power-up and power-down, media mounted and dismounted, backup and recovery operations, and general environmental conditions. Installation, removal, or modification of system or application software must be noted in the log. Any unusual events or operating conditions must also be noted in the log. The data center manager and the system manager must ensure that logs are maintained for a minimum of six months after the date of the last entry."

(U) According to an IRM management official, system owners did not prioritize resources to complete the annual requirements for review and certification of system contingency

⁵⁷ (U) 5 FAM 1064.2.

⁵⁸ (U) NIST SP 800-53, rev. 3, CP-2 Contingency Plan.

⁵⁹ (U) 6 FAM 416.1-3a-3.

⁶⁰ (U) 12 FAM 629.2-11.

plans that included establishing an alternate site strategy, conducting an annual contingency plan test, and validating system backups.

(U) According to IRM management officials, the Office of Emergency Management, in coordination with the Bureau EAC and the EAC Chairperson from each bureau, did not prioritize resources to consistently review, update, and certify the BEAP annually in accordance with 6 FAM 400.⁶¹

(U) Without effective contingency plans that include an established alternate site strategy, the Department may be unable to access critical information and resources to perform mission critical business functions in the event of an extended outage and/or disaster.

(U) Recommendation 19. OIG recommends that the system owners, in coordination with Chief Information Officer and the Bureau of Information Resource Management, Office of Information Assurance, perform and review contingency plan testing annually, including validating system backups and establishing an alternate site strategy in accordance with the *Foreign Affairs Manual* (5 FAM 1064), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Management Response: IRM did not agree with this recommendation, stating that it “believes this responsibility should be with the system owner with a report back to IRM/IA.”

(U) OIG Analysis: OIG considers the recommendation unresolved. 5 FAM 1064 requires that system owners develop and annually test contingency plans. In addition, 5 FAM 1064 requires IRM/IA to ensure contingency planning and continuity of operations efforts are in compliance and assist system owners in correcting deficiencies. OIG has modified the recommendation to state that the system owners, in coordination with the CIO and IRM/IA, should perform and review contingency plan testing annually, including validating system backups and establishing an alternate site strategy in accordance with the *Foreign Affairs Manual* (5 FAM 1064), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Recommendation 20. OIG recommends that the Chief Information Officer, in coordination with the contingency planning coordinator, identify an alternate processing site, alternate storage site, and alternate telecommunications servers for each system in accordance with National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) Management Response: IRM stated that it did “not agree with this overly broad recommendation.” IRM further stated that it “has worked with Bureau of Administration,

⁶¹ (U) 6 FAM 416.1-3a-3.

Office of Emergency Management as appropriate and system owners in their design to meet continuity requirements.”

(U) OIG Analysis: OIG considers the recommendation unresolved. OIG does not agree that this recommendation is overly broad. NIST SP 800-34, Revision 1, specifically requires that an alternate processing site, alternate storage site, and alternate telecommunications services be identified for moderate or higher impact systems. This recommendation can be closed when OIG reviews and accepts documentation from the CIO and contingency planning coordinator showing that alternate processing sites, alternate storage sites, and alternate telecommunications servers have been identified for each system in accordance with NIST SP 800-34, Revision 1.

(U) Recommendation 21. OIG recommends that the Office of Emergency Management, in coordination with the Emergency Action Committee for each bureau, conduct its annual review and certify its Bureau Emergency Action Plans in accordance with the *Foreign Affairs Manual* (6 FAM 400).

(U) Management Response: IRM stated that Bureau of Administration, Office of Emergency Management, had not provided a response to the recommendation but that IRM “will work with this office to prepare for response to the final report.”

(U) OIG Analysis: OIG considers the recommendation unresolved because management did not provide an actionable response, which would state the responsible party and specific tasks to implement the recommendation.

(U) Recommendation 22. OIG recommends that data center managers enforce the log and record keeping policy to show that system backups are being performed in accordance with the *Foreign Affairs Manual* (12 FAM 620).

(U) Management Response: IRM stated that its data center managers “provide different levels of service for different systems, from hosting to completely managed service.” IRM further stated, “For those systems IRM provides a managed service, IRM concurs with this recommendation and believes it is being accomplished.”

(U) OIG Analysis: OIG considers the recommendation unresolved. OIG modified the recommendation to replace “audit trail/log” with “log and record keeping” to show evidence that backups are being performed. This recommendation can be closed when OIG reviews and accepts documentation showing that the data center managers have enforced the log and record keeping for system backups in accordance with 12 FAM 620.

(U) Finding G. Contractor Systems

(U) OIG first identified deficiencies in contractor systems oversight in FY 2010, and many of these same deficiencies remained in FY 2013. The *FAM*, 5 FAM 600,⁶² states, “All

⁶² (U) 5 FAM 611e, *Information Technology Systems*, June 2009.

systems (including applicable contractor systems) and applications associated with any projects must be registered in Information Technology Applications Baseline (ITAB).” ITAB is the former name of the iMatrix application.

(U) The Department had not followed policies and procedures for managing its contractor and government extensions. Specifically,

- (U) IRM and DS maintained separate contractor extension inventory lists, which resulted in discrepancies.
- (U) Some contractor extensions were not documented within iMatrix, which is the Department’s official system of record for extensions.
- (U) As of September 20, 2013, the annual data call memorandum⁶³ to all posts, instructing them to verify existing IT assets and add any new assets hosted by post within iMatrix, was not followed for FY 2013, resulting in an incomplete tracking of inventory within iMatrix.

[Redacted] (b) (5)

- (U) DS/SI/CS did not complete the annual physical inspections for two of the three sampled Government extensions.
- (U) Of three sampled government extensions, two (67 percent) extensions did not specify the clearance requirements within their respective Memorandum of Understanding, as required by 5 FAM 1065.⁶⁴
- (U) For one government extension, 36 (77 percent) of 47 OpenNet users did not comply with the clearance requirements within the Memorandum of Understanding.

(U) 5 FAM 1065⁶⁵ states, “Connectivity requests must include:”

(U) For commercial contractors and consultants with contractual relations with the Department, Form DD-254, Contract Security Classification Specification, or other document containing contract security requirements language specifying all information contained in a connectivity MOA/MOU and ISA.

(U) There was no single resource that managed oversight of contractor and Government extensions within the Department, which caused a lack of communication between IRM, accountable bureaus, and DS. DS maintained its own list of contractor extensions, which was the basis for its yearly reviews. However, by policy, IRM should have the official listing of extensions within iMatrix. Prior to FY 2013, there was no dedicated resource within IRM to work between the two groups. As a result, not all updates were uploaded into iMatrix. In addition, IRM tracked extensions only at contractor sites and third-party vendor sites. IRM did

⁶³ (U) ALDAC Telegram 2012 STATE 15120, *Annual Information Systems Inventory Data Call*, Feb. 2012.

⁶⁴ (U) 5 FAM 1065.3-1b(3), *Risk Management*, Jan. 2009.

⁶⁵ (U) 5 FAM 1065.3-1b(3).

not consider Government agencies (Government extensions) as contractors and therefore did not keep track of them, as required by 5 FAM 600.

(U) DS, in coordination with the Bureau of Resource Management, did not verify completion of required International Boundary and Water Commission background screenings prior to granting employees access to OpenNet.

(U) By not following Department policies for contractor and Government extensions, the Department has minimal assurance that the contractors' information security controls are compliant with FISMA and OMB requirements and NIST standards. In addition, there are increased risks to Department data that is collected, processed, and maintained by contractor systems, which may be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction. The lack of information security requirements in contracts may cause contractor systems to possess lower security requirements and thus make them untrusted systems. Without adequate oversight of contractor and Government extensions, the Department increases the risk of its overall security posture and is exposed to an increased threat of unauthorized access, use, disclosure, disruption, modification, and destruction of data.

(U) **Recommendation 23.** OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, consolidate and track all extensions (for example, contractor sites, other Government agencies, and third-party vendors) within iMatrix, in accordance with the *Foreign Affairs Manual* (5 FAM 600).

(U) **Management Response:** IRM stated, "All extensions have been entered into iMatrix and DS reviews all extensions annually."

(U) **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that all extensions have been entered into iMatrix.

(U) **Recommendation 24.** OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, ensure that annual physical inspections are completed for all OpenNet and ClassNet extensions as defined within each Memorandum of Understanding.

(U) **Management Response:** IRM stated, "The annual physical inspections for OpenNet and ClassNet have either been completed, or are scheduled and currently in process." IRM further stated that it had previously provided OIG documentation confirming the status of physical inspections.

~~(SBU)~~ **OIG Analysis:** OIG considers the recommendation unresolved. [Redacted]

[Redacted] (b) (5)

[Redacted] This recommendation can be closed when OIG reviews and accepts documentation [Redacted] (b) (5)

(U) Recommendation 25. OIG recommends that the Bureau of Diplomatic Security, in coordination with the applicable bureau Information System Security Officers for each contractor and government extension, ensure that all Memorandums of Understanding for extensions contain the required clearance levels for users and that those users are cleared as defined in the *Foreign Affairs Manual* (5 FAM 1065).

(U) Management Response: In its response, IRM provided DS's response to the recommendation. DS concurred with this recommendation, stating that a process was already in place. DS further stated that ISSOs are responsible for identifying all users that require access to OpenNet, the DS Office of Personnel Security and Suitability (DS/SI/PSS) ensures that all Memoranda of Understanding for extensions contain the required clearance levels of users, and that those users have the appropriate clearance."

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that all Memorandums of Understanding for extensions contain the required clearance levels for users and that those users have been cleared as defined in 5 FAM 1065.

(U) Recommendation 26. OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Resource Management, suspend user accounts for unverified individuals at the International Boundary and Water Commission until the required background screenings are completed as required by the Memorandum of Understanding.

(U) Management Response: In its response, IRM stated that CGFS did not concur with this recommendation. IRM further stated that IBWC "is actively and aggressively pursuing adjudication for users of the Global Financial Management System at the IBWC" and that 17 of 22 users had been adjudicated as of October 17 with the remaining five users expected to be adjudicated "in the very near future."

(U) OIG Analysis: OIG considers the recommendation unresolved. Full action has not been completed for this recommendation, and the number of users in management's response does not match the number of users identified in the International Boundary and Water Commission audit. This recommendation can be closed when OIG reviews and accepts documentation showing that required background screenings for all users have been completed as required by the Memorandum of Understanding.

(U) Finding H. Security Training

(U) NIST SP 800-16⁶⁶ states, “Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.”

(U) OIG found that IRM/IA, in coordination with DS/SI/CS, did not have an effective security awareness program. Specifically, key IT personnel with security responsibilities for the Department had not taken specialized, role-based security training. In addition, DS did not fully implement a tracking mechanism for role-based training.

(U) NIST SP 800-53, Revision 3,⁶⁷ states, “The organization provides role-based security-related training before authorizing access to the system.”

(U) The *FAM*, 5 FAM 1067,⁶⁸ states, “Training programs must include specific role-based security training for identified Department personnel with significant information security responsibilities. The Department of State IA Training plan identifies the training requirements.”

(U) NIST SP 800-53, Revision 3,⁶⁹ states, “The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.”

(U) The IA training plan⁷⁰ states, “Among the CISO’s responsibilities is the need to ensure sufficient Information Assurance training for all Department of State system users. This includes general awareness training, as well as specific role based training for those with significant information security responsibilities.”

(U) The CIO, in coordination with IRM/IA and DS/SI/CS, had not finalized the IA training plan for all key IT personnel to include the required role-based training courses. In addition, DS had not prioritized resources to properly track key personnel with security responsibilities.

(U) Without the completion of role-based security training, IT and security personnel may be unaware of risks that may compromise the confidentiality, integrity, and availability of data.

(U) Recommendation 27. OIG recommends the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of

⁶⁶ (U) NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, sec. 1.1, April 1998.

⁶⁷ (U) NIST SP 800-53, rev. 3, AT-3 Security Training.

⁶⁸ (U) 5 FAM 1067.2-2c.

⁶⁹ (U) NIST SP 800-53, rev. 3, AT-4 Security Training Records.

⁷⁰ (U) IA Training Plan, sec. 5.0, Training/Education, FY 2007.

Information Assurance, and the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities take specialized, role-based security training, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Management Response: IRM concurred with the recommendation, stating that the plan had been finalized and was in the clearance/review process.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Information Assurance Training Plan has been finalized and approved.

(U) Recommendation 28. OIG recommends the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, implement a tracking mechanism for role-based training to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Management Response: IRM concurred with this recommendation.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that a tracking mechanism for role-based training has been implemented to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan in accordance with the NIST SP 800-53, Revision 3.

(U) Finding I. Remote Access Management

(U) 12 FAM 680⁷¹ states, “Remote access refers to accessing Department Sensitive but Unclassified (SBU) and Unclassified networks, either domestically or abroad, from non-Department systems (e.g., personally-owned or public access computers, PDAs, laptops, multi-function cell phones, etc.) via a Department-approved remote access program.” In previous years, the Department-approved remote access system was OpenNet Everywhere (ONE); however, on November 11, 2011, ONE was decommissioned and replaced by GO.

(U) According to the ALDAC Telegram 2011 STATE 83703,⁷² with the implementation of GO, the Department “replaces the previous safeword fobs with RSA SecurID tokens, which are not compatible with ONE and are designed to align with the latest federal security requirements. Additionally, the technology of the more secure RSA-based tokens and the tighter

⁷¹ (U) 12 FAM 682.1b, *Remote Access and Mobile Computing Technology*, Aug. 2008.

⁷² (U) ALDAC Telegram 2011 STATE 83703, *Global OpenNet Deployment Update – RSA Tokens*, Aug. 2011.

integration of the two authentication factors prevent the sharing option used with fobs.” RSA tokens are used to authenticate and remotely access the network.

(U) The *FAM*, 12 FAM 680 and 5 FAM 460, still referred to ONE as the Department-approved remote access system and directed users to follow the ONE enrollment process. However, on November 11, 2011, ONE was decommissioned and replaced by GO, which includes the GO enrollment system, Mobile Computing Management System (MCMS).

(U) 5 FAM 460,⁷³ states, “Remote access: Use the methods provided by the OpenNet Everywhere (“ONE”) Program for the secure remote access of PII on the Department’s SBU network, OpenNet, from any Internet-connected computer meeting the system requirements for ONE. To enroll in ONE, you must follow the ONE Enrollment Process.”

(U) 12 FAM 680,⁷⁴ states, “Remote access to Department networks from non-Department-owned systems (e.g., personally-owned or public access computers) is only authorized via Department-approved remote access programs (e.g., OpenNet Everywhere (ONE)).”

(U) According to the ALDAC Telegram 2011 STATE 00891,⁷⁵ ONE services were closed during the fourth quarter of FY 2011 and GO became the only approved remote access method for the Department.

(U) According to an IRM management official, DS and IRM/Operations/Messaging Systems Office/E-Mail Operations Division/Mobile Computing did not prioritize tasks to update 12 FAM 680 and 5 FAM 460. Specifically, 12 FAM 680 and 5 FAM 460 should consider the retirement of ONE and state the utilization of GO, including the MCMS enrollment process, as the only remote access system for approved users.

(U) Without an updated policy, local system administrators cannot enforce the appropriate measures to implement controls for remote access, including unauthorized activities, which could adversely impact confidentiality, integrity, and availability of the Department’s data. Inadequate remote access controls increase the risk that accounts could be accessed and used by individuals to perform unauthorized activities.

(U) Recommendation 29. OIG recommends that the Bureau of Information Resource Management, Operations, Messaging Systems Office, E-Mail Operations Division, Mobile Computing, update the *Foreign Affairs Manual* (5 FAM 460 and 12 FAM 680) to replace the OpenNet Everywhere system with Global OpenNet, including the Mobile Computing Management System enrollment process, as the only remote access system for approved users.

⁷³ (U) 5 FAM 469.4d, *The Privacy Act and Personally Identifiable Information (PII)*, June 2013.

⁷⁴ (U) 12 FAM 682.2-1a.

⁷⁵ (U) ALDAC Telegram 2011 STATE 08891, *Global OpenNet Deployment*, Jan. 2011.

(U) Management Response: IRM concurred with this recommendation.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that 5 FAM 460 and 12 FAM 680 have been updated to replace the ONE system with GO, including the MCMS enrollment process, as the only remote access system for approved users.

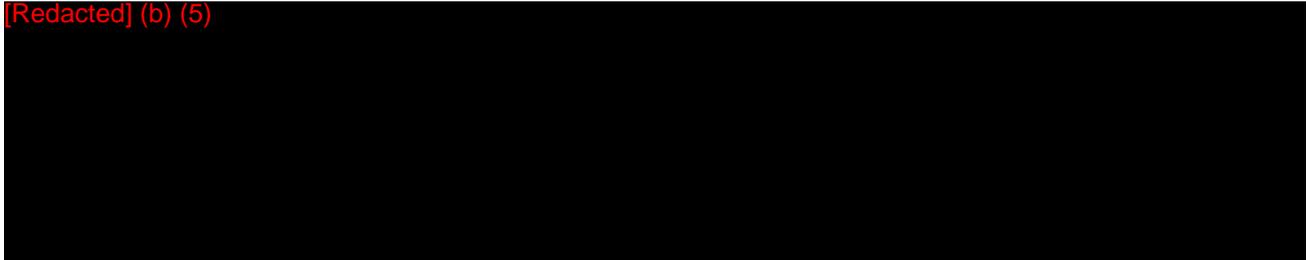
(U) Finding J. Compliance With FISMA Requirements

(U) In FY 2013, OIG found that the Department was in compliance with Incident Response and Security Capital Planning requirements. For incident response, there were no prior year weaknesses that carried over to FY 2013. In FY 2013, OIG noted the prior year Security Capital Planning finding (see Recommendation 31, Appendix B) had been remediated.

(U) List of Current Year Recommendations

(U) Recommendation 1. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, prioritize tasks to ensure that devoted resources identify, document, and finalize a risk management framework for Department of State information systems in accordance with National Institute of Standards and Technology Special Publication 800-30, Revision 1.

[Redacted] (b) (5)



(U) Recommendation 3. OIG recommends that Bureau of Information Resource Management ensure system owners perform security impact analyses for all systems and applications in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3, and reauthorize the systems accordingly.

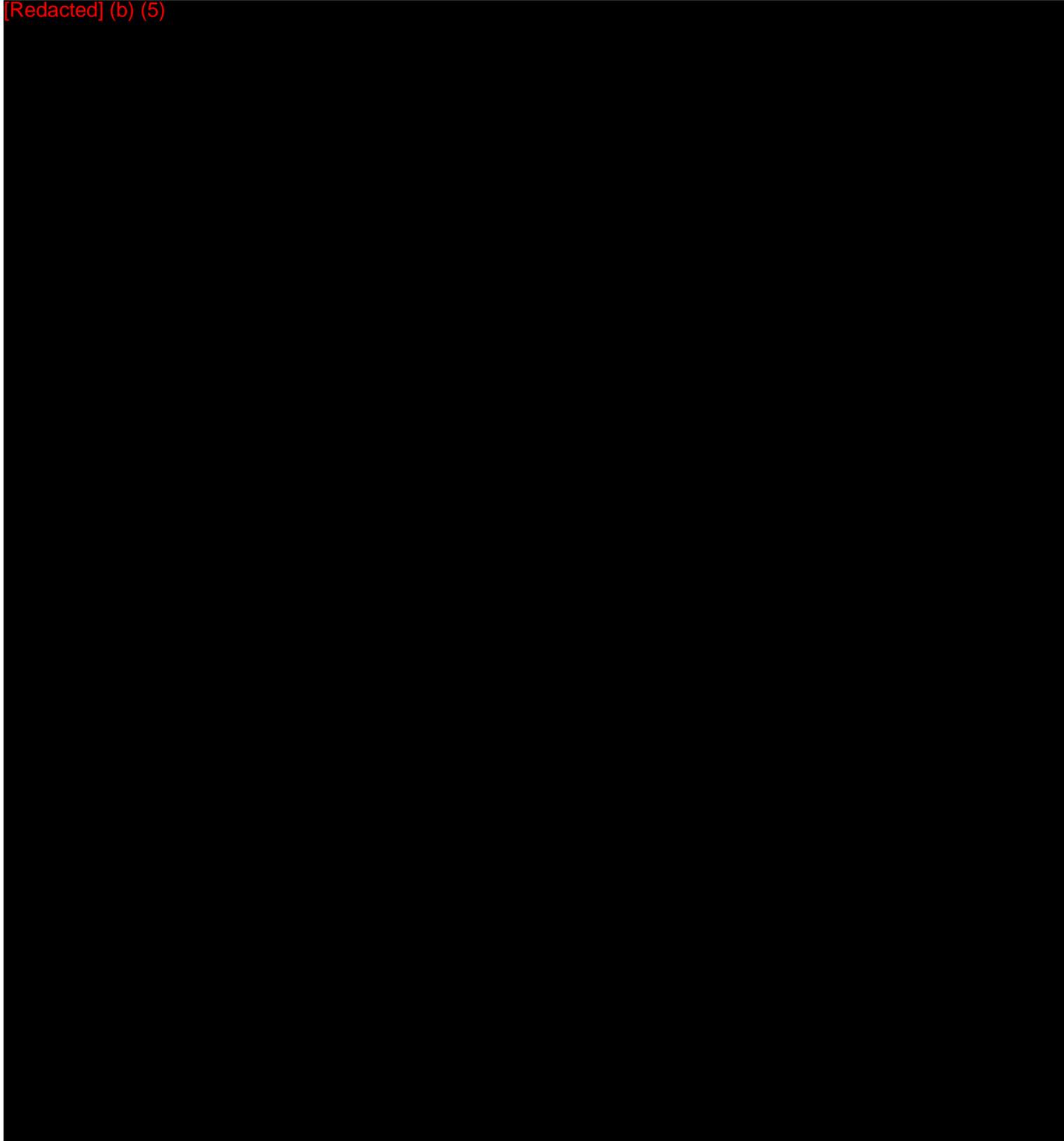
(U) Recommendation 4. OIG recommends that the Chief Information Officer exercise the authorities prescribed in the *Foreign Affairs Manual* (1 FAM 040) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plans of Action and Milestones (POA&M); ensure completion dates for corrective actions are adhered to and/or the remediation dates are updated as needed; implement processes and procedures to cross-reference POA&M information, including costs, to the capital planning budget process with a Unique Investment Identifier; and ensure that written responses for the *Quarterly Plan of Action & Milestones Grade* memorandums are provided to the Bureau of Information Resource Management, Office of Information Assurance.

(U) Recommendation 5. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, include the financial statement audit report findings, identified and communicated by the Bureau of Comptroller and Global Financial Services, within the Plan of Action and Milestone database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Recommendation 6. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify weaknesses resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, and include those weaknesses that are not immediately remediated in the Plan of Action and Milestone database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Recommendation 7. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, document an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems and is consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

[Redacted] (b) (5)

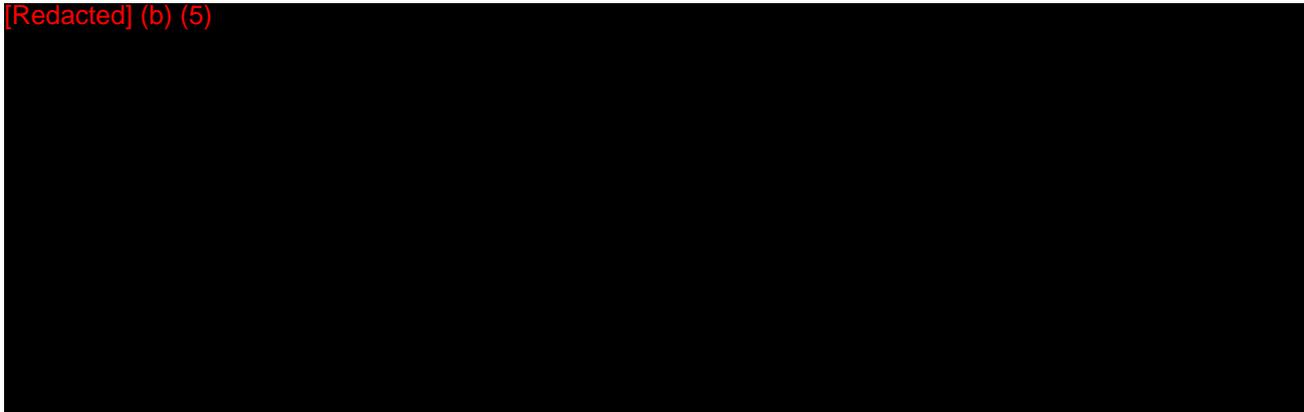


[Redacted] (b) (5)



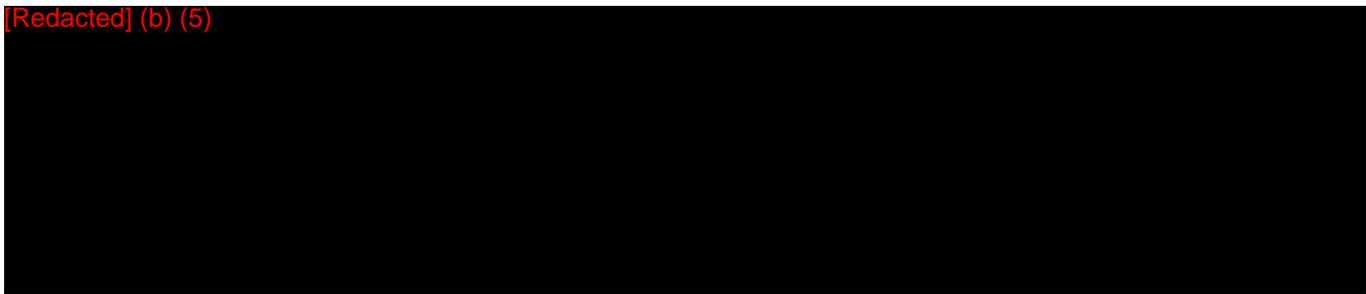
(U) Recommendation 14. OIG recommends system owners (bureaus and posts) follow the *Foreign Affairs Manual* (12 FAM 620) to have the supervisor complete the appropriate system access forms (for example, new user access and elevated rights) prior to granting access.

[Redacted] (b) (5)



(U) Recommendation 17. OIG recommends that management review their Active Directory Organizational Units structure and correct any Organizational Units that do not follow the guidance stated within the Active Directory and Global Address List Standardization.

[Redacted] (b) (5)



(U) Recommendation 19. OIG recommends that the system owners, in coordination with Chief Information Officer and the Bureau of Information Resource Management, Office of Information Assurance, perform and review contingency plan testing annually, including validating system backups and establishing an alternate site strategy in accordance with the *Foreign Affairs Manual* (5 FAM 1064), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Recommendation 20. OIG recommends that the Chief Information Officer, in coordination with the contingency planning coordinator, identify an alternate processing site, alternate storage site, and alternate telecommunications servers for each system in accordance with National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) Recommendation 21. OIG recommends that the Office of Emergency Management, in coordination with the Emergency Action Committee for each bureau, conduct its annual review and certify its Bureau Emergency Action Plans in accordance with the *Foreign Affairs Manual* (6 FAM 400).

(U) Recommendation 22. OIG recommends that data center managers enforce the log and record keeping policy to show that system backups are being performed in accordance with the *Foreign Affairs Manual* (12 FAM 620).

(U) Recommendation 23. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, consolidate and track all extensions (for example, contractor sites, other Government agencies, and third-party vendors) within iMatrix, in accordance with the *Foreign Affairs Manual* (5 FAM 600).

(U) Recommendation 24. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, ensure that annual physical inspections are completed for all OpenNet and ClassNet extensions as defined within each Memorandum of Understanding.

(U) Recommendation 25. OIG recommends that the Bureau of Diplomatic Security, in coordination with the applicable bureau Information System Security Officers for each contractor and government extension, ensure that all Memorandums of Understanding for extensions contain the required clearance levels for users and that those users are cleared as defined in the *Foreign Affairs Manual* (5 FAM 1065).

(U) Recommendation 26. OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Resource Management, suspend user accounts for unverified individuals at the International Boundary and Water Commission until the required background screenings are completed as required by the Memorandum of Understanding.

(U) Recommendation 27. OIG recommends the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities take specialized, role-based security training, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Recommendation 28. OIG recommends the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, implement a tracking mechanism for role-based training to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance

Training Plan in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Recommendation 29. OIG recommends that the Bureau of Information Resource Management, Operations, Messaging Systems Office, E-Mail Operations Division, Mobile Computing, update the *Foreign Affairs Manual* (5 FAM 460 and 12 FAM 680) to replace the OpenNet Everywhere system with Global OpenNet, including the Mobile Computing Management System enrollment process, as the only remote access system for approved users.

(U) Scope and Methodology

(U) In order to fulfill its responsibilities related to the Federal Information Security Management Act of 2002 (FISMA),¹ the Office of Inspector General (OIG), Office of Audits, contracted with Williams, Adley & Company-DC, LLP (referred to as “we” in this appendix), an independent public accountant, to evaluate the Department of State’s (Department) information security program and practices to determine the effectiveness of such programs and practices for FY 2013.

(U) According to FISMA, each Federal agency should develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS).² DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

(U) We conducted the audit from April through September 2013. In addition, we performed the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), FISMA, OMB, and National Institute of Standards and Technology (NIST) guidance. GAGAS requires that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) We used the following laws, regulations, and policies to evaluate the adequacy of the controls in place at the Department:

- (U) DHS Inspector General FISMA Reporting Metrics.³
- (U) OMB Memorandums M-02-01, M-04-04, M-06-19, and M-12-20.⁴
- (U) DHS Federal Information Security Memorandum 12-02.⁵

¹ (U) Pub. L. No. 107-347, tit. III.

² (U) OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security (DHS)* July 6, 2010.

³ (U) Department of Homeland Security’s *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated Nov. 30, 2012.

⁴ (U) OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, Oct. 17, 2001; OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, Dec. 16, 2003; OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006; and OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept. 27, 2012.

- (U) Department policies and procedures such as the *Foreign Affairs Manual* (FAM), 5 FAM and 12 FAM.⁶
- (U) Federal laws, regulations, and standards such as FISMA, OMB Circular A-130, Appendix III,⁷ and OMB Circular No. A-11.⁸
- (U) NIST Special Publications (SP), Federal Information Processing Standards (FIPS), other applicable NIST publications, and industry best practices.

(U) During our audit, we assessed the Department's information security program policies, procedures, and processes in the following areas:

- (U) Continuous monitoring
- (U) Security configuration management
- (U) Account and identity management
- (U) Incident response and reporting
- (U) Risk management framework (formerly Certification & Accreditation)
- (U) Security training
- (U) Plan of action and milestones (POA&M)
- (U) Remote access
- (U) Contingency planning
- (U) Oversight of contractor systems
- (U) Security capital planning

(U) The audit covered the period of October 1, 2012, to September 30, 2013. During the fieldwork, we took the following actions:

- (U) Determined the extent to which the Department's information security plans, programs, and practices complied with FISMA requirements; applicable Federal laws, regulations, and standards; relevant OMB Circular No. A-130, revised processes and reporting requirements included in Appendix III; and NIST and FIPS requirements.
- (U) Reviewed relevant security programs and practices to report on the effectiveness of the Department's agency-wide information security program in accordance with OMB's annual FISMA reporting instructions. The audit approach addressed the DHS *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated November 30, 2012.

⁵ (U) DHS Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Feb. 15, 2012.

⁶ (U) 5 FAM, *Information Management*, and 12 FAM, *Diplomatic Security*.

⁷ (U) OMB Circular No. A-130, Revised, *Management of Federal Information Resources*, app. III, Security of Federal Automated Information Resources, Nov. 30, 2000.

⁸ (U) OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, Aug. 2011.

- (U) Assessed programs for monitoring security policy and program compliance and responding to security events (that is, unauthorized changes detected by intrusion detection systems).
- (U) Assessed the adequacy of internal controls related to the areas reviewed. Control deficiencies identified during the review are included in the report.
- (U) Evaluated the Department's remedial actions taken to address the previously reported information security program control weaknesses identified in OIG's report *Audit of Department of State Information Security Program* (AUD-IT-13-03, Nov. 2012).

(U) Review of Internal Controls

(U) We reviewed the Department's internal controls to determine whether:

- (U) The Department had established an enterprise-wide continuous monitoring program that assessed the security state of information systems that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Department had established and maintained a security configuration management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Department had established and maintained an account and identity management program that was generally consistent with NIST's and OMB's FISMA requirements and identified users and network devices.
- (U) The Department had established and maintained an incident response and reporting program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Department had established a risk management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Department had established and maintained a security training program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Department had established a POA&M program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that tracked and monitored known information security weaknesses.
- (U) The Department had established and maintained a remote access program that was generally consistent with NIST's and OMB's FISMA requirements.
- (U) The Department had established and maintained an entity-wide business continuity/disaster recovery program that was generally consistent with NIST's and OMB's FISMA requirements.
- (U) The Department had established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization.

- (U) The Department had established and maintained a capital planning and investment program for information security.

(U) Use of Computer-Processed Data

(U) During the audit, we utilized computer-processed data to obtain samples and information regarding the existence of information security controls. Specifically, we obtained data extracted from Microsoft's Windows Active Directory and the Department's human resources system to test user account management controls. We assessed the reliability of computer-generated data primarily by comparing selected data with source documents. We determined that the information was reliable for assessing the adequacy of related information security controls.

(U) Generally, for a population of sample items, we used random sampling to test 10 percent of the population or 25, whichever was less. The 10 percent guidance was based on 10 percent of a population of 250, which equals 25.

(U) Followup of Recommendations From the FY 2012 FISMA Report

(U) We reviewed actions implemented by management to mitigate the findings identified in the FY 2012 FISMA report. The current status of each of the recommendations is as follows:

(U) Recommendation 1. We recommend that the Information Security Steering Committee finalize and implement an enterprise-wide continuous monitoring and risk management framework strategy that addresses framing risk, assessing risk, responding to risk, and monitoring risk.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 1 (Finding A) in the FY 2013 report.

(U) Recommendation 2. We recommend the Chief Information Officer, in coordination with the Bureau of Diplomatic Security and the Bureau of Information Resource Management, include, under its continuous monitoring program, an effective method to monitor the security posture for non-Windows operating systems, databases, firewalls, routers, and switches.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 7 (Finding C) in the FY 2013 report.

(U) Recommendation 3. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Enterprise Network Management, and the Bureau of Diplomatic Security, finalize and implement the Cyber Security Architecture draft target architecture and initiative for end-to-end configuration management.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.

(U) Recommendation 4. We recommend that the Chief Information Officer, in coordination with the Bureau of Consular Affairs, the Bureau of Administration, the Bureau of Resource Management, the Office of Medical Services, the Bureau of Overseas Buildings Operations, the Bureau of International Narcotics and Law Enforcement Affairs, the Foreign Service Institute, the Bureau of Diplomatic Security, the Bureau of International Information Program, and the Bureau of Information Resource Management, continue to improve their processes to patch servers within their system boundary in a timely manner.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.

(U) Recommendation 5. We recommend that the Security Configuration Management Branch develop and publish the security configuration baselines for UNIX in accordance with the Foreign Affairs Manual.

(U) *Status: Closed July 2013.* The Security Configuration Management Branch has established and published UNIX standard baselines.

(U) Recommendation 6. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security/Security Infrastructure/Office of Computer Security, research, develop, and implement capabilities (for example, scanning tools) to perform periodic network vulnerability and compliance scans on Oracle databases, applications, network devices (for example, routers and switches), UNIX operating systems, and Demilitarized Zone servers.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.*

(U) Recommendation 7. We recommend that the Chief Information Officer, in coordination with Diplomatic Security/Security Infrastructure/Office of Computer Security, update the Foundstone configuration to include subnets and Demilitarized Zone servers that were not included in the Foundstone configuration for periodic scanning and obtain the administrative credentials needed to perform the scans and periodically perform discovery scanning to identify new components added to the network.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.*

(U) Recommendation 8. We recommend that the Chief Information Officer, in coordination with respective System Administrators from all bureaus, take immediate action to remove or lock accounts that do not require a password.

(U) *Status: Closed June 2013.* We noted the Department had shown significant improvement in this area from the prior year. Utilizing a risk-based approach, we did not find the level of risk associated with the exception noted for accounts that were not set to require a password and/or set to “not expire” passwords to rise to the level of being identified as a finding. From our testing of 122,155 active accounts, we found only one account that was set to not require a password.

(U) Recommendation 9. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, revise the *Foreign Affairs Manual* to provide authority to the Chief Information Officer to review and identify accounts not used within the past 90 days and to de-activate such accounts and require the bureaus and posts to recertify the user account prior to re-activating the account.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.*

(U) Recommendation 10. We recommend that the Chief Information Officer, in coordination with bureau and post Data Center Managers and System Managers, require the posts and bureaus to configure all accounts to expire passwords in accordance with the *Foreign Affairs Manual* (that is, passwords must be changed every 60 days).

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 17 (Finding E) in the FY 2013 report.*

(U) **Recommendation 11.** We recommend that the Chief Information Officer, in coordination with Bureau of Diplomatic Security, determine whether unauthorized access was performed using the terminated employees' credentials and whether Department information had been compromised.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.*

(U) **Recommendation 12.** We recommend that the Chief Information Officer, in coordination with Information System Security Officers and system administrators of the Bureau of East Asian and Pacific Affairs, the Bureau of Near Eastern Affairs, the Washington District of Columbia, and the Bureau of Western Hemisphere Affairs, improve the process of disabling terminated employees user accounts in a timely manner.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. A further root cause was identified during our FY 2013 review, and this finding has been split between Recommendations [Redacted] (b) (5) (Finding E) in the FY 2013 report.*

(U) **Recommendation 13.** We recommend that the Chief Information Officer, in coordination with the Orientation and In-Processing Center, enforce the use of the Department of State Logon Request form for new users in Afghanistan.

(U) *Status: Closed June 2013.* Based upon testing performed, we noted that the Information Technology Mart Standard Operating Procedures include updated account management procedures to enforce the use of the Department of State Logon Request forms.

(U) **Recommendation 14.** We recommend that the Chief Information Officer, in coordination with Information Resource Management/Operations Directorate/Computer Security Office/Desktop Support Division, update the Information Technology Mart Standard Operating Procedures to reflect the updated account management procedures for new users in Afghanistan.

(U) *Status: Closed June 2013.* We noted that the Information Technology Mart Standard Operating Procedures include updated account management procedures for new users.

(U) **Recommendation 15.** We recommend that the Chief Information Officer, in coordination with Office of the Secretary, develop and finalize exemptions/waivers to allow for the deviation from the standard of setting expiration dates for Office of the Secretary user accounts in Active Directory.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become [Redacted] (b) (5) in the FY 2013 report.*

(U) Recommendation 16. We recommend that the Chief Information Officer, in coordination with Office of the Secretary, develop and implement a process that ensures that Office of the Secretary users complete the required Cyber Security Awareness Training on an annual basis.

(U) Status: Closed July 2013. Based upon inspection of a sampled selection of completed security awareness PS800 training, we determined that all sampled new users had completed the security awareness PS800 training.

(U) Recommendation 17. We recommend that the Chief Information Office, in coordination with Information Resource Management/Information Assurance, continue to review the security authorization and annual assessments to ensure that Information System Owner, Information System Security Officer, and Security Control Assessor for all Federal Information Security Management Act reportable systems use the published Certification & Accreditation Toolkit templates during the annual controls assessment to assess the required National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* controls applicable and update the System Security Plan accordingly.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 3 (Finding A) in the FY 2013 report.

(U) Recommendation 18. We recommend that the Chief Information Officer continue to track the progress of the full authorization of the OpenNet general support system.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 2 (Finding A) in the FY 2013 report.

(U) Recommendation 19. We recommend that the Chief Information Officer, in coordination with Information Resource Management/Information Assurance and Office of Computer Security, update the Information Assurance Training Plan to require newly hired and current employees and contractors who are in positions that are responsible for the security of the organization's information and information systems complete role-based security-related training before authorizing access to the system or performing assigned duties and periodically thereafter (for example, annually).

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 27 (Finding H) in the FY 2013 report. However, we noted that the Information Assurance Training Plan has been updated pending formal approval.

(U) Recommendation 20. We recommend that the Chief Information Officer, in coordination with Information Resource Management/Information Assurance and all bureaus, develop and implement monitoring processes and procedures to ensure that personnel with significant security responsibilities receive the appropriate training in accordance with the Information Assurance Training Plan.

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 28 (Finding H) in the FY 2013 report.*

(U) Recommendation 21. We recommend that the Chief Information Officer, in coordination with the Bureau of Consular Affairs, the Bureau of Information Resource Management, the Bureau of Human Resources, the Office of Medical Services, the Bureau of Arms Control, Verification and Compliance, the Office of the Secretary, and the Bureau of Overseas Buildings Operations Bureau Executive Director or Information System Owner, their equivalent, or a designee, ensure that responses are provided for the Quarterly Plan of Action & Milestones Grade Memorandums to address how the bureaus and offices plan to close out the outstanding plan of action and milestones, that the plan of action and milestones completion dates for corrective actions that expired are updated and the resources required for remediation are updated, that remediation actions undertaken for plan of action and milestones are verified in a timely manner, and that required fields within the plan of action and milestones are included (for example, resources).

(U) *Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 4 (Finding B) in the FY 2013 report.*

(U) Recommendation 22. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, update the *Foreign Affairs Manual*, 12 FAM 680, to reflect the current process of granting administrators the capabilities for remote administration (for example, allowing exception waivers for remote access administration).

(U) *Status: Closed July 2013.* The current 12 FAM 680 shows that system administrators are allowed remote access but only from Department-approved systems.

(U) Recommendation 23. We recommend that the Chief Information Officer, in coordination with all bureaus and respective Executive Directors, improve their process for submitting service requests to the Information Technology Service Center for key fobs/tokens for new employees.

(U) *Status: Closed July 2013.* Upon review of lost or stolen devices, we determined that there is little to no risk for not submitting a service request, as the devices are still deactivated.

(U) Recommendation 24. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, update the *Foreign Affairs Manual* to provide guidance and direction for Continuity of Operations Plan development and implementation.

(U) *Status: Closed August 2013.* Upon review, we noted that the *Foreign Affairs Manual* had been updated to provide guidance and direction for Continuity of Operations Plan development and implementation.

(U) Recommendation 25. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, perform an entity-wide Business Impact Analysis and develop a strategy to prioritize recovery of the critical assets within the Department and align the Business Impact Analysis of the primary mission-

critical functions with Information Resource Management's Maximum Tolerable Downtime for the network.

(U) Status: *Closed August 2013.* Upon inspection of the Information Resource Management's Bureau Emergency Action Plan, we noted the entity-wide Business Impact Analysis of the primary mission critical functions aligned with Information Resource Management's Maximum Tolerable Downtime for the network.

(U) Recommendation 26. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, develop a Continuity of Operations Plan for communications and the infrastructure at the Department level (entity) that complies with National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, and includes the standard elements of a Continuity of Operations Plan.

(U) Status: *Closed August 2013.* The Bureau of Information Resource Management had developed a Bureau Emergency Action Plan that incorporates the standard elements of a continuity of operation plan.

(U) Recommendation 27. We recommend that the Chief Information Officer, in coordination with bureaus and the Information System Owners, document and maintain alternate site locations and procedures for accessing the alternate site and perform annual contingency plan tests and update contingency plans with test results as necessary.

(U) Status: *Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 20 (Finding F) in the FY 2013 report.*

(U) Recommendation 28. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, continue to ensure that annual physical inspections are completed for all OpenNet and ClassNet extensions.

(U) Status: *Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 24 (Finding G) in the FY 2013 report.*

(U) Recommendation 29. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, continue to review System Security Assessment packages, annual controls assessments, and contingency plans tests to ensure that bureaus are implementing the required National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* controls and updating System Security Plans for the contractor-hosted systems.

(U) Status: *Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 3 (Finding A) in the FY 2013 report.*

(U) Recommendation 30. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, continue to implement procedures to coordinate security activities for tracking all extensions (that is, contractor sites and other government agencies via iPost) to OpenNet and ClassNet.

(U) Status: Closed. This is a repeat recommendation from the FY 2012 report. It has become Recommendation 23 (Finding G) in the FY 2013 report.

(U) Recommendation 31. We recommend that the Bureau of Information Resource Management senior management ensure that Information Technology Service Line Program Managers obtain the appropriate level of electronic Capital Planning Investment control tool training and understanding regarding their electronic Capital Planning Investment Control reporting requirements and that they are held accountable for completing their respective Exhibits 300, including the accurate reporting of the resources required to protect their information systems, as part of the next electronic Capital Planning Investment Control submission.

(U) Status: Closed May 2013. Bureau of Information Resource Management/Business Management and Planning Project Managers have completed the Program Planning Manager training, obtained certification, and tracked Planning Project Managers training all year round. Furthermore, the audit team reviewed the CPIC process flow and determined the process details the pre-select, select, control, and evaluation procedures for completing Exhibit 300s.

(U) End-to-End Configuration Management Process Needs Improvement

(U) Although the Department was taking actions to address the prior year noted weaknesses with the configuration management controls, the weaknesses within configuration management process still existed. [Redacted] (b) (5)

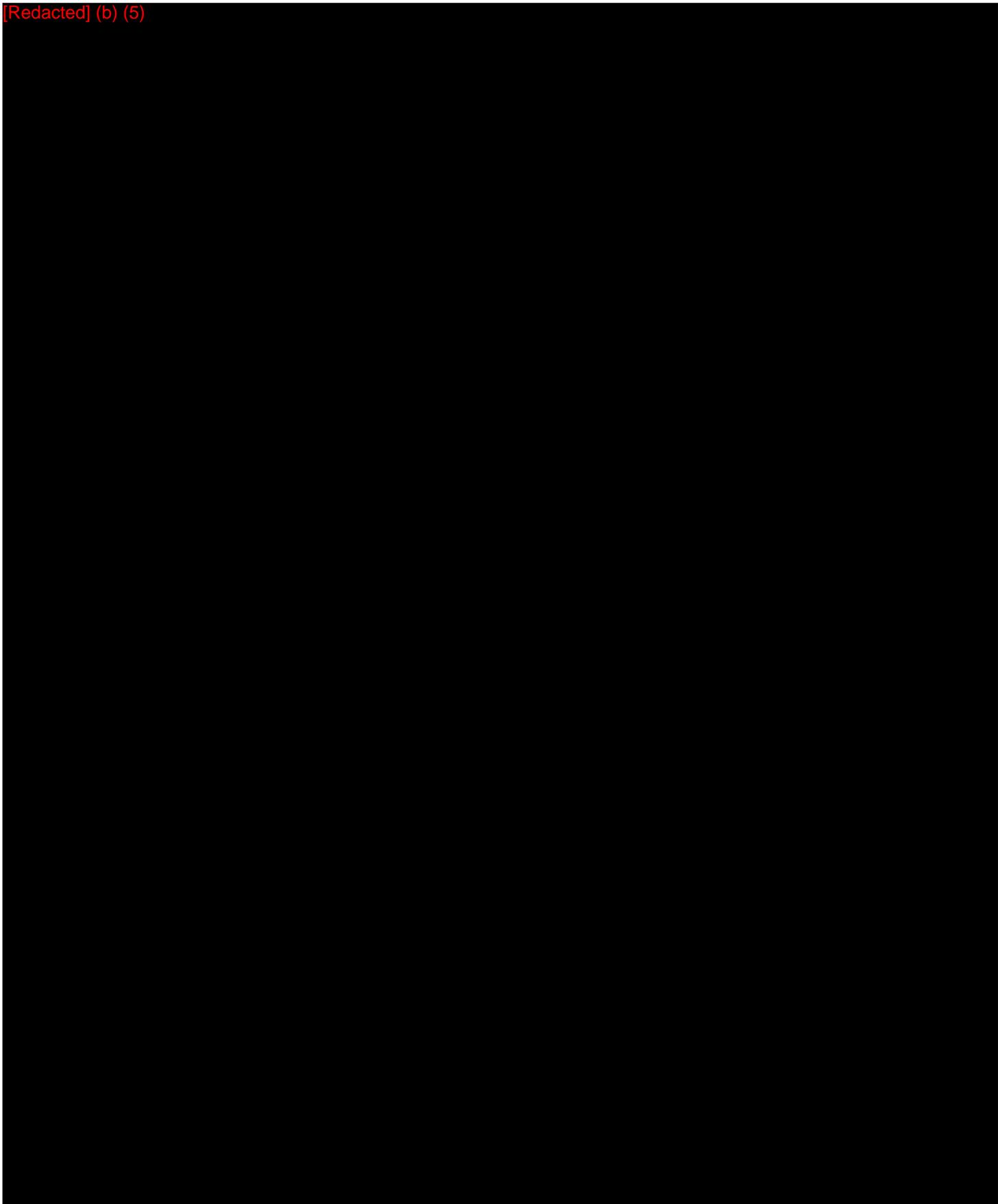
[Redacted]

[Redacted] (b) (5)

[Redacted]

(U) The Bureau of Diplomatic Security did not provide the vulnerability scan results for the following five information systems under scope for OIG FISMA Audit 2013: PRAS, GTS, GINL, EXTRANET, and SMSe.

[Redacted] (b) (5)



(U) Department of State Response



United States Department of State

Washington, D.C. 20520

~~SENSITIVE BUT UNCLASSIFIED~~

MEMORANDUM

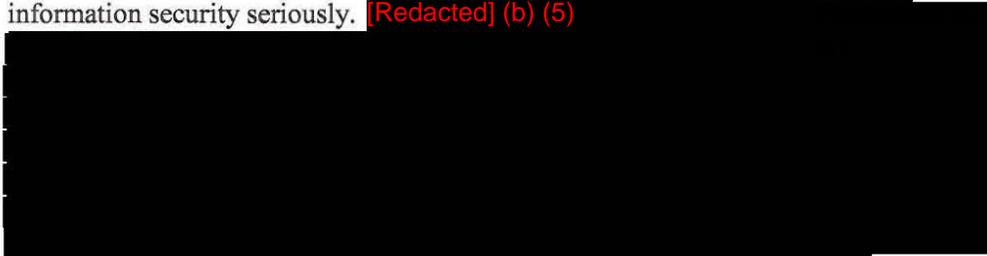
October 22, 2013

To: OIG/AUD – Norman P. Brown, Acting

From: IRM – Steven C. Taylor *ST*

Subject: Draft Report on Audit of Department of State Information Security Program

(SBU) We want to thank the OIG for the opportunity to review and comment on the subject draft report. We agree that the areas of focus are important and given their broad scope it is not surprising that these findings were identified though many differ in substance from what was identified in previous years. Over the past four years, we have made much progress addressing the various recommendations. We do not agree with the assertion that the findings constitute a significant deficiency. Our actions demonstrate that we take information security seriously. [Redacted] (b) (5)



(U) We have included as requested an initial response to each of the recommendations contained in the FY 2013 report. We will provide greater detail in our response to the final released report. We would also like to enlist your assistance in the area of POA&M oversight in connecting remediation requirements to funding. We would be interested in OIG suggested approaches that will assure adequate planning and direction of funds within the bureaus to carry out needed mitigation actions.

Attachments:

Tab 1 - Response to Recommendations of the OIG Audit on Information Security

Tab 2 - DS/IS/IND Proposed Response to OIG Finding G of OIG Draft

Response to Recommendations of the OIG Audit on Information Security

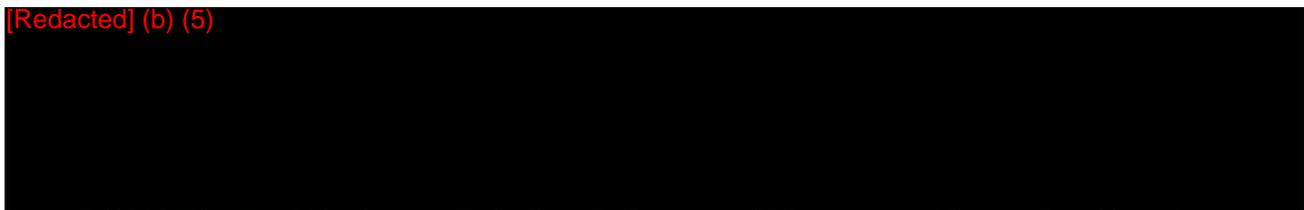
Tab 1

Response to Recommendations of the OIG Audit on Information Security

(U) Recommendation 1. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, prioritize tasks to ensure devoted resources identify, document, and finalize a risk management framework for the Department's information systems in accordance with National Institute of Standards and Technology Special Publication 800-30, Revision 1.

(U) IRM Response to Draft Recommendation 1: IRM concurs with this recommendation.

[Redacted] (b) (5)



(U) IRM Response to Draft Recommendation 2: IRM concurs with this recommendation and notes this work is in process.

(U) Recommendation 3. OIG recommends that Bureau of Information Resource Management ensure system owners perform security impact analyses for all systems and applications in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3, and reauthorize the systems accordingly.

(U) IRM Response to Draft Recommendation 3: IRM does not concur with this recommendation as this is part of the IA Toolkit for A&A.

(U) Recommendation 4. OIG recommends that the Chief Information Officer exercise the authorities prescribed in the Foreign Affairs Manual (1 FAM 040) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plan of Action and Milestones (POA&M); ensure completion dates for corrective actions are adhered to and/or the remediation dates are updated as needed; implement processes and procedures to cross-reference POA&M information, including costs, to the capital planning budget process with a Unique Investment Identifier; and ensure that written responses for the *Quarterly Plan of Action & Milestones Grade* memorandums are provided to the Bureau of Information Resource Management, Office of Information Assurance.

(U) IRM Response to Draft Recommendation 4: IRM does not concur in totality with this recommendation. The Department has made and continues to make progress with tracking of POA&Ms. However, we welcome OIG recommendations on how to do this more effectively.

~~SENSITIVE BUT UNCLASSIFIED~~

Response to Recommendations of the OIG Audit on Information Security

(U) Recommendation 5. OIG recommends that the Bureau of the Comptroller and Global Financial Services communicate the financial statement audit report findings to the Bureau of Information Resource Management, Office of Information Assurance in accordance with Office of Management and Budget Memorandum M-11-33.

(U) IRM Response to Draft Recommendation 5: This recommendation is referred to the Bureau of the Comptroller and Global Financial Services. However, we will acknowledge that IRM/IA is in receipt of both the report sought during the FISMA review, and the most recent audit report findings. CGFS annually posts the Agency Financial Report to the Department's web site enabling bureaus and all employees access to this information

(U) Recommendation 6. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify weaknesses resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, and include those weaknesses that are not immediately remediated in the Plan of Action and Milestone database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) IRM Response to Draft Recommendation 6: IRM concurs with this recommendation.

(U) Recommendation 7. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, document an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems and is consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) IRM Response to Draft Recommendation 7: IRM provided documentation in 2012.

[Redacted] (b) (5)



(U) IRM Response to Draft Recommendation 8: IRM concurs with this recommendation.

[Redacted] (b) (5)



(U) IRM Response to Draft Recommendation 9: IRM concurs with this recommendation.

~~SENSITIVE BUT UNCLASSIFIED~~

Response to Recommendations of the OIG Audit on Information Security

[Redacted] (b) (5)

(U) **IRM Response to Draft Recommendation 10:** IRM and DS concur with the recommendation.

[Redacted] (b) (5)

(U) **IRM Response to Draft Recommendation 11:** IRM and DS concur with this recommendation.

[Redacted] (b) (5)

(U) **IRM Response to Draft Recommendation 12:** IRM and DS concur and have been working toward this recommendation for several years. However we do not believe that these devices represent the highest risk to the Department.

[Redacted] (b) (5)

(U) **IRM Response to Draft Recommendation 13:** IRM and DS concur with the recommendation and add that in order to fully resolve this Recommendation, IRM will look for an effective means for identifying new subnets to facilitate notifying DS.

(U) **Recommendation 14.** OIG recommends system owners (bureaus and posts) follow the Foreign Affairs Manual (12 FAM 620) to have the supervisor complete the appropriate system access forms (for example, new user access and elevated rights) prior to granting access.

~~SENSITIVE BUT UNCLASSIFIED~~

Response to Recommendations of the OIG Audit on Information Security

(U) IRM Response to Draft Recommendation 14: IRM and DS believe this is a prudent action and look to the OIG to audit these during their audit of bureaus and posts.

[Redacted] (b) (5)

(U) IRM Response to Draft Recommendation 15: IRM concurs with this recommendation.

[Redacted] (b) (5)

[Redacted] (b) (5) DS requests OIG review the intent of this recommendation and redirect action to the appropriate organization. This recommendation is outside the scope of the DS Monitoring and Incident Response Program. Rather, ISSOs are responsible for maintaining a current list of authorized users at their respective Department sites. More specifically, as per 12 FAM 632.1-11, ISSOs are responsible for generating and reviewing audit logs at least once a month.

(U) Recommendation 17. OIG recommends management review their Active Directory Organizational Units structure and correct any Organizational Units that do not follow the guidance stated within the Active Directory and Global Address List Standardization.

(U) IRM Response to Draft Recommendation 17: IRM does not concur with this recommendation and believe it is impractical in the Department's environment and also suggest with the appropriate implementation of recommendations 14 and 15 the risk can be adequately managed.

[Redacted] (b) (5)

(U) DS Response to Draft Recommendation 18: DS deems this recommendation resolved. The 12 FAM 600 revisions governing the framework for the creation, activation and retirement of unclassified user accounts have been drafted and are undergoing Department review and clearance.

(U) Recommendation 19. OIG recommends that the Chief Information Officer, in coordination with system owners and Bureau of Information Resource Management, Office of Information Assurance, perform and review contingency plan testing annually, including validating system backups and establishing an alternate site strategy in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

~~SENSITIVE BUT UNCLASSIFIED~~

Response to Recommendations of the OIG Audit on Information Security

(U) IRM Response to Draft Recommendation 19: IRM does not agree with this recommendation and believes this responsibility should be with the System Owner with a report back to IRM/IA.

(U) Recommendation 20. OIG recommends that the Chief Information Officer, in coordination with the contingency planning coordinator, identify an alternate processing site, alternate storage site, and alternate telecommunications servers for each system in accordance with National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) IRM Response to Draft Recommendation 20: IRM does not agree with this overly broad recommendation. IRM has worked with A/OEM as appropriate and System Owners in their design to meet continuity requirements

(U) Recommendation 21. OIG recommends that the Office of Emergency Management, in coordination with the Emergency Action Committee for each Bureau, conduct annual review and certify their Bureau Emergency Action Plans in accordance with the Foreign Affairs Manual (6 FAM 400).

(U) A/OEM Response to Draft Recommendation 21: A/OEM has not provided a response. IRM will work with this office to prepare for response to the final report.

(U) Recommendation 22. OIG recommends that data center managers enforce the audit trail/log policy in accordance with the Foreign Affairs Manual (12 FAM 620).

(U) IRM Response to Draft Recommendation 22: IRM's data center managers provide different levels of service for different systems, from hosting to completely managed service. For those systems IRM provides a managed service, IRM concurs with this recommendation and believes it is being accomplished.

(U) Recommendation 23. OIG recommends that the Chief Information Officer in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security consolidate and track all extensions (for example, contractor sites, other government agencies, and third party vendors) within iMatrix, in accordance with the Foreign Affairs Manual (5 FAM 600).

(U) IRM and DS Response to Draft Recommendation 23: All extensions have been entered into iMatrix and DS reviews all extensions annually.

(U) Recommendation 24. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, ensure that annual physical inspections are completed for all Government OpenNet and ClassNet extensions as defined within each Memorandum of Understanding.

~~SENSITIVE BUT UNCLASSIFIED~~

Response to Recommendations of the OIG Audit on Information Security

(U) IRM and DS Response to Draft Recommendation 24: The annual physical inspections for OpenNet and ClassNet have either been completed, or are scheduled and currently in process. Documentation confirming the status of physical inspections was previously provided to the OIG.

(U) Recommendation 25. OIG recommends that the Bureau of Diplomatic Security, in coordination with the applicable bureau Information System Security Officers for each Government extension, ensure that all Memorandums of Understanding for extensions contain the required clearance levels for users, and those users are cleared as defined in the Foreign Affairs Manual (5 FAM 1065).

(U) DS Response to Draft Recommendation 25: DS concurs with this recommendation and a process is already in place. ISSOs are responsible for identifying all users that require access to OpenNet, the DS Office of Personnel Security and Suitability (DS/SI/PSS) ensures that all Memoranda of Understanding for extensions contain the required clearance levels for users, and that those users have the appropriate clearance.

(U) Recommendation 26. OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of the Comptroller and Global Financial Services, suspend user accounts for unverified individuals at the International Boundary and Water Commission until the required background screenings are completed as required by the Memorandum of Understanding.

(U) IRM Response to Draft Recommendation 26: CGFS does not concur with this recommendation. IBWC is actively and aggressively pursuing adjudication for users of the Global Financial Management System at the IBWC. As of October 17, 17 of the 22 users have been adjudicated. The remaining 5 users are expected to be adjudicated in the very near future.

(U) Recommendation 27. OIG recommends the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities take specialized, role-based security training as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) IRM Response to Draft Recommendation 27: IRM concurs with the recommendation. The plan has been finalized and is in the clearance/review process.

(U) Recommendation 28. OIG recommends the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, implement a tracking mechanism for role-based training to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) IRM Response to Draft Recommendation 28: IRM concurs with the recommendation.

~~**SENSITIVE BUT UNCLASSIFIED**~~

Response to Recommendations of the OIG Audit on Information Security

(U) Recommendation 29. OIG recommends that the Bureau of Information Resource Management, Operations, Messaging Systems Office, E-Mail Operations Division, Mobile Computing, update the Foreign Affairs Manual (5 FAM 460 and 12 FAM 680) to replace the OpenNet Everywhere system with Global OpenNet, including the Mobile Computing Management System enrollment process, as the only remote access system for approved users.

(U) IRM Response to Draft Recommendation 29: IRM concurs with this recommendation.

~~**SENSITIVE BUT UNCLASSIFIED**~~

Tab 2

DS/IS/IND Proposed Response to OIG Finding G of OIG Draft FISMA Report

(U) Finding G. Contractor Systems

(U) OIG first identified deficiencies in contractor and Government extensions' systems oversight in FY 2010, and many of these same deficiencies remained in FY 2013. 5 FAM 600⁶⁰ states, "All systems (including applicable contractor systems) and applications associated with any projects must be registered in Information Technology Applications Baseline (ITAB)." ITAB is the former name of the iMatrix application.

(U) The Department had not followed policies and procedures on managing its contractor and government extensions. Specifically,

- (U) IRM and DS maintained separate contractor extension inventory lists, which resulted in discrepancies.
- (U) Some contractor extensions were not documented within iMatrix, which is the Department's official system of record for extensions.
- (U) As of September 20, 2013, the annual data call memo⁶¹ to all posts, instructing them to verify existing IT assets and add any new assets hosted by post within iMatrix, was not completed for FY2013.

[Redacted] (b) (5)

- (U) DS/IS/CS did not complete the annual re-certification for two of the three sampled government extensions.
- (U) Of three sampled government extensions, two (67 percent) extensions did not specify the clearance requirements within their respective Memorandum of Understanding as required by 5 FAM 1065.⁶²
- (U) For one government extension, 36 (77 percent) of 47 OpenNet users did not comply with the clearance requirements within the Memorandum of Understanding.

(U) 5 FAM 600⁶³ states, "All systems (including applicable contractor systems) and applications associated with any projects must be registered in Information Technology Applications Baseline."

(U) 5 FAM 1065⁶⁴ states, "Connectivity requests must include:"

[Redacted] (b) (5)

(U)...For commercial contractors and consultants with contractual relations with the Department, Form DD-254, Contract Security Classification Specification, or other document containing contract security requirements language specifying all information contained in a connectivity MOA/MOU and ISA.

(U) There was no single resource that managed oversight of contractor and government extensions within the Department, which caused a lack of communication between IRM, accountable bureaus, and DS. DS maintained their own list of contractor extensions, which was the basis of its yearly reviews. However, by policy, IRM should have the official listing of extensions within iMatrix. Prior to FY 2013, there was no dedicated resource within IRM to work between the two groups. As a result, not all updates were uploaded into iMatrix. In addition, IRM only tracked extensions at contractor sites and third party vendors. They did not consider government agencies (government extensions) as contractors and therefore did not keep track of them as required by 5 FAM 600.

(U) DS, in coordination with the Bureau of Resource Management, did not verify completion of required International Boundary and Water Commission background screenings prior to granting its employees access to OpenNet.

(U) By not following Department policies for contractor and government extensions, the Department has minimal assurance that the contractors' information security controls are compliant with FISMA, OMB requirements, and NIST standards. In addition, there are increased risks to Department data that is collected, processed, and maintained by contractor systems, which may be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction. The lack of information security requirements in contracts may cause contractor systems to possess lower security requirements, and thus make them untrusted systems. Without adequate oversight of contractor and government extensions, the Department increases the risk of their overall security posture and is exposed to an increased threat of unauthorized access, use, disclosure, disruption, modification and destruction of data.

[Redacted] (b) (5)



**FRAUD, WASTE, ABUSE,
OR MISMANAGEMENT
OF FEDERAL PROGRAMS
HURTS EVERYONE.**

CONTACT THE
OFFICE OF INSPECTOR GENERAL
HOTLINE
TO REPORT ILLEGAL
OR WASTEFUL ACTIVITIES:

202-647-3320
800-409-9926
oighotline@state.gov
oig.state.gov

Office of Inspector General
U.S. Department of State
P.O. Box 9778
Arlington, VA 22219