



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

AUD-IT-15-17

Office of Audits

October 2014

Audit of the 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 of 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.



(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 Broadcasting Board of Governors Information Security Program for FY 2014. 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 Broadcasting Board of Governors, 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, continuous monitoring, contingency planning, incident response and reporting, plans of actions and milestones, remote access management, configuration management, identity and access management, and security training and awareness.

(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 "N. P. Brown".

(U) Norman P. Brown
(U) Assistant Inspector General
for Audits



Audit of the Department of State Information Security Program

October 22, 2014

Office of Inspector General
U.S. Department of State and the Broadcasting Board of Governors
Washington, DC

Williams, Adley & Company-DC, LLP has performed an audit of the Department of State's (Department) Information Security Program. We audited the Department'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 and the Broadcasting Board of Governors Office of Inspector General.

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

Williams, Adley & Company-DC, LLP

SENSITIVE BUT UNCLASSIFIED

(U) Acronyms

(U) AD	Active Directory
(U) ATO	Authority to Operate
(U) CIO	Chief Information Officer
(U) CIRT	Computer Incident Response Team
(U) DHS	Department of Homeland Security
(U) DMZ	Demilitarized Zone
(U) DS	Bureau of Diplomatic Security
(U) DS/SI/CS	Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security
(U) FAM	<i>Foreign Affairs Manual</i>
(U) FISMA	Federal Information Security Management Act of 2002
(U) IRM	Bureau of Information Resource Management
(U) IRM/IA	Bureau of Information Resource Management, Office of Information Assurance
(U) ISCP	Information System Contingency Plans
(U) ISSC	Information Security Steering Committee
(U) IT	information technology
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) POA&M	Plans of Action and Milestones
(U) SI	Security Infrastructure Directorate
(U) SSP	System Security Plan
(U) SP	Special Publication
(U) US-CERT	U.S. Computer Emergency Readiness Team
(U) UII	Unique Investment Identifiers

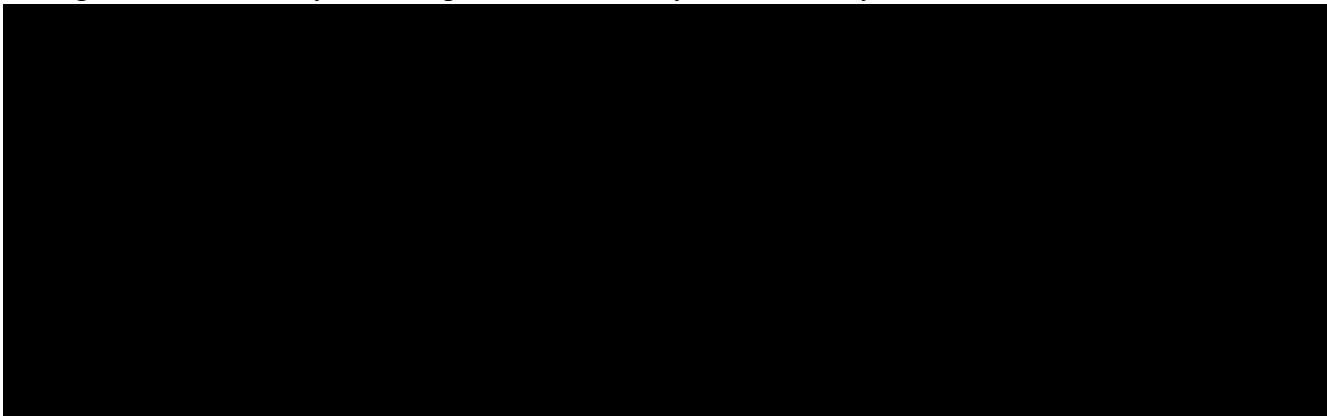
(U) TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
(U) Executive Summary	1
(U) Background	3
(U) Objective	4
(U) Results of Audit.....	4
(U) A. The Department Has Not Effectively Managed Risk for All Phases of the Risk Management Framework	4
(U) B. The Department Has Not Implemented [REDACTED]	8
(U) C. The Department Has Not Implemented [Redacted] (b) (5)	9
(U) D. The Department Has Not Implemented [REDACTED]	13
(U) E. The Department Has Not Effectively Managed Its Plans of Action and Milestones ..	16
(U) F. The Department Has Not Fully Documented and [Redacted] (b) (5)	19
(U) G. The Department Has Not Tracked [REDACTED]	21
(U) H. The Department Has Not Provided and Tracked Security Awareness Training for All Users	23
(U) I. The Department Has Not Updated the Foreign Affairs Manual With Information on the [REDACTED]	24
(U) J. The Department Has Not Fully Followed Incident Response Guidance for Reporting Potential Data Spillage Incidents	26
(U) List of Recommendations.....	27
(U) Appendices	32
(U) A. Scope and Methodology	32
(U) B. Follow-up of Recommendations from the FY 2013 Audit of the Department of State Information Security Program	37
(U) C. [REDACTED] Management Process Needs Improvement.....	44
(U) D. Sample Selection of Information Systems Listed In Information Technology Asset Baseline Used For FY 2014 Audit.....	46
(U) E. Criteria for Findings.....	48
(U) F. Management’s Response to the Draft Report	55

(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). See Appendix A for more information on our audit scope and methodology. Based on the results of the audit, we found that the Department was not in compliance with FISMA, OMB, and NIST requirements.

(SBU) Collectively, the control deficiencies we identified during this audit represent a significant deficiency² to enterprise-wide security, as defined by OMB Memorandum M-14-04.³



(SBU) In addition, we have identified information security program areas that need improvement, including [Redacted] (b) (5) [Redacted]. Information technology security controls are important to protect confidentiality, integrity, and availability of information and information systems. When they are absent or deficient, information becomes vulnerable to compromise. [Redacted] (b) (5)



¹ (U) Pub. L. No. 107-347, tit. III, 116 Stat. 2946, (2002).

² (U) According to OMB Memorandum M-14-04, a significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

³ (U) OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013.

⁴ (U) See Appendix D, Table 2, for a list of sampled systems tested since FY 2010.

⁵ (U) [Redacted] (b) (5)



SENSITIVE BUT UNCLASSIFIED

is collaborating to improve the security of unclassified networks through the testing of technical controls to safeguard information systems.

(U) The Department has taken action to address deficiencies reported in OIG's FY 2013 FISMA report. For example, the Department has:

- (U) Approved a risk management framework within its information security program.
- (U) Obtained an Authority to Operate (ATO) for the OpenNet general support system.
- (U) Approved an enterprise-wide continuous monitoring strategy.
- (U) Implemented periodic vulnerability and compliance scanning.
- (U) Acquired a software application to manage POA&Ms enterprise-wide.

(U) In addition, the Chief Information Security Officer stated that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), received a budget of \$14 million in FY 2014, an increase from \$7 million in FY 2013.⁶ A majority of the budget was used for contractor support to improve FISMA compliance efforts.

(U) Although we acknowledge the Department's actions to improve its information security program, we continue to find security control deficiencies in multiple information security program areas that were previously reported in FY 2010,⁷ FY 2011,⁸ FY 2012,⁹ and FY 2013.¹⁰ Over this period, we consistently identified similar control deficiencies in more than 100 different systems.¹¹ As a result, the OIG issued a Management Alert in November 2013 titled "OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program"¹² that discussed significant and recurring control weaknesses in the Department's Information System Security Program [Redacted] (b) (5) [Redacted]. The FY 2013 FISMA audit report contained 29 recommendations intended to address identified security deficiencies. During this audit, we reviewed corrective actions taken by the Department to address the deficiencies reported in the FY 2013 FISMA report. Based on the actions taken by the Department, OIG closed 4 of 29 recommendations from the FY 2013 report (see Appendix B, "Follow up of Recommendations from the FY 2013 Audit of the Department of State Information Security Program"). In this report, we are making 33 recommendations to the Department to address security deficiencies identified in 11 FISMA reportable areas.

⁶ (U) www.federalnewsradio.com, *Federal News Radio*, "State on path toward recovery after harsh IG report on cyber," July 2014.

⁷ (U) OIG, AUD/IT-11-07, *Review of Department of State Information Security Program*, November 2010.

⁸ (U) OIG, AUD/IT-12-14, *Evaluation of Department of State Information Security Program*, November 2011.

⁹ (U) OIG, AUD-IT-13-03, *Audit of Department of State Information Security Program*, November 2012.

¹⁰ (U) OIG, AUD-IT-14-03, *Audit of Department of State Information Security Program*, November 2013.

¹¹ (U) See Appendix D, Table 2, of this report for details on the systems tested.

¹² (U) <http://oig.state.gov/documents/organization/220066.pdf>, *OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program*, November 2013.

SENSITIVE BUT UNCLASSIFIED

(U) In response to the draft report (see Appendix F), both the Bureau of Information Resource Management and the Bureau of Diplomatic Security concurred with the recommendations we offered to strengthen the Department's information security program. Based on the response, OIG considers all 33 of the recommendations resolved, pending further action. Management's response and OIG's reply are presented after each recommendation.

(U) Background

(U) The Department is the U.S. Government's principal agency for advancing freedom for the benefit of the American people and the international community by helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed states that respond to the needs of their people, reduce widespread poverty, and act responsibly within the international system. The Department's mission is carried out by seven bureaus covering the geographic regions of the world and international organizations and over 30 functional and management bureaus. These bureaus provide policy guidance, program management, administrative support, and in depth expertise in matters such as law enforcement, economics, the environment, intelligence, arms control, human rights, counterterrorism, public diplomacy, humanitarian assistance, security, nonproliferation, consular services, and other areas.

(U) With the passage of FISMA, Congress recognized the importance of information security to the economic and national security interests of the United States and required each Federal agency to 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, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that support Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

(U) To strengthen information system security, FISMA has assigned specific responsibilities to the Department of Homeland Security (DHS), NIST, OMB, and other Federal agencies. In particular, FISMA requires the head of each agency to 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, FISMA requires agency program officials, CIOs, 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 provides guidance with reporting categories and questions to meet the current year's reporting requirements.¹³ OMB uses responses to its questions to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

¹³ (U) DHS, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, December 2013.

(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 2014 and included testing the effectiveness of security controls for a subset of systems as required.

(U) Results of Audit

(U) We identified control deficiencies in all [REDACTED] of the information security program areas used to evaluate the Department's information security program. Although we recognize that the Department has made progress in the areas of risk management, configuration management, and POA&M since FY 2013, we concluded that the Department is not in compliance with FISMA, OMB, and NIST requirements. Collectively, the control deficiencies we identified during this audit represent a significant deficiency to enterprise-wide security, as defined by OMB Memorandum M-14-04.

(U) Finding A. The Department Has Not Effectively Managed Risk for All Phases of the Risk Management Framework

(U) The Department has not effectively managed risk for all phases of the risk management framework.¹⁴ Since FY 2010, this has been a perennially recurring problem across many Department systems and is undoubtedly systemic in nature, requiring global measures in attempt to remedy this deficiency. OIG acknowledges that the Department, with guidance from the Information Security Steering Committee (ISSC), has documented and approved an enterprise-wide risk management strategy to address previously identified risk management findings, but the strategy had not been fully implemented at the time of this audit. In addition, the Department has not effectively managed risk for all six phases of the risk management framework (categorize, select controls, implement, assess, authorize, and monitor).

(U) Risk Management Framework Phases: Categorize, Select Controls, Implement, Authorize

- (U) Of 17 systems tested, 5 (29 percent) have been placed into production without a System Security Plan (SSP).
- (U) Of the 12 systems with an SSP, we found:
 - a. (U) Of 12 SSPs, 7 (58 percent) have not been approved by the system owner.
 - b. (U) Of 12 SSPs, 2 (17 percent) have not been aligned with the respective Security Categorization Form.¹⁵
 - i. (SBU) [Redacted] (b) (5)

¹⁴ (U) OIG has reported deficiencies related to risk management since its FY 2010 audit. Many of the same deficiencies remained uncorrected in FY 2014.

¹⁵ (U) The Security Categorization Form determines the NIST controls that are required to be selected and implemented prior to the system operating in production.

SENSITIVE BUT UNCLASSIFIED

Security Categorization Form, but categorized as “high” within its SSP.

- ii. (SBU) [Redacted] (b) (5)
[Redacted]
- c. (U) Of 12 SSPs, 1 (8 percent) has not been updated (that is, within 3 years); has not documented accreditation boundaries that included people, processes, and technology; and has not aligned to the NIST Special Publication (SP) 800-60 Volume 2, Revision 1, categorizations.
- d. (U) Of 12 SSPs, 3 (25 percent) have used outdated NIST SP 800-53 controls (that is, Revision 2 or earlier) to perform security impact analyses.

(U) *Risk Management Framework Phases: Assess, Monitor*

- (U) Of 17 systems tested, 7 (41 percent) do not have required Security Assessment Reports, which assist in determining security control effectiveness.

(U) *Risk Management Framework phases: Authorize, Monitor*

- (SBU) [Redacted] (b) (5)
[Redacted]

(U) Please see Appendix E, Table 1, for OMB, Committee on National Security Systems, and the Department’s Assessment and Authorization Toolkit requirements related to internal and external risk management.

(SBU) [Redacted] (b) (5)
[Redacted]

¹⁶ (U) In addition to the 17 systems tested for general risk management requirements, two of the Department’s general support systems (OpenNet and ClassNet) were added to our sample, bringing the total number of systems tested for ATOs to 19 systems.

(SBU) [Redacted] (b) (5)

(U) Without implementing an effective 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, the Department cannot appropriately set Department boundaries, perform timely Assessment and Authorization activities, and authorize its systems. Further, without explicit authorization to operate a system, Department information systems have operated at an unknown risk level and could introduce vulnerabilities into the Department's information systems.

(U) **Recommendation 1.** OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement a risk management framework strategy for the Department that 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 concurred with this recommendation.

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has implemented a risk management framework strategy.

(SBU) **Recommendation 2.** [Redacted] (b) (5)

(SBU) **Management Response:** IRM concurred with this recommendation and stated that [Redacted] on September 17, 2014.

(SBU) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has completed [Redacted] (b) (5)

(SBU) **Recommendation 3.** [Redacted]

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

SENSITIVE BUT UNCLASSIFIED

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation [Redacted] (b) (5)

[Redacted]

(SBU) Recommendation 4. [Redacted]

[Redacted]

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

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation [Redacted] (b) (5)

[Redacted]

(SBU) Recommendation 5. [Redacted]

[Redacted]

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

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation [Redacted]

[Redacted]

(SBU) Recommendation 6. [Redacted]

[Redacted]

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

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that [Redacted]

[Redacted]

[Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]

(U) Finding B. The Department Has Not Implemented an [Redacted] (b) (5)
[Redacted]

(U) The Department, in coordination with the ISSC, has not implemented the [Redacted] strategy. Since FY 2010, this has been a perennially recurring problem across many Department systems, which is indicative of a systemic problem. Consequently, it requires global measures in attempting to remedy this deficiency. In view of the systemic nature of this problem, the primary addressee for the recommendation concerning this deficiency is the CIO. OIG acknowledges that the Department has documented and finalized an [Redacted] strategy to address [Redacted] findings previously identified during FISMA audits, but it has not fully implemented the strategy. We also noted deficiencies with the strategy. Specifically, the Department’s strategy does not address ClassNet or the implementation of processes associated with the Risk Executive Function, which establishes organizational tolerance and guides agency risk decisions.

(U) Please see Appendix E, Table 2, for criteria provided by OMB to implement continuous monitoring activities.

(SBU) [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) An implemented enterprise-wide [Redacted] (b) (5) strategy will provide stakeholders, system owners, and personnel with a unified understanding of the information system security goals, allowing the Department to [Redacted] (b) (5) a dynamic network environment with changing threats, vulnerabilities, technologies, missions, and business functions of the Department. However, as a result of not implementing a [Redacted] (b) (5) strategy, we found the following control deficiencies that would have been identified if a [Redacted] process had been implemented. Specifically, we found:

- (SBU) [Redacted] (b) (5)
[Redacted]
- (SBU) [Redacted] (b) (5)
[Redacted]

¹⁷ (U) See Finding C of this report for further details.

¹⁸ (U) See Finding A of this report for further details.

- (SBU) [Redacted] (b) (5) [Redacted]
- (SBU) [Redacted] (b) (5) [Redacted]
- (SBU) [Redacted] (b) (5) [Redacted]
- (SBU) [Redacted] (b) (5) [Redacted]

(U) **Recommendation 7.** OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement the Department's [Redacted] (b) (5) strategy, that includes a [Redacted] (b) (5) policy, 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 concurred with this recommendation.

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department's [Redacted] strategy, that includes a [Redacted] (b) (5) policy, has been implemented.

(U) Finding C. The Department Has Not Implemented End-To-End [Redacted] of Its Components

(SBU) [Redacted] (b) (5) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(SBU) [Redacted] (b) (5) [Redacted]
[Redacted]
[Redacted]

¹⁹ (U) See Finding A of this report for further details.
²⁰ (U) See Appendix C of this report for further details.
²¹ (U) See Finding F of this report for further details.
²² (U) See Finding D of this report for further details.
²³ (U) [Redacted] is the entire process of a change cycle, software or hardware, from the idea phase, to the implementation phase, and on to the release phase.

SENSITIVE BUT UNCLASSIFIED

[Redacted] (b) (5) [Redacted]
[Redacted]

- (SBU) [Redacted] (b) (5) [Redacted]
[Redacted]
[Redacted]
- a. (SBU) [Redacted] (b) (5) [Redacted]
- b. (SBU) [Redacted] (b) (5) [Redacted]
- c. (SBU) [Redacted] (b) (5) [Redacted]
- (SBU) [Redacted]
- (SBU) [Redacted]
- (SBU) [Redacted]
[Redacted]
[Redacted]
- (SBU) [Redacted]
[Redacted]
[Redacted]

(U) Please see Appendix E, Table 3, for NIST and *Foreign Affairs Manual* (FAM) requirements relating to internal and [Redacted] (b) (5).

(SBU) [Redacted] (b) (5) [Redacted]
[Redacted]

- (SBU) [Redacted]
[Redacted]
- (SBU) [Redacted] (b) (5) [Redacted]
[Redacted]
- (SBU) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(SBU) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

24 (U) [Redacted] (b) (5) [Redacted]

25 (U) [Redacted] (b) (5) [Redacted]
[Redacted]

26 (U) See Appendix D for the list of systems selected for testing.

SENSITIVE BUT UNCLASSIFIED

[Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) Recommendation 8. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Enterprise Network Management Office, and the Bureau of Diplomatic Security, develop, finalize, and

[Redacted]
[Redacted]
[Redacted]

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has developed, finalized, and [Redacted] (b) (5)

[Redacted]

(U) Recommendation 9. OIG recommends that the Chief Information Officer, in coordination with all bureaus and/or offices, continue to improve processes [Redacted]

[Redacted] (b) (5)
[Redacted]

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has continued to improve processes to [Redacted]

[Redacted]

(SBU) Recommendation 10. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine an appropriate timeframe to [Redacted] (b) (5)

[Redacted]
[Redacted].

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

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has determined an appropriate timeframe to [Redacted] (b) (5)

[Redacted]
[Redacted]

SENSITIVE BUT UNCLASSIFIED

(SBU) Recommendation 11. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine whether the [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

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

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that (1) the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, has determined whether the [REDACTED]

[REDACTED] (5)
[REDACTED]
[REDACTED]

(SBU) Recommendation 12. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, research, develop, and implement capabilities to perform [REDACTED]

[Redacted] (b) (5)
[REDACTED]
[REDACTED]
[REDACTED]

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

(SBU) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, has researched, developed, and implemented

[REDACTED]
[REDACTED]
[REDACTED]

(SBU) Recommendation 13. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, update the [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

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

(SBU) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department has updated [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Finding D. The Department Has Not Implemented Effective [REDACTED]
[REDACTED]

(U) The Department has not implemented [REDACTED] Department systems. Since FY 2010, this has been a perennially recurring problem across many Department systems, which is indicative of a systemic problem. Consequently, it requires global measures in attempting to remedy this deficiency. In view of the systemic nature of this problem, one of the recommendations involves revising the *Foreign Affairs Manual*. Specifically, we found:

- (SBU) [REDACTED]
[REDACTED]
- (U) System owners have not provisioned user accounts effectively for OpenNet and ClassNet Active Directory (AD) accounts.²⁸ Specifically,
 - a. (SBU) [Redacted] (b) (5) [REDACTED]
[REDACTED]
 - b. (U) Of 22 tested new user accounts created in FY 2014, (17 OpenNet and 5 ClassNet), the Department was unable to provide 19 (86 percent) new user account request forms.
 - c. (U) Of 22 [REDACTED]
[REDACTED]
 - d. (U) For systems that resided on ClassNet, system owners have not:
 - i. (SBU) [Redacted] (b) (5) [REDACTED]
[REDACTED]
 - ii. (SBU) [Redacted] (b) (5) [REDACTED]
[REDACTED]

²⁷ (U) Elevated access request forms are required prior to creating administrator accounts.

²⁸ (U) We sampled three different populations of accounts: [REDACTED]
[REDACTED].

²⁹ (U) Active Directory is a directory service developed by Microsoft for the Windows domain network.

³⁰ (SBU) [REDACTED]

SENSITIVE BUT UNCLASSIFIED

(U) Please see Appendix E, Table 4, for requirements relating to internal and external access management such as the FAM, NIST, the Department of State Global Address List and Active Directory Standardization, and All Diplomatic and Consular Posts Telegram.

(SBU) The Department has used a [REDACTED]. Specifically,

- (U) System owners have failed to comply with the documented policy, which has resulted in users inconsistently completing the appropriate access forms (that is, for new user access and elevated rights) prior to granting access.
- (SBU) [Redacted] (b) (5) [REDACTED]
[REDACTED]
[REDACTED].
- (U) System owners have failed to comply with the Department's [REDACTED] [Redacted] (b) (5) [REDACTED].

(U) In addition, as of June 2014, the Department's FAM does not define a time period for [Redacted] (b) (5) [REDACTED].

(U) Without effective identity and access management, the risk of [REDACTED]
[REDACTED]
[REDACTED]

(U) Recommendation 14. OIG recommends the Bureau of Information Resource Management, Office of Information Assurance, in coordination with 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 concurred with this recommendation.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has followed 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) Recommendation 15. OIG recommends that the Bureau of Information Resource Management, in coordination with Human Resources and system owners, ensure the [Redacted] (b) (5) [REDACTED]
[REDACTED]

³¹ (U) The Department's Active Directory and Global Address List Standardization guidelines aids account administration across the enterprise.

SENSITIVE BUT UNCLASSIFIED

(U) Management Response: IRM and HR concurred with this recommendation and stated that a pilot arrangement has been designed to help [REDACTED]
[REDACTED]

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has ensured [REDACTED]
[REDACTED]

(U) Recommendation 16. OIG recommends that the Chief Information Officer, in coordination with bureaus, review its [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has reviewed its [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Recommendation 17. OIG recommends the Bureau of Diplomatic Security revise the *Foreign Affairs Manual* for unclassified systems to define a [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

(U) Management Response: DS concurred with this recommendation and stated that the *Foreign Affairs Handbook* [REDACTED] (b) (5) [REDACTED] and *Foreign Affairs Manual* [REDACTED] [REDACTED] have been updated, and published, to [REDACTED] (b) (5) [REDACTED]
[REDACTED]

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Bureau of Diplomatic Security has revised the *Foreign Affairs Manual* for unclassified systems to define a time period for bureaus and posts [REDACTED]
[REDACTED]

(U) Finding E. The Department Has Not Effectively Managed Its Plans of Action and Milestones

(U) The Department has not consistently identified, assessed, prioritized, and monitored the progress of corrective actions for identified security deficiencies found in its information security program. Since FY 2010, this has been a perennially recurring problem across many Department systems, which is indicative of a systemic problem. Consequently, it requires global measures in attempting to remedy this deficiency. OIG acknowledges that the Department has acquired a new [REDACTED] to address previously identified POA&M findings, but the tool was not being fully applied at the time of our audit. Therefore, the management of the POA&M process continues to be ineffective and does not capture necessary elements for remediation and capital planning. Various bureau system owners have also failed to follow the Department's policy of completing all the necessary elements of a POA&M. Specifically,

- (U) For systems that reside on OpenNet, we found:
 - a. (U) System owners and IRM/IA have been unable to provide evidence of remediation efforts for 2 (9 percent) of 22 closed POA&Ms (that is, POA&Ms with corrective actions verified by IRM/IA).
 - b. (SBU) [REDACTED],
 - i. (U) Of 29 findings identified in the FY 2013 FISMA audit report, none (100 percent) were incorporated in the master POA&M database.
 - ii. (SBU) [REDACTED]
 - iii. (U) The POA&M database excluded findings from DS vulnerability assessments.
 - c. (U) System owners have not adhered to established completion dates for POA&Ms. Specifically, of 22 completed POA&Ms (that is, actions submitted by system owners pending IRM/IA validation), 2 POA&Ms (9 percent) exceeded the scheduled completion dates by 600 or more days.
 - d. (U) System owners have not consistently updated all POA&M fields. Specifically,
 - i. (U) Of 901 POA&Ms closed in FY 2014, 116 (13 percent) have not budgeted resources.
 - ii. (U) Of 901 POA&Ms closed in FY 2014, 82 (9 percent) have not recorded Unique Investment Identifiers (UIIs).³²
 - (U) 69 (8 percent) of 901 actions have been reported as “no major investment,” and
 - (U) 13 (1 percent) of 901 actions have been reported as “Not Provided.”
 - e. (U) The CIO has not integrated the POA&M information, including costs and resources for corrective actions, into the capital planning process.

³² (U) A UII 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.

SENSITIVE BUT UNCLASSIFIED

- f. (U) The Department has not cross-referenced the POA&Ms to the budget submissions with a UII.
- g. (U) IRM/IA has not sent POA&M grading memos to Department bureaus. Specifically, for the first quarter of FY 2014, 1 of 8 (13 percent) bureaus tested did not receive a grading memo from IRM/IA. For the second quarter of FY 2014, 7 of 8 (88 percent) bureaus tested did not receive a grading memo from IRM/IA.
- h. (U) Of 8 bureaus tested, 7 bureaus (88 percent) did not send their responses, after receipt of the POA&M grading memos from IRM/IA, to close out corrective actions to the CIO.

(U) For systems residing on ClassNet, we found:

- i. (U) System owners did not consistently update all POA&M fields. Specifically,
 - i. (U) Of 26 POA&Ms closed in FY 2014, 11 (42 percent) have not budgeted resources.
 - ii. (U) Of 26 POA&Ms closed in FY 2014, 2 (8 percent) have not recorded a UII.

(U) Please see Appendix E, Table 5, for Clinger Cohen Act, FAM, NIST, OMB, and POA&M Toolkit requirements relating to POA&Ms.

(U) The POA&M deficiencies we identified occurred, in part, because:

- (U) The ISSC, and all appropriate system owners, did not develop priorities and determine the availability of resources to ensure that Department bureaus complied with POA&M requirements, as required by the FAM.
- (U) Bureau system owners failed to take management actions to ensure that they entered UII data, including costs that link POA&Ms to the agency's budget submission, and completed work on schedule.
- (U) Bureau system owners did not consistently provide corrective action plans to resolve open actions to IRM/IA.
- (U) IRM/IA and system owners did not prioritize resources to include the ongoing vulnerability assessment results, found by DS/SI/CS, within the quarterly updated POA&M database because of the biweekly frequency of the vulnerability assessments performed. In addition, Department officials stated that these vulnerabilities were expected to be closed within a short amount of time, thus recording them in the POA&M database was unnecessary.
- (U) The POA&M Toolkit did not define a time period for when deficiencies identified during audits should be included in the master POA&M database, in accordance with NIST SP 800-53, Revision 4.

(U) Without adequate identification, assessment, prioritization, and monitoring of corrective actions on an enterprise basis, the most important actions (highest security risks) affecting the Department may not be fully funded, resolved within a timely manner, or

SENSITIVE BUT UNCLASSIFIED

communicated to senior management, thus exposing the Department's sensitive data, systems, and hardware to unauthorized access and potentially malicious attacks.

(U) Recommendation 18. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, exercise the authorities prescribed in the *Foreign Affairs Manual* (1 FAM 040 and 5 FAM 119) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plans of Action and Milestones.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has effectively implemented and validated remediation actions prior to closing Plans of Action and Milestones.

(U) Recommendation 19. OIG recommends that system owners, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, ensure that bureaus, offices, and posts adhere to completion dates for corrective actions and/or ensure that the remediation dates are updated, as needed. In addition, OIG recommends system owners implement processes and procedures to cross-reference Plans of Action and Milestones information, including costs, to the capital planning budget process with a Unique Investment Identifier.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that bureaus, offices, and posts have adhered to completion dates for corrective actions and/or ensured that the remediation dates are updated, as needed. In addition, this recommendation can be closed when OIG receives and accepts documentation showing that system owners have implemented processes and procedures to cross-reference Plans of Action and Milestones information, including costs, to the capital planning budget process with a Unique Investment Identifier.

(U) Recommendation 20. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), consistently assess overall bureau risk and provide bureaus with *Quarterly Plans of Action & Milestones Grade* memoranda. In addition, OIG recommends that bureaus and/or offices provide written responses for the *Quarterly Plans of Action & Milestones Grade* memoranda to IRM/IA.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that IRM/IA has

SENSITIVE BUT UNCLASSIFIED

systematically assessed bureau risk and *Quarterly Plans of Action & Milestones Grade* memoranda have been issued and written responses received from the bureaus.

(U) Recommendation 21. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), define a time period for bureaus and/or offices to include identified deficiencies resulting from audits into the Plans of Action and Milestones (POA&M) database and communicate findings to IRM/IA in accordance with Office of Management and Budget Memorandum M-11-33.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that IRM/IA has defined a time period for bureaus and/or offices to include identified deficiencies resulting from audits into the POA&M database and communicate the findings to IRM/IA.

(U) Recommendation 22. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify deficiencies resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, and include those vulnerabilities that are not immediately remediated in the Plans of Action and Milestones database in accordance with Office of Management and Budget Memorandum M-11-33.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has identified deficiencies resulting from the vulnerability scans and includes those vulnerabilities that are not immediately remediated in the Plans of Action and Milestones database.

(U) Finding F. The Department Has Not Fully Documented and Implemented Its [REDACTED]

(U) The Department has not fully documented and implemented [REDACTED] [REDACTED] which has been reported as a FISMA deficiency since FY 2010. Although the Department has documented and finalized its [REDACTED] [REDACTED]

33 (U) [REDACTED]

SENSITIVE BUT UNCLASSIFIED

Revision 1,³⁴ and NIST SP 800-53, Revision 4.³⁵ Specifically, we found that the Department has not:

- (U) Documented [Redacted] (b) (5) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]

(U) Please see Appendix E, Table 6, for NIST and FAM requirements relating to [Redacted].

(U) The [Redacted] identified occurred, in part, because IRM/IA has not consistently assessed the [Redacted] and communicated the outstanding actions to system owners. In addition, system owners have not consistently mitigated outstanding actions. Furthermore, system owners have not prioritized resources to complete the annual requirements for review and approval of [Redacted].

(U) Without fully developed and implemented [Redacted].

(U) Recommendation 23. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, review system owner-prepared [Redacted] with the applicable *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department

³⁴ (U) [Redacted] (b) (5) [Redacted].

³⁵ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organization*, April 2013 (last updated January 2014).

[Redacted] (b) (5)

(U) Recommendation 24. OIG recommends that the Chief Information Officer, in coordination with system owners and the Bureau of Information Resource Management, Office of Information Assurance, review [Redacted] [Redacted] *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines, including the identification [Redacted]

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has reviewed [Redacted] for compliance with applicable *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines, including the [Redacted]

(U) Finding G. The Department Has Not Tracked [Redacted]

(SBU) [Redacted] (b) (5)

(U) Please see Appendix E, Table 7, for FAM requirements related to the [Redacted]

(U) No single office within the Department has managed the oversight [Redacted] This is due to the lack of communication between IRM, DS, and applicable bureaus related to this topic. DS has maintained its own list of [Redacted], which has been the basis for its yearly review. However, by policy, IRM should maintain the official listing of [Redacted] (b) (5) within iMATRIX. However, IRM has not dedicated a resource to do so or implemented procedures to coordinate with DS and applicable bureaus.

³⁶ (U) [Redacted] (b) (5)

SENSITIVE BUT UNCLASSIFIED

(U) By not following Department policies for [REDACTED], the Department has minimal assurance that the information security controls for [Redacted] (b) (5) are compliant with FISMA, OMB requirements, and NIST standards. In addition, there is an increased risk that the Department's data that is collected and processed may be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

(U) Recommendation 25. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, consolidate and track [REDACTED] within iMATRIX, in accordance with the *Foreign Affairs Manual* [Redacted] (b) (5)

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and [REDACTED] within iMATRIX.

(U) Recommendation 26. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security ensure that Memoranda of Agreement are completed [REDACTED] as defined in accordance with the *Foreign Affairs Manual* [Redacted] (b) (5)

(U) Management Response: IRM concurred with this recommendation and stated that IRM will update the requirements in [REDACTED] regarding Memorandum of Agreements with regard to [REDACTED]

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has ensured that Memoranda of Agreement are completed for all [REDACTED] extensions as defined in accordance with the *Foreign Affairs Manual* [REDACTED]

(U) Recommendation 27. OIG recommends that the Assistant Secretary for Diplomatic Security ensure that [REDACTED] are completed for [REDACTED] as defined within each Memorandum of Agreement.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Assistant Secretary for Diplomatic Security has ensured that [REDACTED] as defined within each Memorandum of Agreement.

(U) Finding H. The Department Has Not Provided and Tracked Security Awareness Training for All Users

(U) The Department has not provided and tracked the completion of security awareness training for all users with access to the Department's systems. Specifically, we found:

- (U) Key IT personnel, such as users with privileged network user accounts or users who have responsibilities that allow them to increase or decrease cybersecurity, have not taken specialized role-based security training.
- (U) DS has not fully implemented a tracking mechanism for role-based training.
- (U) For 22 existing users tested, 1 existing user (5 percent) has not completed an annual security awareness course since 2012, but still retained access to ClassNet.³⁷

(U) Please see, Appendix E, Table 8, for NIST and FAM requirements relating to security awareness training.

(U) The deficiencies we identified occurred because IRM/IA, in coordination with DS/SI/CS, has not implemented an effective security awareness program. Although we found that the Cybersecurity Awareness, Training, Education and Professionalism Working Group had developed a training plan that included the required role-based training courses for all key IT personnel, the Chief Information Security Officer has not approved the plan for implementation. Further, according to a DS official, DS has not implemented a general security awareness course for ClassNet users that do not have access to OpenNet.

(U) Without appropriate training and tracking of all personnel with access to Department systems, including IT personnel with specific security responsibilities, users could compromise the security of the network, resulting in a loss of information; compromise of Personally Identifiable Information; and introduce vulnerabilities to systems.

(U) Recommendation 28. 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's Security Infrastructure Directorate, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities for the Department take specialized role-based security training as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has finalized the Information Assurance Training Plan to ensure key information

³⁷ (U) The user did not have an OpenNet account; however, the user still has had access to classified information through ClassNet increasing the risk of a loss of information, the compromise of Personally Identifiable Information, and the introduction of vulnerabilities to systems.

technology personnel with security responsibilities for the Department take specialized role-based security training.

(U) Recommendation 29. 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's Security Infrastructure Directorate, Office of Computer Security, implement a tracking mechanism for role-based training, in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4, to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has implemented a tracking mechanism for role-based training.

(U) Recommendation 30. OIG recommends that the Information System Steering Committee, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security's Security Infrastructure Directorate, Office of Computer Security, implement a general security awareness course, specific to users with only ClassNet access that do not have OpenNet access, to ensure that those personnel receive the appropriate general security awareness training in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has implemented a general security awareness course, specific to users with only ClassNet access that do not have OpenNet access, to ensure that those personnel received the appropriate general security awareness training.

(U) Finding I. The Department Has Not Updated the *Foreign Affairs Manual* With Information on the Current [REDACTED]

(U) The Department has not updated the FAM with information on the current [REDACTED]

Everywhere enrollment process, instead of the [REDACTED]

³⁸ (U) On November 11, 2011, [Redacted] (b) (5) [REDACTED]

SENSITIVE BUT UNCLASSIFIED

(U) Please see Appendix E, Table 9, for guidance outlined in the FAM relating to the current [REDACTED]

(U) Although the Department has taken actions to address the deficiencies noted in the FY 2013 FISMA report by drafting updates to [REDACTED] the CIO, in coordination with the Bureau of Administration, has not approved the changes yet.

(U) Without an updated policy, local system administrators cannot enforce the appropriate measures for [REDACTED] which could adversely impact confidentiality, integrity, and availability of the Department's data. It has also resulted in users with [REDACTED]

(U) **Recommendation 31.** OIG recommends that the Chief Information Officer, in coordination with the Bureau of Administration, finalize the *Foreign Affairs Manual* [Redacted] (b) (5) [REDACTED] to replace the [REDACTED]

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

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Department has finalized the *Foreign Affairs Manual* [REDACTED]

(U) **Recommendation 32.** OIG recommends that the Bureau of Information Resource Management, Operations, [REDACTED]

[REDACTED] have been finalized.

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

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Bureau of Information Resource Management, Operations, [REDACTED]

(U) Finding J. The Department Has Not Fully Followed Incident Response Guidance for Reporting Potential Data Spillage Incidents

(U) Although we found the Department's Computer Incident Response Team (CIRT) Standard Operating Procedures aligned with NIST SP 800-61, Revision 2,³⁹ procedures do not clearly state all the bureaus, offices, and organizations that require notification prior to closing an incident. As a result, DS/SI/CS did not report all incidents to the U.S. Computer Emergency Readiness Team (US-CERT) as required. Specifically, 1 out of 22 (5 percent) security incidents we tested was not reported to the US-CERT, even though it was a Category 4⁴⁰ incident and involved potential classified spillage. If the Department does not report data spillage incidents (potential or confirmed) to US-CERT within the established timeframes, US-CERT may not be able to help contain the incident and notify appropriate officials within the allotted timeframe.

(U) Please see Appendix E, Table 10, for US-CERT and the Department's requirements relating to incident reporting.

(U) According to a senior DS official, the reason CIRT did not notify US-CERT of the incident mentioned above was because of conflicting guidance within the CIRT Standard Operating Procedures. That is, the guidance was interpreted to indicate that the incident ticket should be closed after reporting the incident to DS/SI, Office of Information Security, Program Applications Division.

(U) Recommendation 33. OIG recommends that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, update the Computer Incident Response Team Standard Operating Procedures to require the Computer Incident Response Team to notify the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.

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

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, has updated the Computer Incident Response Team Standard Operating Procedures to require the Computer Incident Response Team to notify the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.

³⁹ (U) NIST SP 800-61, rev. 2, *Computer Security Incident Handling Guide*, August 2012.

⁴⁰ (U) Category 4 incidents are incidents involving improper usage of Department systems or networks (that is, a person that violates acceptable computing use policies).

(U) List of Recommendations

(U) Recommendation 1. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement a risk management framework strategy for the Department that is consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(SBU) Recommendation 2. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(SBU) Recommendation 3. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(SBU) Recommendation 4. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(SBU) Recommendation 5. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(SBU) Recommendation 6. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Recommendation 7. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement the Department's [Redacted] (b) (5) [REDACTED] 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.

SENSITIVE BUT UNCLASSIFIED

(U) Recommendation 8. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, [REDACTED]

(U) Recommendation 9. OIG recommends that the Chief Information Officer, in coordination with all bureaus and/or offices, continue to improve processes to [REDACTED]

(SBU) Recommendation 10. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine an appropriate timeframe to [REDACTED]

(SBU) Recommendation 11. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine whether [REDACTED]

(SBU) Recommendation 12. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, research, develop, and implement capabilities to [REDACTED]

(SBU) Recommendation 13. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, update the [REDACTED]

(U) Recommendation 14. OIG recommends the Bureau of Information Resource Management, Office of Information Assurance, in coordination with 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) Recommendation 15. OIG recommends that the Bureau of Information Resource Management, in coordination with Human Resources and system owners, [Redacted] (b) (5)

[REDACTED], as required by the *Foreign Affairs Manual* [Redacted] (b) (5)

(U) Recommendation 16. OIG recommends that the Chief Information Officer, in coordination with bureaus, review its [REDACTED]

(U) Recommendation 17. OIG recommends the Bureau of Diplomatic Security revise the *Foreign Affairs Manual* for unclassified systems to [REDACTED]

(U) Recommendation 18. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, exercise the authorities prescribed in the *Foreign Affairs Manual* (1 FAM 040 and 5 FAM 119) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plans of Action and Milestones.

(U) Recommendation 19. OIG recommends that system owners, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, ensure that bureaus, offices, and posts adhere to completion dates for corrective actions and/or ensure that the remediation dates are updated, as needed. In addition, OIG recommends system owners implement processes and procedures to cross-reference Plans of Action and Milestones information, including costs, to the capital planning budget process with a Unique Investment Identifier.

(U) Recommendation 20. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), consistently assess overall bureau risk and provide bureaus with *Quarterly Plans of Action & Milestones Grade* memoranda. In addition, OIG recommends that bureaus and/or offices provide written responses for the *Quarterly Plans of Action & Milestones Grade* memoranda to IRM/IA.

(U) Recommendation 21. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), define a time period for bureaus and/or offices to include identified deficiencies resulting from audits into the Plans of Action and Milestones (POA&M) database and communicate findings to IRM/IA in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Recommendation 22. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify deficiencies resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, and include those

SENSITIVE BUT UNCLASSIFIED

vulnerabilities that are not immediately remediated in the Plans of Action and Milestones database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) Recommendation 23. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, review system owner-prepared [REDACTED] in accordance with the applicable *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines.

(U) Recommendation 24. OIG recommends that the Chief Information Officer, in coordination with system owners and the Bureau of Information Resource Management, Office of Information Assurance, review [REDACTED] applicable *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines, [REDACTED]

(U) Recommendation 25. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security,

[REDACTED] (b) (5) within iMATRIX, in accordance with the *Foreign Affairs Manual* [REDACTED]

(U) Recommendation 26. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security ensure that Memoranda of Agreement are completed [REDACTED] in accordance with the *Foreign Affairs Manual* [REDACTED] (b) (5)

(U) Recommendation 27. OIG recommends that the Assistant Secretary for Diplomatic Security ensure that [REDACTED] as defined within each Memorandum of Agreement.

(U) Recommendation 28. 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's Security Infrastructure Directorate, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities for the Department take specialized role-based security training as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Recommendation 29. 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's Security Infrastructure Directorate, Office of Computer Security, implement a tracking mechanism for role-based training, in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4, to ensure that

SENSITIVE BUT UNCLASSIFIED

personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan.

(U) Recommendation 30. OIG recommends that the Information System Steering Committee, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security's Security Infrastructure Directorate, Office of Computer Security, implement a general security awareness course, specific to users with only ClassNet access that do not have OpenNet access, to ensure that those personnel receive the appropriate general security awareness training in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Recommendation 31. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Administration, finalize the *Foreign Affairs Manual* [REDACTED]

(U) Recommendation 32. OIG recommends that the Bureau of Information Resource Management, Operations, [REDACTED]

[REDACTED] once the updates to the *Foreign Affairs Manual* [REDACTED] [REDACTED] have been finalized..

(U) Recommendation 33. OIG recommends that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, update the Computer Incident Response Team Standard Operating Procedures to require the Computer Incident Response Team to notify the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.

(U) Scope and Methodology

(U) 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 2014.

(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 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 March through August 2014. In addition, we performed the audit in accordance with Generally Accepted Government Auditing Standards, FISMA, OMB, and National Institute of Standards and Technology (NIST) guidance. Generally Accepted Government Auditing Standards 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, M-12-20, and M-14-04.⁴

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) DHS, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, December 2013.

⁴ (U) OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001; OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003; OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006; OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 2012; OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013.

SENSITIVE BUT UNCLASSIFIED

- (U) Department policies and procedures such as the *Foreign Affairs Manual*.
- (U) Federal laws, regulations, and standards such as FISMA, OMB Circular A-130, Appendix III,⁵ and OMB Circular No. A-11.⁶
- (U) NIST Special Publications (SP), Federal Information Processing Standards, 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) [Redacted] (b) (5)
- (U) [Redacted] (b) (5)
- (U) [Redacted] (b) (5)
- (U) Incident response and reporting
- (U) Risk management
- (U) Security training
- (U) Plans of Action and Milestones (POA&M)
- (U) [Redacted] (b) (5)
- (U) [Redacted] (b) (5)
- (U) [Redacted] (b) (5)
- (U) Security capital planning

(U) The audit covered the period of October 1, 2013 to August 31, 2014. 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 Federal Information Processing Standards 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 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, dated December 2013.
- (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 OIG identified are presented in the ‘Results of Audit’ section of this report.

⁵ (U) OMB Circular No. A-130, Revised, *Management of Federal Information Resources*, “Security of Federal Automated Information Resources,” November 2000.

⁶ (U) OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, August 2011.

SENSITIVE BUT UNCLASSIFIED

- (U) Evaluated the Department's remedial actions taken to address the previously reported information security program control deficiencies identified in OIG's report *Audit of Department of State Information Security Program* (AUD-IT-14-03, Nov. 2013).

(U) Review of Internal Controls

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

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

(U) On October 16, 2014, OIG held an exit conference to present all findings identified during the audit with the Department. Deficiencies identified with the Department's internal controls are presented in the Audit Results section of this report.

(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 sufficiently reliable for assessing the adequacy of related information security controls.

(U) Sampling Methodology

(U) We received, from the Bureau of Information Resource Management, a population of 17 FY 2014 new and recertified Federal Information Security Management Act of 2002 (FISMA) reportable systems operating for the Department. We tested all 17 of these systems, which are listed in Table 1 of Appendix D.

(U) With respect to the sampling methodology employed, *Government Auditing Standards* indicate that either a statistical or judgment sample can yield sufficient and appropriate audit evidence. A statistical sample is generally preferable, although it may not always be practicable. By definition, a statistical sample requires that each sampling unit in the population be selected via a random process and have a known, non-zero chance of selection. These requirements often have posed a problem when conducting audits of the Department. All information systems, irrespective of size or importance, must have a chance to be randomly selected. Therefore, the exclusion of one or more of the small or insignificant systems cannot be allowed. All information systems—large and small—must have a chance to be randomly selected, and that chance must not be zero. However, a Department auditee would undoubtedly deem many small or insignificant information systems too atypical in most instances to merit inclusion in our sample.

(U) Consequently, we must often employ another type of sample permitted by *Government Auditing Standards*—namely, a non-statistical sample known as a judgment sample. A judgment sample is a sample selected by using discretionary criteria rather than criteria based on the laws of probability. In this audit, we have taken great care in determining the criteria to use for sampling information systems. Moreover, we used, whenever practicable, random numbers to preclude the introduction of any bias in sample selection although a non-statistical technique was utilized. We acknowledge that it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist at all in other information systems that were not tested. However, a prudent person without any basis in fact would not automatically assume that these deficiencies are non-existent with other systems. Such a supposition would be especially ill-advised for an issue as important as information security. Moreover, we identified control deficiencies across a total of 102 different systems reviewed over 5 years,⁷ yet many of the same deficiencies have persisted. It would therefore be irrational to presume that other systems would have fared better if selected by us for review.

⁷ (U) See Appendix D, Table 4, of this report.

SENSITIVE BUT UNCLASSIFIED

(U) Where we deemed it was appropriate, we used audit sampling techniques to perform audit procedures to less than 100 percent of the population to enable us to evaluate audit evidence of the items selected to assist in forming a conclusion concerning the population. Generally, for a large population of sample items (more than 2,000), we used non-statistical sampling methods to test 22 items.⁸ For small populations and infrequently operating controls, we used the following table as guidance to select sample sizes:

(U) Table 1. Small Population Size⁹

Control Frequency	Sample Size
Quarterly (4)	2
Monthly (12)	2
Semimonthly (24)	3
Weekly (52)	5

⁸ (U) Items may include sources other than information systems, such as training records, user accounts, documents, or incident tickets.

⁹ (U) *AICPA Audit Guide*, “Small Populations and Infrequently Operating Controls Table 3-5,” March 2012.

(U) Follow-up of Recommendations from the FY 2013 Audit of the Department of State Information Security Program

(U) We have reviewed actions implemented by management to mitigate the findings identified in the FY 2013 Department of State FISMA report. The current status of each of the recommendations is as follows:

(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) Status: Closed. OIG noted that the Chief Information Officer has documented and approved a risk management framework.

(SBU) Recommendation 2. [Redacted] (b) (5)

[Redacted]

(U) Status: Closed. OIG noted that while the full authorization for OpenNet support system is in place, system owners have yet to complete the full authorization on ClassNet to operate in accordance with National Institute of Standards and Technology Special Publication 800-34, Revision 1. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 2 (Finding A) in the FY 2014 report.

(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) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 5 (Finding A) in the FY 2014 report.

(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

SENSITIVE BUT UNCLASSIFIED

Quarterly Plan of Action & Milestones Grade memorandums are provided to the Bureau of Information Resource Management, Office of Information Assurance.

(U) Status: *Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendations 18, 19, 20 (Finding E) in the FY 2014 report.*

(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.

Status: *Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 21 (Finding E) in the FY 2014 report.*

(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) Status: *Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 22 (Finding E) in the FY 2014 report.*

(U) Recommendation 7. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, document an [REDACTED] [REDACTED] consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) Status: *Closed. OIG noted that the Chief Information Officer has [REDACTED] [REDACTED]*

(SBU) Recommendation 8. [Redacted] (b) (5) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(SBU) Status: *Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 8 (Finding C) in the FY 2014 report.*

SENSITIVE BUT UNCLASSIFIED

(SBU) Recommendation 9. [Redacted] (b) (5)
[Redacted]
[Redacted]

(SBU) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 9 (Finding C) in the FY 2014 report.

(SBU) Recommendation 10. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted].

(SBU) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 10 (Finding C) in the FY 2014 report.

(SBU) Recommendation 11. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(SBU) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 11 (Finding C) in the FY 2014 report.

(SBU) Recommendation 12. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

*(SBU) Status: Closed. OIG noted that [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted] This is a repeat recommendation from the FY 2013 report. It has become Recommendation 12 (Finding C) in the FY 2014 report.*

(SBU) Recommendation 13. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted] (b) (5)

(SBU) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 13 (Finding C) in the FY 2014 report.

(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) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 14 (Finding D) in the FY 2014 report.

(SBU) Recommendation 15. [Redacted] (b) (5)

(SBU) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 15 (Finding D) in the FY 2014 report.

(SBU) Recommendation 16. [Redacted] (b) (5)

(SBU) Status: Closed. OIG noted that by addressing Recommendation 15 (Finding D) of this report, the Department could close this finding. Therefore, this is a repeat recommendation from FY 2013 report. It is incorporated into Recommendations 15 (Finding D) in the FY 2014 report.

(U) Recommendation 17. OIG recommends that management review their [Redacted] (b) (5)

(U) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 16 (Finding D) in the FY 2014 report.

(SBU) Recommendation 18. [Redacted] (b) (5)

SENSITIVE BUT UNCLASSIFIED

(SBU) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 17 (Finding D) in the FY 2014 report.

(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 [REDACTED] in accordance with the *Foreign Affairs Manual* [REDACTED] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendations 23 (Finding F) in the FY 2014 report.

(U) Recommendation 20. OIG recommends that the Chief Information Officer, in coordination with [REDACTED] in accordance with National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 24 (Finding F) in the FY 2014 report.

(U) Recommendation 21. OIG recommends that the Office of [REDACTED], in coordination with [REDACTED] Committee for each bureau, [REDACTED] in accordance with the *Foreign Affairs Manual* [REDACTED] (b) (5)

(U) Status: Closed. OIG noted that all [REDACTED] that were tested in FY 2014 were in accordance with the Foreign Affairs Manual [REDACTED] (b) (5)

(U) Recommendation 22. OIG recommends that data center managers enforce the log and record keeping policy to show that [REDACTED] in accordance with the *Foreign Affairs Manual* [REDACTED] (b) (5)

(U) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 23 (Finding F) in the FY 2014 report.

(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 [REDACTED] within iMATRIX, in accordance with the *Foreign Affairs Manual* [REDACTED] (b) (5)

(U) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 25 (Finding G) in the FY 2014 report.

SENSITIVE BUT UNCLASSIFIED

(U) Recommendation 24. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, ensure [REDACTED] as defined within each Memorandum of Understanding.

(U) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 27 (Finding G) in the FY 2014 report.

(U) Recommendation 25. OIG recommends that the Bureau of Diplomatic Security, in coordination with the applicable bureau Information System Security Officers for each [REDACTED], ensure that all Memorandums of Understanding [REDACTED] as defined in the *Foreign Affairs Manual* [REDACTED] (b) (5)

(U) Status: Closed. OIG noted that in FY 2014 for all Memorandums of Understanding each [REDACTED] (b) (5) as defined in the Foreign Affairs Manual [REDACTED] (b) (5)

(SBU) Recommendation 26. [REDACTED] (b) (5)

(U) Status: Closed. As of March 2014, [REDACTED] (b) (5) developed a formal certification process with the Department of State Bureau of Resource Management.

(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) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 28 (Finding H) in the FY 2014 report.

(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) Status: Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 29 (Finding H) in the FY 2014 report.

SENSITIVE BUT UNCLASSIFIED

(U) Recommendation 29. OIG recommends that the Bureau of Information Resource Management, Operations, Messaging Systems Office, E-Mail Operations Division, [Redacted] (b) (5) [Redacted] update the *Foreign Affairs Manual* [Redacted] [Redacted] Management System enrollment process, as the only remote access system for approved users.

(U) Status: *Closed. This is a repeat recommendation from the FY 2013 report. It has become Recommendation 31 and 32 (Finding I) in the FY 2014 report.*

(U) [REDACTED] **Management Process Needs Improvement**

(U) Although the Department has taken actions to address the deficiencies identified in prior years [REDACTED] process still exist in FY 2014. During the vulnerability analysis performed, we identified the following deficiencies:

[Redacted] (b) (5)



(SBU) [Redacted] (b) (5)

A large section of the page is redacted with black bars. The redaction covers approximately four lines of text, starting from the first line below the header and extending down to the first line above the footer.

**(U) Sample Selection of Information Systems Listed In Information
Technology Asset Baseline Used For FY 2014 Audit**

(U) We received, from the Bureau of Information Resource Management, a list of 17 FY 2014 new and recertified Federal Information Security Management Act of 2002 (FISMA) reportable systems operating for the Department. We selected all 17 systems to test.

[Redacted] (b) (5)



[Redacted] (b) (5)



(U) Criteria for Findings

(U) Table 1. Risk Management Requirements

<p>(U) The Department’s Assessment and Authorization Toolkit</p>	<p>(U) “After the SSP has be[en] reviewed, updated and approved by the system owner (in writing), it must be sent to IRM/IA. The SSP will be checked against IRM/IA Detailed SSP Review Checklist which is based on the requirements detailed in NIST SP 800-18.”¹</p> <p>(U) “The assessment information produced by an assessor during continuous monitoring is provided to the information system owner and common control provider in an updated security assessment report. The information system owner and common control provider initiate remediation actions on outstanding items listed in the plan of actions and milestones and findings produced during the ongoing monitoring of security controls.”²</p> <p>(U) “The Authorizing Official will make a determination as to the level of risk that the system brings to the Department's operations, assets, and individuals. If the risk is determined to be acceptable, the Authorizing Official will explicitly accept the risk and then authorize the information system to operate.”³</p>
<p>(U) Office of Management and Budget (OMB) M-10-15</p>	<p>(U) “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.”⁴</p>
<p>(U) Committee on National Security Systems Instruction No. 1253</p>	<p>(U) “The Committee on National Security Systems (CNSS) Instruction No. 1253, <i>Security Categorization and Control Selection for National Security Systems</i>, provides all Federal Government departments, agencies, bureaus, and offices with guidance on the first two steps of the Risk Management Framework (RMF), Categorize and Select, for national security systems (NSS). This Instruction builds on and is a companion document to National Institute of Standards and Technology (NIST) Special Publication (SP), 800-53, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>; therefore, it is formatted to align with that document’s section numbering scheme.”⁵</p>

¹ **(U)** *Assessment and Authorization Toolkit*, “11b. RMF Step 2 – Select Security Controls.”

² **(U)** *Assessment and Authorization Toolkit*, “11f. RMF Step 6 – Monitor Security Controls.”

³ **(U)** *Assessment and Authorization Toolkit*, “11e. RMF Step 5 – Authorize Information System.”

⁴ **(U)** OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, “NIST Standards and Guidelines,” April 2010.

⁵ **(U)** Committee on National Security Systems Instruction No. 1253, *Security Categorization And Control Selection For National Security Systems*, March 2014.

(U) Table 4. Identity and Access Management Requirements

Criteria	
(U) FAM	[Redacted]
(U) NIST SP 800-53, Revision 4	[Redacted]
(U) The Department of [Redacted] [Redacted] (b) (5) [Redacted]	[Redacted]

12 (U) 12 FAM [Redacted]

13 (U) 12 FAM [Redacted]

14 (U) 12 FAM [Redacted]

15 (U) 12 FAM [Redacted]

16 (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “AC-2 Account Management | Disable Inactive Accounts,” April 2013 (last updated January 2014).

17 (U) [Redacted] (b) (5)
[Redacted]

SENSITIVE BUT UNCLASSIFIED

(U) All Diplomatic and Consular Posts Telegram 2008 STATE 8277

(U) Table 5. Plans of Action and Milestones Requirements

(U) Clinger Cohen Act	(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 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.” ¹⁹
(U) FAM	(U) The Information Security Steering Committee (ISSC) shall develop priorities and determine availability of resources for security of Department information systems. ²⁰
(U) NIST SP 800-53, Revision 4	(U) The Department shall update “existing plan of action and milestones...based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.” ²¹
(U) OMB	(U) The required data elements are weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status. ²² (U) “Specifically, for each POA&M that relates to a project (including systems) for which a capital asset plan and justification (2) (exhibit 300) was submitted or was a part of the exhibit 53, the unique project identifier must be reflected on the POA&M. This identifier will provide the link to agency budget materials. Also, for each POA&M for which there is an associated capital asset plan, agencies must also provide the security costs reported on the Exhibit 53” ²³

18 (U) [Redacted] (b) (5)

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

20 (U) 5 FAM 119b, *Information Technology Management*, “Information Security Steering Committee,” February 2008.

21 (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “CA-5 Plan of Action and Milestones,” April 2013 (last updated January 2014).

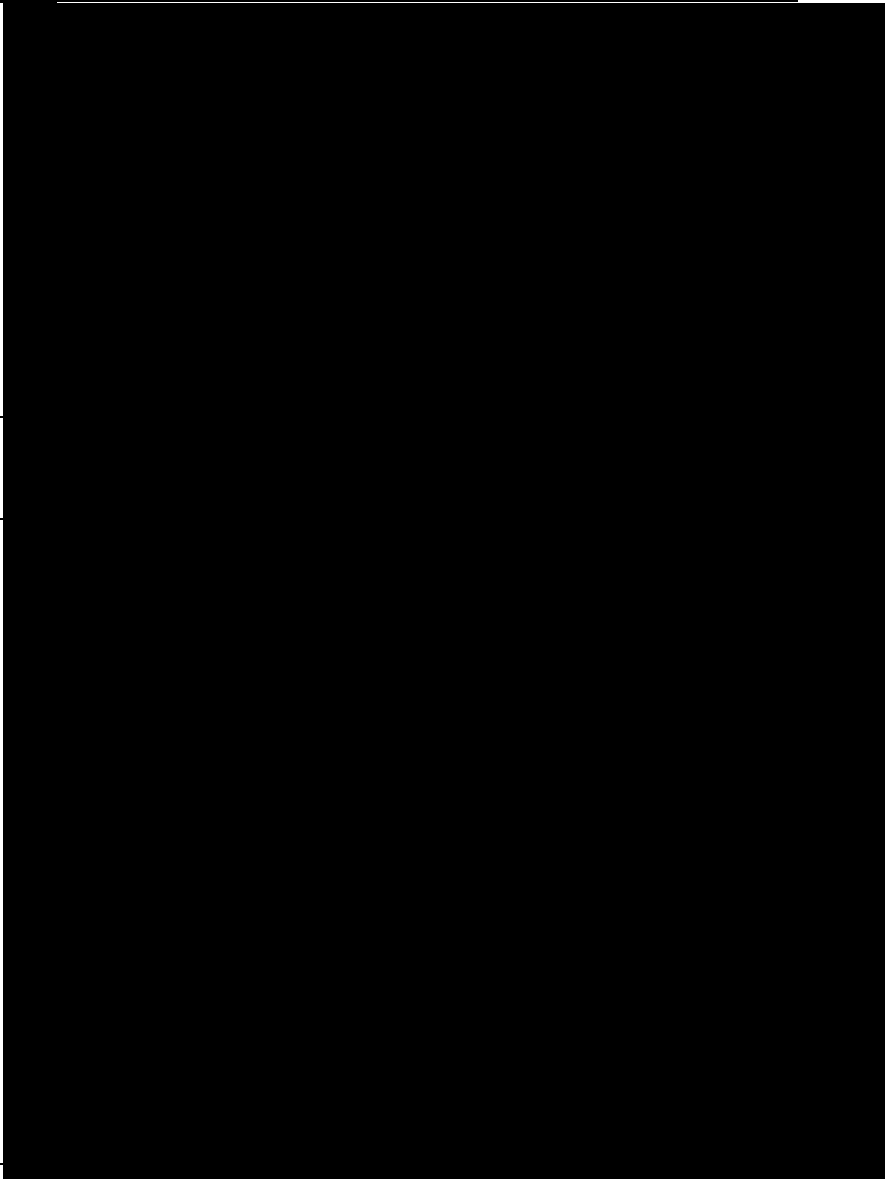
22 (U) OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 2011.

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

SENSITIVE BUT UNCLASSIFIED

(U) Plans of Action and Milestones Toolkit	(U) The Department did not comply with their Plans of Action and Milestones Toolkit. ²⁴
--	--



(U) Table 6. [Redacted] (b) (5) Requirements

(U) NIST SP 800-34, Revision 1	
(U) NIST SP 800-53, Revision 4	
(U) FAM	

²⁴ (U) *POA&M Toolkit*, “How does a Bureau (and its Information System Owners) record that POA&M actions are closed,” “How should a Bureau (and its Information System Owners) identify and enter security weaknesses as POA&M actions?,” “How does the CIO provide oversight and review of the POA&M process?,” “Why is the process to manage POA&Ms and their actions important?,” “How is the quality of the POA&M process monitored?.”

²⁵ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organization*, April 2013 (last updated January 2014).

²⁶ (U) NIST SP [Redacted] (b) (5) 


²⁷ (U) NIST SP 800-53, rev. 4, [Redacted] (b) (5) 


SENSITIVE BUT UNCLASSIFIED

	[Redacted] (b) (5)
--	--------------------

(U) Table 7. [Redacted] (b) (5) Requirements

(U) FAM	[Redacted]
---------	------------

(U) Table 8. Security Awareness Training Requirements

Criteria	
(U) NIST SP 800-53, Revision 4	(U) The “organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.” ³²
(U) FAM	(U) The FAM requires users to complete security awareness training for new users and annually thereafter. ³³

(U) Table 9. [Redacted] (b) Requirements

	Criteria
(U) FAM	[Redacted] (b) (5)

²⁸ (U) 5 FAM [Redacted] (b) (5)

²⁹ (U) 5 FAM [Redacted] (b) (5)

³⁰ (U) 5 FAM [Redacted] (b) (5)

³¹ (U) 5 FAM [Redacted] (b) (5)

³² (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “AT-4 Security Training Records,” April 2013 (last updated January 2014).

³³ (U) 5 FAM 1067.2-2, *Information Assurance Management*, “Training and Education Program,” January 2009.

³⁴ (U) 5 FAM 469.4d, *The Privacy Act and Personally Identifiable Information (PII)*, “Avoiding Technical Threats to Personally Identifiable Information (PII),” June 2013.

SENSITIVE BUT UNCLASSIFIED

	[Redacted] (b) (5) 35
--	--------------------------

(U) Table 10. Incident Reporting Requirements

(U) U.S. Computer Emergency Readiness Team (US-CERT)	(U) US-CERT requires that CIRT report CAT-4 incidents within 1 week of occurrence and that CIRT should not delay reporting in order to gain additional information. ³⁶
(U) Computer Incident Response Team (CIRT) Standard Operating Procedures	(U) In regards to classified spillage, “After the incident is reported to DS/SI/IS/APD [Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division], CIRT can close the ticket. Any follow-up to include verification that the spillage has been contained will be conducted by APD.” ³⁷

³⁵ (U) 12 FAM [Redacted] (b) (5)

³⁶ (U) www.us-cert.gov, *Federal Incident Reporting Guidelines*, “Federal Agency Incident Categories.”

³⁷ (U) CIRT Standard Operating Procedures, “Classified Spillage Incidents,” August 2013.

(U) Management's Response to the Draft Report

(U) We received separate responses to the draft report from the Bureau of Information Resource Management and the Bureau of Diplomatic Security. The Bureau of Information Resource Management provided responses to all recommendations from the draft report. In addition, the Bureau of Diplomatic Security provided responses for Recommendations 17, 27, and 33. Both responses are shown below.

SENSITIVE BUT UNCLASSIFIED

(U) Bureau of Information Resource Management Response



United States Department of State

Washington, D.C. 20520


October 17, 2014

SENSITIVE BUT UNCLASSIFIED

(UNCLASSIFIED when separated from Attachment)


MEMORANDUM

TO: OIG/AUD – Norman P. Brown

FROM: IRM – Steven C. Taylor 

SUBJECT: IRM responses to the draft FY 2014 OIG Audit of the Department of State Information Security Program

Thank you for the opportunity to review and comment on the subject draft report and for recognizing the actions taken this year to improve the Department's Information Security Program. We concur with all 33 recommendations. However, we do not agree with the assessment that the identified weaknesses represent a significant deficiency. In a changing business environment of the Department's size and geographic dispersion, we expect to encounter challenges on a regular basis. However, we believe that based on our progress against the 2014 Corrective Action Plan, instituted in response to the OIG's 2013 audit report, that we have created a foundation for correcting several existing weaknesses and an ability to address new issues as they arise.

Since the CAP inception IRM has kept the OIG aware of our progress in meeting the actions identified to achieve a better Information Security Program. I am pleased to report that we have successfully met the milestones to date. 

[Redacted] (b) (5)

Additionally in the 2014 CAP we identified new personnel resources and aligned our processes to ensure greater compliance with federally mandated security practices.

Additionally, we have published new Department policy and implemented corrective actions to manage [REDACTED]

[Redacted] (b) (5)

[REDACTED]. Collectively, these tools address the automatable aspects of the transition to ongoing authorization as directed by the Office of Management and Budget.

Based on the OIG's 2014 audit report IRM plans to establish and measure performance against a 2015 CAP. This will allow for Department management and the OIG to track the progress toward a FISMA compliant environment.

IRM acknowledges there will always be room for improvement in the Department's Information Security Program and looks forward to continuing the work with the OIG to improve what we all agree is a very important high priority undertaking.

Attachment:

Response to Recommendations of the OIG Audit on Information Security

SENSITIVE BUT UNCLASSIFIED

Drafted: IRM/IA – Peter Gouldmann 10/16/2014 [Redacted] (b) (6)

Approved: IRM/IA – William G. Lay (ok)

Cleared:

IRM/OPS – Glen H. Johnson (ok)

IRM/BMP – Patricia A. Lacina (ok)

IRM/FO – Jeffrey L. Graham (ok)

Response to Recommendations of the OIG Audit on Information Security

Please find the Bureau of Information Resource Management (IRM) responses to recommendations 1-33 contained in the draft FY 2014 OIG Audit of the Department of State's, Information Security Program below:

(U) Recommendation 1. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement a risk management framework strategy for the Department that 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 1: IRM concurs with this recommendation.

(SBU) Recommendation 2. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) IRM Response to Draft Recommendation 2: IRM concurs with this recommendation [Redacted] (b) (5)
[Redacted]
[Redacted]

(SBU) Recommendation 3. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) IRM Response to Draft Recommendation 3: IRM concurs with this recommendation.

(SBU) Recommendation 4 [Redacted] (b) (5)
[Redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] (b) (5)
[Redacted]
[Redacted]

(U) IRM Response to Draft Recommendation 4: IRM concurs with this recommendation.

(SBU) Recommendation 5. [Redacted]
[Redacted]
[Redacted]
[Redacted]

(SBU) IRM Response to Draft Recommendation 5: IRM concurs with this recommendation.

[Redacted] (b) (5)
[Redacted]
[Redacted]

(SBU) Recommendation 6. [Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

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

[Redacted] (b) (5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] (b) (5)

(U) Recommendation 7. OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, implement the Department's [Redacted]

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 concurs with this recommendation.

(U) Recommendation 8. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Information Resource Management [Redacted]

[Redacted] (b) (5)

(U) IRM Response to Draft Recommendation 8: IRM and DS concur with this recommendation.

[Redacted] (b) (5)

(U) Recommendation 9. OIG recommends that the Chief Information Officer, in coordination with all bureaus and/or offices, continue to improve processes to [Redacted] (b) (5)

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

(SBU) Recommendation 10. OIG recommends that the Chief Information

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine an appropriate timeframe to [REDACTED]

(SBU) IRM Response to Draft Recommendation 10: IRM and DS concur with this recommendation.

(SBU) Recommendation 11. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, determine whether [REDACTED]

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

(SBU) Recommendation 12. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, research, develop, and implement capabilities to [REDACTED]

(SBU) IRM Response to Draft Recommendation 12: IRM and DS concur with this recommendation.

[Redacted] (b) (5)

(SBU) Recommendation 13. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Office of Computer Security, update the [REDACTED]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] (b) (5)

(SBU) IRM Response to Draft Recommendation 13: IRM and DS concur with this recommendation.

[Redacted] (b) (5)

(U) Recommendation 14. OIG recommends the Bureau of Information Resource Management, Office of Information Assurance, in coordination with 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) IRM Response to Draft Recommendation 14: IRM concurs with this recommendation.

IRM will work with system owners to raise awareness of their obligation to comply with the FAM.

(U) Recommendation 15. OIG recommends that the Bureau of Information Resource Management, in coordination with Human Resources and system owners,

[Redacted] (b) (5)

(U) IRM Response to Draft Recommendation 15: IRM and HR concur with this recommendation.

IRM and HR have agreed to a pilot arrangement to help consolidate employee separation data.

(U) Recommendation 16. OIG recommends that the Chief Information Officer, in coordination with bureaus, review its [Redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] (b) (5)

(U) **IRM Response to Draft Recommendation 16:** IRM concurs with this recommendation.

(U) **Recommendation 17.** OIG recommends the Bureau of Diplomatic Security revise the *Foreign Affairs Manual* for unclassified systems to [Redacted] (b) (5)

(SBU) **DS Response to Draft Recommendation 17:** DS concurs with this recommendation.

[Redacted] (b) (5)

(U) **Recommendation 18.** OIG recommends that the Chief Information Officer, in coordination with the Information Security Steering Committee, exercise the authorities prescribed in the *Foreign Affairs Manual* (1 FAM 040 and 5 FAM 119) and direct bureaus and/or offices to prioritize resources to effectively implement and validate remediation actions prior to closing Plans of Action and Milestones.

(U) **IRM Response to Draft Recommendation 18:** IRM concurs with this recommendation.

(U) **Recommendation 19.** OIG recommends that system owners, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, ensure that bureaus, offices, and posts adhere to completion dates for corrective actions and/or ensure that the remediation dates are updated, as needed. In addition, OIG recommends system owners

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

implement processes and procedures to cross-reference Plans of Action and Milestones information, including costs, to the capital planning budget process with a Unique Investment Identifier.

(U) IRM Response to Draft Recommendation 19: IRM concurs with this recommendation.

(U) Recommendation 20. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), consistently assess overall bureau risk and provide bureaus with *Quarterly Plans of Action & Milestones Grade* memoranda. In addition, OIG recommends that bureaus and/or offices provide written responses for the *Quarterly Plans of Action & Milestones Grade* memoranda to IRM/IA.

(U) IRM Response to Draft Recommendation 20: IRM concurs with this recommendation.

(U) Recommendation 21. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), define a time period for bureaus and/or offices to include identified deficiencies, resulting from audits, into the Plans of Action and Milestones (POA&M) database and communicate findings to IRM/IA in accordance with Office of Management and Budget Memorandum M-11-33.

(U) IRM Response to Draft Recommendation 21: IRM concurs with this recommendation.

(U) Recommendation 22. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with system owners, identify deficiencies resulting from the vulnerability scans performed by the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, and include those vulnerabilities that are not immediately remediated in the Plans of Action and Milestones database in accordance with Office of Management and Budget Memorandum M-11-33.

(U) IRM Response to Draft Recommendation 22: IRM concurs with this recommendation.

(U) Recommendation 23. OIG recommends that the Chief Information Officer,

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

in coordination with the Bureau of Information Resource Management, Office of Information Assurance, review system owner-prepared [REDACTED] [REDACTED] in accordance with the applicable *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines.

(U) IRM Response to Draft Recommendation 23: IRM concurs with this recommendation.

(U) Recommendation 24. OIG recommends that the Chief Information Officer, in coordination with system owners and the Bureau of Information Resource Management, Office of Information Assurance, review [Redacted] (b) (5) [REDACTED] applicable *Foreign Affairs Manual* and National Institute of Standards and Technology guidelines, including the [REDACTED] [REDACTED]

(U) IRM Response to Draft Recommendation 24: IRM concurs with this recommendation.

(U) Recommendation 25. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security, [REDACTED] within [REDACTED] iMATRIX, in accordance with the *Foreign Affairs Manual* (5 FAM 600).

(U) IRM Response to Draft Recommendation 25: IRM and DS concur with this recommendation.

(U) Recommendation 26. OIG recommends that the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security ensure that Memoranda of Agreement are completed [Redacted] (b) (5) [REDACTED] accordance with the *Foreign Affairs Manual* [Redacted] (b) (5) [REDACTED]

(U) IRM Response to Draft Recommendation 26: IRM concurs with the intent of this recommendation.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

IRM and DS will work to ensure the intent of the OIG's recommendation is implemented and IRM will update the requirements in 5 FAM 1065 regarding Memorandum of Agreements with regard to OpenNet and ClassNet extensions.

(U) Recommendation 27. OIG recommends that the Assistant Secretary for Diplomatic Security ensure that [Redacted] (b) (5) as defined within each Memorandum of Agreement.

(U) DS Response to Draft Recommendation 27: DS concurs with this recommendation.

(U) Recommendation 28. 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's Security Infrastructure Directorate, Office of Computer Security, finalize the Information Assurance Training Plan to ensure key information technology personnel with security responsibilities for the Department take specialized role-based security training as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) IRM Response to Draft Recommendation 28: IRM and DS concur with this recommendation.

(U) Recommendation 29. 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's Security Infrastructure Directorate, Office of Computer Security, implement a tracking mechanism for role-based training, in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4, to ensure that personnel with significant security responsibilities receive the appropriate training according to the Information Assurance Training Plan.

(U) IRM Response to Draft Recommendation 29: IRM and DS concur with this recommendation.

Page 9

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

(U) Recommendation 30. OIG recommends that the Information System Steering Committee, in coordination with the Bureau of Information Resource Management, Office of Information Assurance, and the Bureau of Diplomatic Security's Security Infrastructure Directorate, Office of Computer Security, implement a general security awareness course, specific to users with only ClassNet access that do not have OpenNet access, to ensure that those personnel receive the appropriate general security awareness training in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) IRM Response to Draft Recommendation 30: IRM and DS concur with this recommendation.

DS is already in the process of developing a general security awareness course for ClassNet users in coordination with IRM. Please note that the authority for this recommendation is CNSS 1253 dated 27 March 2014 vice NIST SP 800-53 Rev 4 which does not apply to National Security Systems.

(U) Recommendation 31. OIG recommends that the Chief Information Officer, in coordination with the Bureau of Administration, finalize the *Foreign Affairs Manual* [Redacted] (b) (5)

(U) IRM Response to Draft Recommendation 31: IRM and DS concur with this recommendation.

The reference to OpenNet Everywhere was removed from 5 FAM 460 and published on 01 October 2014. 12 FAM 680 is in clearance and the draft language concerning this recommendation which DS and IRM have agreed is available on the EFAM site. IRM and DS request this recommendation be closed.

(U) Recommendation 32. OIG recommends that the Bureau of Information Resource Management, Operations, [Redacted] [Redacted] once the updates to the *Foreign Affairs Manual* (5 FAM 460 and 12 FAM 680) have been finalized.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

(U) IRM Response to Draft Recommendation 32: IRM concurs with this recommendation.

(U) Recommendation 33. OIG recommends that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, update the Computer Incident Response Team Standard Operating Procedures to require the Computer Incident Response Team to notify the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.

(U) IRM Response to Draft Recommendation 33: DS concurs with this recommendation.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

(U) Bureau of Diplomatic Security Responses



United States Department of State

*Assistant Secretary of State
for Diplomatic Security*

Washington, D.C. 20520

SENSITIVE BUT UNCLASSIFIED
(UNCLASSIFIED when separated from attachments)

October 20, 2014

INFORMATION MEMO TO INSPECTOR GENERAL LINICK – OIG

FROM: DS – Gregory B. Starr  OCT 20 2014

SUBJECT: Response to Draft Audit of Department of State Information Security Program

Attached is the Bureau of Diplomatic Security's response to recommendations 17, 27, and 33 of the draft Audit of Department of State Information Security Program.

Attachments:
As stated.

SENSITIVE BUT UNCLASSIFIED
(UNCLASSIFIED when separated from attachments)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

DS Response to Draft Audit
Department of State Information Security Program
Report Number: AUD-XX-XX-XX, October 2014

Recommendations directed towards DS:

(U) **Recommendation 17:** OIG recommends the Bureau of Diplomatic Security revise the Foreign Affairs Manual for unclassified systems to [Redacted] (b) (5)

[Redacted]
[Redacted]
[Redacted]
[Redacted]

(SBU) **Management Response (10/14/14):** DS concurs with this recommendation and notes that the Department's policies [Redacted] (b) (5)

[Redacted]
[Redacted]
[Redacted] DS requests this recommendation be closed.

(U) **Recommendation 27:** OIG recommends that the Assistant Secretary for Diplomatic Security ensure that [Redacted] (b) (5) as defined within each Memorandum of Agreement.

(SBU) **Management Response (10/14/14):** DS concurs with this recommendation [Redacted] (b) (5) as defined within each Memorandum of Agreement.

(U) **Recommendation 33:** OIG recommends that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, update the Computer Incident Response Team Standard Operating Procedures to require the Computer Incident Response Team to notify the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Information Security, Program Applications Division, and the U.S. Computer Emergency Readiness Team in the event of a potential data spillage prior to closing a security incident ticket.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

(SBU) Management Response (10/14/14): DS concurs with this recommendation and will work to notify the offices listed above in the event of a potential data spillage prior to closing a security incident ticket.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED



**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

SENSITIVE BUT UNCLASSIFIED