UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

OFFICE OF INSPECTOR GENERAL

AUD-IT-13-03 Office of Audits November 2012

Audit of Department of State Information Security Program

~~**IMPORTANT NOTICE**: This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies 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.~~

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

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.

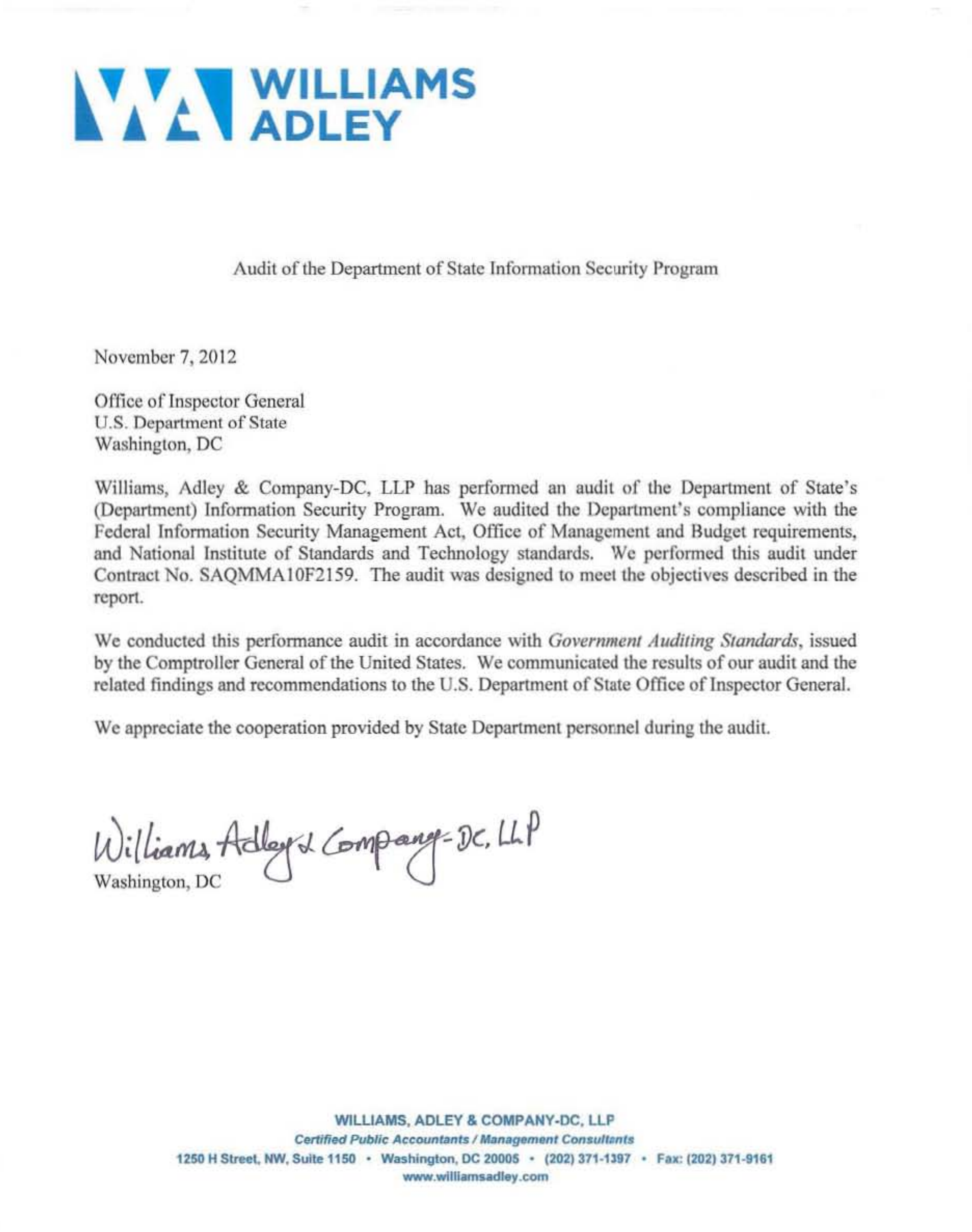
In accordance with the Federal Information Security Management Act of 2002 (FISMA), OIG performed an audit of the Department of State Information Security Program for FY 2012. To perform this audit, OIG contracted with the independent public accountant Williams, Adley & Company, LLP. The contract required that the independent public accountant perform its evaluation in accordance with guidance contained in the *Government Auditing Standards*, issued by the Comptroller General of the United States. The public accountant's report is included. The report is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The independent public accountant identified areas in which improvements could be made, including the risk management program, security configuration management, security awareness and role-based training, plans of actions and milestones, account and identity management, user provisioning process, continuous monitoring, remote access, continuity of operations program, information systems contingency planning, oversight of contractor systems, and capital planning.

OIG evaluated the nature, extent, and timing of Williams, Adley & Company's work; monitored progress throughout the evaluation; reviewed Williams, Adley & Company's supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with Williams, Adley & Company's findings, and the recommendations contained in the report were developed on the basis of the best knowledge available and were 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.

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

Harold W. Geisel
Deputy Inspector General



WILLIAMS
ADLEY

Audit of the Department of State Information Security Program

November 7, 2012

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

Williams, Adley & Company-DC, LLP has performed an audit of the Department of State'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 Office of Inspector General.

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

Williams Adley & Company-DC, LLP
Washington, DC

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1250 H Street, NW, Suite 1150 • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

Acronyms

AD	Active Directory
ATO	Authorization to Operate
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CM	Configuration Management
COOP	Continuity of Operations Plan
Department	Department of State
DHS	Department of Homeland Security
DS	Bureau of Diplomatic Security
DS/SI/CS	Diplomatic Security/Security Infrastructure/Office of Computer Security
eCPIC	electronic Capital Planning Investment Control
FAM	Foreign Affairs Manual
FISMA	Federal Information Security Management Act
GAGAS	Generally Accepted Government Auditing Standards
GO	Global OpenNet
HR/ER/WLD	Human Resources/Employee Relations/Work Life Division
IRM/IA	Bureau of Information Resource Management, Office of Information Assurance
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIP	Orientation and In Processing
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SP	Special Publication
SSA	Systems Security Authorization
SSR	Significant Security Responsibilities

Table of Contents

Section Page

Executive Summary

In accordance with the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG) contracted with Williams, Adley & Company, 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). Additionally, the results are designed to assist OIG in providing responses to FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics, dated March 6, 2012.

Overall, we found that the Department had implemented an information security program and had made progress during FY 2012, but we identified control weaknesses that significantly impact the information security program. If these control weaknesses were exploited, the Department could experience security breaches. The FY 2011 FISMA report[2] contained 19 recommendations intended to address security deficiencies, and the most significant of these deficiencies involved the Department's risk management strategy and security authorizations, security configuration management, Plans of Action and Milestones (POA&M), and the continuous monitoring program. Although we observed an increased level of effort to address the findings we presented in previous years, only four of the 19 recommendations from the prior audit report were remediated and confirmed during the audit period. The FY 2012 FISMA report contains 31 recommendations, with many repeat findings identified in the FY 2011 FISMA audit.

Collectively, the control weaknesses we identified in this audit, along with the weaknesses identified by OIG in the report *Audit of Department of State Access Controls for Major Applications*,[3] represent a significant deficiency, as defined by OMB Memorandum M-12-20,[4] to enterprise-wide security, including the Department's financial systems. The weakened security controls could adversely affect the confidentiality, integrity, and availability of information and information systems. A further compounding factor is that the Department had not fully taken corrective action to remediate all of the control weaknesses identified in the FY 2011 FISMA report.

The Department had taken action to resolve the continuous monitoring control weaknesses identified in the FY 2010 and FY 2011 FISMA reports on the Department's information security program by developing a formal continuous monitoring strategy to address framing and assessing risk, responding to risk, and monitoring risk, all of which are required by NIST Special Publication (SP) 800-39, "Managing Information Security Risk", March 2011. Although the strategy was finalized in August 2012, the control processes supporting the implementation of the continuous monitoring strategy had not been implemented. In addition, we found that subnets within the system's boundary residing on ClassNet were not included in

[1] Pub. L. No. 107-347, title III.

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

[3] *Audit of Department of State Access Controls for Major Applications* (AUD/IT-12-44, Sep. 2012).

[4] OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Oct. 2, 2012.

the periodic scans. Further, our review of the Department's remedial actions taken to resolve weaknesses identified in the FY 2010 and FY 2011 FISMA reports were not complete, and the following repeat deficiencies were found:

- The scanning tools do not assess Oracle, the Department's most common database management system, for configuration control weaknesses that could adversely impact application access controls.
- Scanning results for routers, firewalls, and Demilitarized Zone servers were not available in iPost;[5] therefore, the results were not used in risk scoring.
- Security configuration baselines for UNIX had not been developed and published. Without effective configuration management controls, sensitive data, systems, and hardware are exposed to loss of availability, integrity, and confidentiality.

Although we found that the Chief Information Officer was taking actions to address the prior year's weaknesses with the configuration management controls, the configuration management process continues to experience deficiencies in installing critical security patches within required timeframes.

The Department needs to improve account management processes in Active Directory[6] (AD) for OpenNet and ClassNet. From a population of 116,821 OpenNet AD user accounts, we identified 5,717 accounts that had not been used (never logged on); 529 accounts (user, service, and mailbox) with passwords set "not to expire;" 19,335 (user, service, and mailbox) accounts that had been set to not require passwords; and 6,269 users that had not logged into their accounts between 2005 and 2011. Using a risk-based approach, we identified random instances of the findings mentioned on the ClassNet AD as well. Upon notification of the findings noted, the Department implemented remedial actions to address the passwords set "not to expire" for OpenNet AD user accounts.

The Department made significant progress in disabling user accounts of terminated employees in a timely manner. From a population of 198 Foreign Service and Civil Service terminated employees (Domestic) and 186 Foreign Service and Civil Service terminated employees (Overseas) during FY 2012, we found only five user accounts that had not been disabled in a timely manner. In addition, we determined that the five user accounts for the terminated employees had last log-on dates after the dates the employees had been terminated. We commend the Department for taking immediate remediation efforts to disable these accounts and for performing analyses to determine whether any unauthorized activities had been performed on these accounts to resolve this finding. However, the Department's user provisioning process for creating new users' accounts was not in compliance with the

[5] iPost is a system that provides the ability to monitor outputs of the various network monitoring applications. It allows key personnel to monitor network, computer, and application resources; check for potential problems; initiate corrective actions; and gather performance, compliance, and security data for near real-time and historical reporting.

[6] Active Directory is a technology created by Microsoft that provides a variety of network services, such as identification and authentication, and directory access.

Department's *Foreign Affairs Manual* (FAM).[7] We found that Network Access Request Forms had not been received for four of a sample of 25 new user accounts created during FY 2012.

The Department's risk management program for information security needs improvement at the system level. We noted that system security plans for nine systems residing on the OpenNet did not comply with NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations." In addition, the security authorization process was not properly managed on the Department's primary general support systems for unclassified systems. These deficiencies weaken the Department's risk management framework and its ability to assess, respond to, and monitor information security risk.

The Department needs to improve its process and procedures for role-based security-related training. The Department was not tracking and documenting significant security responsibilities (SSR) training attendance, and it did not require role-based security-related training to be completed before authorizing access to the network. From a sample of 46 new employees hired during FY 2012 with SSR (that is, Chief of Mission, Deputy Assistant Secretary, Information Management Specialist, Information Technology Specialist, Office Director, and Security Engineering Officer), we found that all 46 employees had not taken the recommended[8] role-based security-related training course in the timeframe (that is, 6 months) as recommended in the Information Assurance Training Plan.

The Department's POA&M process had not been fully and effectively implemented, and the program remained noncompliant with OMB and Committee on National Security Systems requirements.[9] Although in August, 2012 the Department implemented a process to centrally manage, address, and resolve security weaknesses identified on systems residing on the ClassNet, the Department's bureaus had not implemented effective corrective actions to address the POA&M control weaknesses within systems residing on the OpenNet in a timely manner.

Remote access controls can be improved. The Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), has a process in place to authorize remote access administration using Remote Desktop Protocol via Global OpenNet (GO) for administrators, which contradicts 12 FAM 680, which prohibits the use of remote administration. We requested a sample of Remedy tickets to test authorization requests for key fobs/tokens, and Remedy tickets evidencing service requests could not be located for 19 of 25 new employees.

The Department's Continuity of Operations Program was not operating effectively and was not documented in accordance with NIST SP 800-34, Revision 1,[10] and Federal Continuity

[7] 12 FAM 622.1-2(b).

[8] The Department's Information Assurance Training Plan states: "This training is recommended upon title designation; individuals should complete training within 6 months of assuming the position. Training is recommended again once every 2 years for refresher purposes."

[9] OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," Oct. 2001; OMB Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," Aug. 2004; and "Committee on National Security Systems Policy No.22," Jan. 2012.

[10] NIST Special Publication 800-34, Rev. 1, "Contingency Planning Guide for Federal Information Systems," May 2010.

Directive 2.[11] The Department is required by NIST to have a collection of plans to prepare for response, continuity, recovery, and resumption of mission/business processes and information systems. Although contingency plans had been developed at the system level, the bureau level, and the national level, the Continuity of Operations Plan (COOP) for communications and the infrastructure had not been documented at the Department level (entity). In addition, an entity-wide Business Impact Analysis (BIA) had not been documented to facilitate the coordination of the recovery prioritizations of critical mission/business processes and services in the event of a disruption.

The Department had not implemented an effective oversight program of its contractor hosted systems and extensions, specifically, government extensions. Not all government extensions (older sites) had been documented (that is, an OpenNet extension that exists at the Broadcasting Board of Governors and authorization memoranda were not available or did not exist).

Information security was not fully integrated into the Department's Capital Planning and Investment Control process. IRM senior management needs to strengthen its oversight process of information technology (IT) investments. Our review of the business cases and OMB Exhibits 300[12] for the new enterprise-level IT investments (Application Services, Data Center Services/Hosting, and Deployment, Maintenance & Refresh) found that IRM exhibits were not complete because they were newly established Exhibits 300 this fiscal year. For example, we found that Investment level Acquisition Plan, Earned Value, Integrated Program Team Charter, Investment Charter, Project Charters (as appropriate), and Risk Management Plan were incomplete within electronic Capital Planning Investment Control (eCPIC).[13]

This report contains 31 recommendations to address security deficiencies identified in 14 reportable areas, and we believe the most significant security deficiencies are the findings related to risk management strategy and security authorizations (Finding A), security configuration management (Finding B), POA&Ms (Finding D), and the continuous monitoring program (Finding G).

In its November 7, 2012, response to the draft report (see Appendix I), the Department concurred with 24 recommendations, partially concurred with two recommendations, and did not concur with five recommendations.[14] Based on the response, OIG considers 27 recommendations resolved, pending further action, and four (4) recommendations unresolved. Based on the response OIG added a new recommendation and revised three other recommendations. This addition and revisions are noted in management's responses and OIG's analyses, which are presented after each recommendation.

[11] Federal Continuity Directive 2, "Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process," Feb. 2008.
[12] OMB Circular No A-11, Exhibit 300, "Capital Asset Plan and Business Case Summary."
[13] The Department of State's electronic Capital Planning Investment Control (eCPIC) portfolio management tool which is used for managing IT investments.
[14] In their response, management requested to divide the former Recommendation 15 into two recommendations. After the change, the final report now contains 31 recommendations.

We reviewed the Department's remedial actions taken to address the reported information security program control weaknesses identified in the FY 2011 FISMA report.[15] The status of each recommendation from the FY 2011 FISMA report is in Appendix B of this report.

Since FY 2011, the Department has taken the following actions to improve management controls:

- Developed automated process for the Foreign Service Institute's Cyber security tracking system to update the user's AD account expiration date immediately after the student completes the Cyber Security Awareness (PS800) training. This AD update extends the user's account expiration date by 368 days. If the user fails to retake the test in 368 days, the user's account expires and the user cannot access the system without manual intervention by an administrator.

- Developed System Security Plan templates that comply with NIST Special Publication 800-53, Revision 3.

- Developed and implemented procedures to distribute quarterly POA&M Grade Memorandums to the bureaus' and offices' senior management (executive director) as required by OMB Memorandum M-04-25.[16]

- Revised the IRM/IA Contingency Plan Test Review Checklist to address the following items:

    - Recovery and damage assessment procedures
    - Alternate recovery site details
    - Back-up procedures
    - Back-up test results for moderate- and high-impact systems

- Revised the Contingency Plan Policy to include an organization-defined frequency for backup testing.

- Revised the FAM to require system owners to report to IRM/IA on the test results and updates to the contingency plans.

- Established procedures to identify the total number of contractors who have access to the Department's systems.

- Developed procedures that ensure that the IRM's Directorate of Business Management and Planning track all obligations and expenditures for IT security investments.

- Developed procedures to provide a summary of non-major investments that make up the IT infrastructure and other major investments.

[15] AUD/IT-12-14, Nov. 2011.
[16] OMB Memorandum M-04-25, Aug. 2004.

- Developed procedures to include the Unique Project Identifier in the Department's POA&M database.

Background

Through FISMA, Congress recognized the importance of information security to the economic and national security interests of the United States. FISMA requires 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 information and information systems provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

FISMA assigns specific responsibilities to Federal agencies, NIST, OMB, and the Department of Homeland Security (DHS) in order to strengthen information system security. 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, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS.

On an annual basis, OMB, in coordination with DHS, provides guidance with reporting categories and questions for meeting the current year's reporting requirements.[17] OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

Objective

The objective of this audit was to perform an independent evaluation of the Department's Information Security Program and practices for FY 2012 and included testing the effectiveness of security controls for a subset of systems as required.

Results of Audit

Overall, we found that the Department had implemented an information security program, but we identified control weaknesses that significantly impacted the Information Security Program. If these control weaknesses were exploited, the Department could experience security breaches. Collectively, the control weaknesses we identified in this audit, along with the weaknesses identified by OIG in the report *Audit of Department of State Access Controls for Major Applications*,[18] represent a significant deficiency, as defined in OMB Memorandum M-

[17] OMB Memorandum M-12-20, Oct. 2, 2012.
[18] AUD/IT-12-44, Sep. 2012.

12-20,[19] to enterprise-wide security, including the Department's financial system. The weakened security controls could adversely affect the confidentiality, integrity, and availability of information and information systems. A further compounding factor is that the Department had not taken corrective action to remediate all of the control weaknesses identified in the FY 2010 and FY 2011 FISMA reports. To improve the Information Security Program and to bring the program into compliance with FISMA, OMB, and NIST requirements, the Department needs to address the control weaknesses described.

Finding A. Continuous Monitoring Program Needs To Be Improved

Although the Information Security Steering Committee published, in August 2012, a continuous monitoring and risk management framework strategy that addressed framing risk, assessing risk, responding to risk, and monitoring risk, the control processes supporting the implementation of the continuous monitoring strategy had not been fully implemented. In addition, the Department's remedial actions taken to resolve weaknesses identified in the FY 2010 and FY 2011 FISMA reports were not complete. Further, not all Windows servers (seven of the eight systems on ClassNet selected for testing) were reporting security posture information in iPost.

The continuous monitoring and risk management framework strategy did not address how the Department planned to monitor the security posture of the components described, as the components were not configured to report information into iPost (primary continuous monitoring tool used by the Department). The components are as follows:

- Oracle (the Department's most common database system)
- UNIX security configurations
- Network components (for example, routers and switches)
- Demilitarized Zone servers

The repeat conditions at the system scanning level occurred because the Bureau of Diplomatic Security (DS) and IRM were still working on a solution; DS and IRM agreed that the conditions still existed. The lack of an enterprise-wide continuous monitoring strategy and security weaknesses of relevant IT components, such as databases and network devices, were not included in iPost.

NIST SP 800-37[20] and NIST SP 800-53 CA-7[21] require that an organization-defined continuous monitoring strategy be implemented.

The causes for the conditions were as follows: (1) the Department had not finalized an enterprise-wide continuous monitoring program strategy to assist system owners in evaluating various control deficiencies and (2) Diplomatic Security/Security Infrastructure Directorate

[19] OMB Memorandum M-12-20, Oct. 2, 2012.

[20] NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," Feb. 2010.

[21] NIST SP 800-53, Rev. 3, CA-7, "Continuous Monitoring."

Office of Computer Security (DS/SI/CS) scheduled periodic vulnerability and compliance scans by subnet but did not include all of the subnets in the Foundstone[22] configuration.

Not having a robust continuous monitoring program prevents the Department from understanding the security state of the information system over time. It also prevents the Department from effectively monitoring a highly dynamic network environment with changing threats, vulnerabilities, technologies, and missions/business functions.

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

Management Response: The Department concurred with the recommendation, stating that it had provided the OIG with a document "specific to" Finding A in the reports. The Department further stated that this document would be presented to the "Information Security Steering Committee for review and approval" within the next 6 months.

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that the Department has developed and implemented a continuous monitoring strategy.

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

Management Response: The Department concurred with the recommendation, stating that it "will hold discussions and develop documentation identifying methods for monitoring the security posture for non-Windows operating systems, databases, firewalls, routers, and switches."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing methods to monitor the security posture for non-Windows operating systems, databases, firewalls, routers, and switches.

Finding B. End-to-End Configuration Management Process Needs Improvement

Although the Department had taken actions to address the prior year noted weaknesses with the configuration management controls, the weakness within configuration management

[22] A tool created by McAfee that performs vulnerability scans and generates reports with the results.

process still existed. We identified the following deficiencies as a result of vulnerability scanning analysis on selected systems (see Appendix D):

1. The bureaus were not installing critical security patches in a timely manner on 14 of 15 systems residing on OpenNet, including the general support system selected for testing. (Details are in Appendix C.)

2. Systems were configured to allow unauthorized users access to system resources via anonymous logins and passwords, default credentials, and unsecured access points. (Details are in Appendix C.)

The FAM[23] requires the installation of critical patches on workstations and servers at an installation rate of 100 percent and 90 percent for non-critical patches. Also, the FAM[24] requires that unique user accounts be used and passwords be changed

Responsibility for the implementation of configuration management controls for the systems, operating systems, databases, and network is decentralized; it is fragmented among the various system owners, database administrators, and network administrators. Additionally, the Information System Security Officers had not established and implemented a reporting process to verify that the responsible groups had implemented the security configuration patches and software updates identified by DS and IRM. To correct these weaknesses, IRM/Enterprise Network Management, was implementing the end-to-end configuration management initiative, which includes a standard operating environment to support development of strong configuration management plans for the computing environments commonly used throughout the Department.

Configuration management controls allow agencies to improve system performance, decrease operating costs, increase security, and ensure public confidence in the confidentiality, integrity, and availability of Government information. Without effective configuration management controls, the Department increases the risks that Department sensitive data, systems, and hardware will be exposed to loss of integrity and confidentiality. Additionally, the Department increases the risks that known security weaknesses will be exploited by individuals to perform unauthorized activities. The Department’s decentralized patch management and configuration management processes and procedures do not ensure that all system and operating system security residing on the network will be properly patched to reduce the security exposure to other bureaus and system owners in a timely manner.

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

Management Response: The Department stated that it “believes . . . the current configuration management controls for the Standard Operating Environment (SOE) platform have been fully documented and are operating effectively and efficiently” and

[23] 5 FAM 1067.3 (b).
[24] 12 FAM 622.1-3 (a).

that "further documentation of key components may be useful," concluding that "such actions will be taken to meet the intent of this recommendation."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that the Cyber Security Architecture has been finalized and implemented.

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

Management Response: The Department concurred with the recommendation, stating that it "is continually improving processes to patch servers within their system boundary in a timely manner" and that it will generate updates "periodically via email or cable to ensure that there is proper notification within the Department."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing how the Department is improving its processes to patch servers in a timely manner.

Finding C. Standard Configuration Baselines for UNIX Need To Be Developed

Although the Security Configuration Management Branch (SCM) had developed and implemented security configuration baselines for Windows operating systems, database, network devices, and Web applications, SCM had not developed and published the security configuration baselines for UNIX.

The FAM[25] states that Diplomatic Security/Security Infrastructure/Office of Computer Security (DS/SI/CS) is responsible for the development and updates of security configuration standards of specific IT products that are used throughout the Department.

Because of the limited number of UNIX servers in use, SCM had not assigned the resources needed to develop the security configuration baselines for UNIX.

Configuration management controls allow agencies to improve system performance, decrease operating costs, increase security, and ensure public confidence in the confidentiality, integrity, and availability of Government information. Without effective configuration management controls, the Department increases the risk that Department sensitive data, systems, and hardware are exposed to loss of availability, integrity, and confidentiality.

[25] 1 FAM 262.6-2(1)(2)(3)(6)(7)(8)(9)(17)(18)(20) and (21).

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

Management Response: The Department concurred with the recommendation, stating that it "will review, develop and publish the security configuration baselines for UNIX, as needed, in accordance with 12 FAM."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves the security configuration baselines for UNIX in accordance with the FAM.

Finding D. Periodic Vulnerability and Compliance Scans Process and Capabilities Need Improvement

Although the Department had developed and implemented periodic vulnerability and compliance scans using Foundstone Enterprise and Policy Auditor[26] on Windows servers to address prior audit recommendations, we determined that the following weaknesses still existed:

- Capabilities to periodically scan the following components for compliance and vulnerabilities were not implemented:
  - Oracle databases
  - Applications
  - Network devices (for example, routers and switches)
  - UNIX operating systems
  - Demilitarized Zone servers
- Foundstone is currently configured to scan by subnet; however, during the independent vulnerability scan, we determined that seven of eight sampled systems on ClassNet (including the ClassNet general support system) had subnets within the system's boundary that were not included in the periodic scans. DS/SI/CS had taken action to include the identified subnets in the Foundstone configuration for periodic scanning.

The FAM[27] states that DS/SI/CS is responsible for conducting continuous and directed network- or application-specific vulnerability assessment testing, independent penetration testing, and intelligence monitoring to identify specific risks to those systems and develops risk mitigation strategies to protect the Department's IT infrastructure.

Based on interviews with key personnel and review of documents supporting the processes and procedures, we identified the following causes for the weaknesses:

[26] A tool created by McAfee that performs compliance scans and generates reports with the results.
[27] 1 FAM 262.6-2(20).

- Vulnerability and Compliance Scanning Tools had not been implemented to perform periodic vulnerability and compliance scans on Oracle databases, Applications, Network devices (for example, routers and switches), and UNIX operating systems.
- Discovery scans were not performed on a periodic basis to identity new components added to the network.
- DS did not have the administrative credentials needed for Demilitarized Zone servers to perform periodic scanning.

Configuration management controls allow the Department to improve system performance, decrease operating costs, increase security, and ensure public confidence in the confidentiality, integrity, and availability of the Department's information. Without effective configuration management controls, the Department increases the risks that Department sensitive data, systems, and hardware will be exposed to loss of availability, integrity, and confidentiality.

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

Management Response: The Department concurred with the recommendation, stating that IRM/IA and DS had "previously identified these areas as requiring tools"; that the process of identifying and acquiring the appropriate tools "will continue"; and that once the tools have been acquired, they "will be incorporated into the Department's scanning program."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that the vulnerability and compliance tools specified have been incorporated into the Department's scanning program.

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

Management Response: The Department concurred with the recommendation, stating that IRM/IA and DS had "identified these areas for improvement in the current scanning capability" and were "working collaboratively to establish this capability."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that the subnets and

Demilitarized Zone servers are included in the Foundstone configuration for periodic scanning.

Finding E. Account Management Processes in Active Directory Need To Be Improved

The Department needs to improve account management processes in AD for OpenNet and ClassNet. As first identified in the FY 2010 audit, OIG reported deficiencies in account management, and we found that account management deficiencies still existed within AD for OpenNet and ClassNet.

From a population of 116,821 active OpenNet AD user accounts (see Appendix D), we identified the following deficiencies:

- 5,717 accounts created from 2002 to 2011 had not been used (never logged on). The FAM[28] requires user privileges to be reviewed annually to verify that privileges are still appropriate.

- 6,269 active user accounts had not logged on within the last 5 months. These user accounts had last logon dates between 2005 and 2011. The FAM[29] requires user privileges to be reviewed annually to verify that privileges are still appropriate.

From a population of 121,702 active OpenNet AD accounts, including users, service, and mailbox accounts, we identified the following deficiencies:

- 529 accounts had passwords set not to expire. The FAM[30] requires passwords to be changed at least every 60 days.

- 19,335 accounts had been set to not require passwords. The FAM[31] requires the removal of non-permanent (that is, visitor and training) user accounts and passwords.

AD for ClassNet had similar deficiencies. Using a risk-based audit approach, we identified instances of the same deficiencies on ClassNet as on the OpenNet AD; therefore, we did not perform detailed analyses on the ClassNet AD.

The Department uses a decentralized and fragmented process to manage AD. Specifically, each bureau and post is responsible for user account management (adding new users and removing or modifying existing users' accounts). System Administrators identified a bit flag within AD that was enabled to permit setting certain accounts to "not require a password."

Bureaus and posts that choose not to comply with the Department's security standards jeopardize the safety and security of the entire network. Inadequate account and identity

[28] 12 FAM 622.1-3(i).
[29] Ibid.
[30] 12 FAM 622.1-3(j).
[31] 12 FAM 622.1-3 (e) and (i).

management controls increase the risk that temporary and active accounts may used by unauthorized Department and contractor personnel to perform unauthorized activities.

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

Management Response: The Department concurred with the part of the recommendation for accounts that do not require a password, stating that IRM receives automatic [AD] "alerts when any account is created that does not require a password," which "results in an immediate intervening response by IRM/IA."

The Department did not concur with the part of the recommendation for accounts that have not been used for 90 days, stating that this is a "separate issue" and recommended that this issue "be addressed" in Recommendation 9.

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that accounts that do not require a password are removed or locked.

Based on the Department's response, Recommendation 8 has been modified to remove reference to accounts that have not been used for 90 days.

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

Management Response: The Department concurred with the recommendation, stating it "has initiated actions in coordination with [DS] to revise the 12 FAM to include language that provides authority to the [CIO] to review and identify accounts not used within the past 90 days and to de-activate such accounts and require the bureaus and posts to recertify the user account prior to re-activating the account."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that 12 FAM has been revised and that the accounts not used within the past 90 days have been de-activated and recertifed by bureaus and posts.

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

Management Response: The Department did not concur with the recommendation and "suggest[ed] that the recommendation be closed. The Department stated that its "actions are compliant with the applicable FAM" in that it "requires that user accounts be configured to require an account password."

OIG Analysis: OIG considers the recommendation unresolved and open because there are accounts with passwords on the network that are set to not expire. However, OIG modified the recommendation to require that passwords to be changed every 60 days in accordance with the FAM. The recommendation can be closed when OIG reviews and approves documentation showing that the Department has configured its accounts so that passwords are changed every 60 days.

Finding F. The User Provisioning Process for Creating, Modifying, and Disabling Users' Accounts Requires Significant Improvement

The Department had made significant progress in improving the user provisioning process; however, we found the following:

- From a population of 198 Foreign Service and Civil Service terminated employees (Domestic) and 186 Foreign Service and Civil Service terminated employees (Overseas), we identified user accounts for six terminated employees in the OpenNet AD accounts that were not disabled and found that the user accounts had last logon dates after the date of the employees' termination. Upon notification, the Department disabled and removed these accounts from AD and conducted analyses to determine whether any unauthorized activities had been performed on these accounts.

- Of the 25 samples selected for new user testing, we determined the following:
    - Four new user account request forms could not be located:
        - None of three new users in Kabul, Afghanistan.
        - One of 11 new users at the Foreign Service Institute.
    - Expiration dates were not set for either of the two users in the Office of the Secretary.

The FAM[32] requires the data center manager and the system manager, in conjunction with the Information System Security Officer, to revoke user access privileges for terminated or transferred personnel. Personnel officers must notify the data center manager, the system manager, and the Information System Security Officer immediately of any employee or contractor with access to the system whose employment is being terminated for any reason. The FAM[33] requires supervisors to complete a system access request form for each staff member who requires automated information system access. The Department's procedure[34] states that expiration dates need to be set in AD to ensure that accounts lock after one year if the users do not complete the annual Cyber Security Awareness Training.

[32] 12 FAM 621.3-3.
[33] 12 FAM 622.1-2(b).
[34] Department of State Global Address List (GAL) and Active Directory Standardization Guide, dated Feb. 24, 2012.

The user provisioning weaknesses occurred because the bureaus were not disabling accounts in a timely manner. Furthermore, in lieu of the Department of State Logon Request form, users in Afghanistan send emails via the Office of Orientation and In Processing (OIP) directly to IRM/Operations/Customer Service Office/Desktop Support Division IT Mart to create accounts for users in Afghanistan. Although all OIP Afghanistan computer account requests are supposed to be entered into SharePoint by Program Assistants, OIP could not locate the emails initiating the request for these accounts. The Foreign Service Institute could not locate the new user access request form for the new user selected for testing. Because of the nature of the work performed by members in the Office of the Secretary, AD accounts are not set to expire.

Ineffective user provisioning program procedures and practices increase the Department's risk of unauthorized access, use, disclosure, disruption, modification, or destruction of information. These control weaknesses increase the potential for unauthorized activities to occur without being detected timely and to adversely affect the confidentiality, integrity, and availability of the data on the network.

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

Management Response: The Department concurred with the recommendation, stating that "corrective actions have been taken" by IRM "to disable and remove the accounts" from AD and that analyses are conducted to determine where "any unauthorized activities had been performed on these accounts."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves the documentation showing that the accounts have been disabled and removed and an analysis of unauthorized activity has been performed.

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

Management Response: The Department concurred with the recommendation, stating that it "will initiate a policy that requires periodic review ensuring that" user accounts for employees who have been terminated "are disabled in a timely manner."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that user accounts of terminated employees have been disabled in a timely manner.

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

Management Response: The Department concurred with the recommendation, stating that "a process will be developed and implemented ensuring that new users in overseas locations complete the Department of State Logon Request form."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that the Department has developed and implemented a process ensuring that new users in overseas locations complete the form.

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

Management Response: The Department concurred with the recommendation, stating that it "will develop and update procedures on account management for new users in overseas locations."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing the procedures on account management for new users in overseas locations.

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

Management Response: The Department generally did not concur with the recommendation "as stated" and suggested that the recommendation in the draft report "be revised to separately address" two issues.

Based on the response, OIG revised Recommendation 15 in the draft report to become Recommendations 15 and 16 in this final report.

The Department concurred with the new recommendation, stating that the Office of the Secretary "already has a procedure in place to set expiration dates manually for user accounts in [AD], a waiver to the automatic expiration policy will allow [the Office of the Secretary] to continue monitoring the accounts and modifying them manually to ensure no interruption in service and compliance with the relevant portions of the DS Security policy."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves the final policy on exemptions/waivers from the standard of setting expiration dates for Office of the Secretary user accounts in AD.

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

Management Response: The Department concurred with the new Recommendation 16 in this report, stating that the Office of the Secretary "will ensure" all employees receive cyber security awareness training.

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approved documentation showing that Office of the Secretary users are completing the required Cyber Security Awareness Training annually.

Finding G. Risk Management Framework Needs Improvement

Although the Department had made progress to address prior year findings, weaknesses still existed within the risk management process, particularly the security controls assessments. The following discrepancies were noted with the controls:

- System security plans did not comply with NIST SP 800-53, Revision 3, for nine of 16 systems selected for testing residing on the OpenNet. (Details are in Appendix F.)

- The OpenNet general support system authorization to operate (ATO) expired in August 2010, and the security controls assessment will not be completed until FY 2013.

OMB[35] states that agencies' legacy information systems are expected to be in compliance with NIST standards and guidelines within a year of the publication date unless otherwise directed by OMB. Also, OMB Circular A-130, Appendix III, requires that general support and major systems' security controls be reviewed at least every 3 years or when a major change occurs.

The Department did not publish the updated Certification & Accreditation (C&A) Toolkit and required templates until December 2011, even though NIST SP 800-53, Revision 3, was finalized in August 2009. The updates addressed the NIST SP 800-53, Revision 3, requirements. Also, in February 2010, NIST SP 800-37, Revision 1, was released and introduced changes to the security authorization process. As such, the Chief Information Officer extended the OpenNet ATO through August 2011 in an effort to develop continuous security authorization by leveraging iPost capabilities to increase security while reducing costs. The ATO was then extended twice after August 2011, from March 2012 to December 2012. The decision to conduct the full security authorization was not made until February 2012.

Systems where assessments had not performed in accordance with NIST SP 800-53, Revision 3, might not possess the security controls needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational

[35] OMB Memorandum M-12-20, Oct. 2, 2012.

missions and business functions. Systems residing on OpenNet inherit controls from the OpenNet general support system. Since the OpenNet ATO had expired, Department officials might not have the desired or required level of assurance that the inherited security controls, as implemented, were effective.

> **Recommendation 17.** We recommend that the Chief Information Office, in coordination with Information Resource Management/Information Assurance, continue to review the security authorization and annual assessments to ensure that Information System Owner, Information System Security Officer, and Security Control Assessor for all Federal Information Security Management Act reportable systems use the published Certification & Accreditation Toolkit templates during the annual controls assessment to assess the required National Institute of Standards and Technology Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," controls applicable and update the System Security Plan accordingly.
>
> **Management Response:** The Department did not concur with the recommendation, stating that it "asserts that the referenced practices and controls are being fully implemented."
>
> **OIG Analysis:** OIG considers the recommendation unresolved and open. OIG concurs with the Department that the Department has implemented practices to ensure compliance with NIST SP 800-53, Revision 3. However, the Department needs to make progress regarding the security authorization process, since OIG identified nine of 25 system security plans that did not comply with the publication and the OpenNet general support system authorization to operate (ATO) expired in August 2010.
>
> This recommendation can be closed when OIG reviews and approves documentation showing the Department is complying with NIST SP 800-53, Revision 3, as it pertains to the applicable controls.
>
> **Recommendation 18.** We recommend that the Chief Information Officer continue to track the progress of the full authorization of the OpenNet general support system.
>
> **Management Response:** The Department concurred with the recommendation, stating that the Chief Information Officer, IRM/IA, and IRM's Office of Operations are all "expending significant time and resources to ensure [that] progress of the full authorization of the OpenNet general support system is occurring." The Department further stated, "Ongoing progress reports are submitted to the Chief Information Officer."
>
> **OIG Analysis:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing the full authorization of the OpenNet general support system.

Finding H. Information Security Training Requirements Were Not Enforced

Although DS/SI/CS had made progress with the Information Security Training Program in FY 2012 to resolve the deficiencies identified in FY 2011, security control weaknesses still existed.

We selected a sample of six SSRs identified in the Information Assurance Training Plan and identified 46 new employees who were assigned those responsibilities. We found that all 46 of the new employees with SSR had not taken the Department's recommended role-based security-related training courses as of May 22, 2012.

In addition, the FY 2011 evaluation found that the Department had established controls to identify SSR positions and required role-based security-related training in the Information Assurance Training Plan; however, the Department was not tracking and documenting SSR training attendance.

IRM/IA and DS/SI/CS rely on employees to track their own role-based training. The Department had not established procedures to track and document compliance with SSR training attendance. Also, the IA Training Plan did not mandate when role-based training was to be completed.

The Information Assurance Training Plan recommends that personnel with significant security responsibilities attend their designated role-based security-related courses within 6 months of title designation and every 3 years thereafter for refresher training. Also, NIST SP 800-53, Revision 3, requires the organization to provide role-based security-related training (i) before authorizing access to the system or performing assigned duties, (ii) when required by system changes, and (iii) on a periodic basis (defined by the organization) thereafter.

Employees and contractors who are in positions that are responsible for the security of the organization's information and information systems need to be properly trained on how to protect classified information. Without proper training, these employees and contractors could create a risk for the Department because they may cause vulnerabilities or security breaches, which increases the risk of a computer security incident that could result in a security breach or the loss of sensitive data.

> **Recommendation 19.** We recommend that the Chief Information Officer, in coordination with Information Resource Management/Information Assurance and Office of Computer Security (Diplomatic Security/Systems Integrity/Civil Service), update the Information Assurance Training Plan to require newly hired and current employees and contractors who are in positions that are responsible for the security of the organization's information and information systems complete role-based security-related training before authorizing access to the system or performing assigned duties and periodically thereafter (for example, annually).
>
> **Management Response:** The Department concurred with the recommendation, stating that IRM/IA and DS/SI/CS "have initiated actions to update the Information Assurance

Training Plan and develop additional language on newly hired and current employees, contractors, including role-based security-related training."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves the finalized Information Assurance Training Plan and additional language on newly hired and current employees, contractors, including role-based security-related training.

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

Management Response: The Department concurred with the recommendation, stating that IRM/IA and DS/SI/CS "have initiated actions to update the Information Assurance Training Plan and develop additional language on newly hired and current employees, contractors, including role-based security-related training."

OIG Analysis: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves the finalized Information Assurance Training Plan and additional language on newly hired and current employees, contractors, including role-based security-related training.

Finding I. Plans of Action and Milestones Are Not Effective

Various bureaus and offices, including the Bureau of Consular Affairs, IRM, the Bureau of Human Resources, the Office of Medical Services, the Bureau of Arms Control, Verification and Compliance, the Office of the Secretary, and the Bureau of Overseas Buildings Operations, were not compliant with the Department's POA&M process.[36]

1. For systems residing on OpenNet:
    a. 58 percent of the open POA&Ms (that is, 2,006 of 3,458) control weaknesses were overdue by more than 90 days. For example,
        i. 235 open POA&Ms were over 2 years old.
        ii. Bureau of Consular Affairs alone had 927 POA&Ms that were overdue.
    b. There were 515 POA&Ms that were remediated from December 2009 to March 2012, but verification had not been performed by the Bureau Executive, Information System Owner, or designee to close out those POA&Ms.
    c. POA&M fields were not being consistently updated as required:
        i. For 2,858 POA&Ms (83 percent), resources were not budgeted.

[36] Department of State POA&M Toolkit.

2. For systems residing on ClassNet, 36 percent of open actions (that is, 365 of 1,006) control weaknesses were overdue by more than 290 days. For example,
    a. 39 open POA&Ms were over 2 years old.
    b. The Office of the Secretary and IRM each had more than 100 open POA&Ms that were overdue.

POA&M is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.[37] The POA&M should also identify other non-funding obstacles and challenges to resolving the weakness. POA&Ms must include all security weaknesses found during any other review done by, for, or on behalf of the agency. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.[38]

Information System Owner or the Executive Director (or Designee) for a bureau is not taking the following actions:

- Providing the resources needed to close actions.
- Taking management action, as needed, to ensure work is completed on schedule.
- Reviewing status (at least quarterly) by looking at relevant bureau POA&M tracking database reports (after the database is updated for the quarter).

IRM/IA distributes a quarterly POA&M grading memorandum for OpenNet systems to Bureau Executives. However, there is no requirement in the memorandum for responses to be provided to IRM/IA as to what actions the bureaus intend to implement to ensure the outstanding POA&Ms are closed out in a timely manner. At the conclusion of our fieldwork, IRM/IA had updated the memorandum with the response requirement and stated that it would be implementing this requirement in Quarter 4 of FY 2012 and that IRM/IA had been working with its counterparts within each bureau to reduce the number of outstanding POA&Ms.

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

[37] OMB Memorandum M-02-01, Oct. 17, 2001.
[38] OMB Memorandum M-04-25, Aug. 2004.

Management Response: The Department concurred with the recommendation, stating that IRM/IA and DS/SI/CS had "taken action to include in the recently issued . . . POA&M grading memos, instructions for the [b]ureaus to respond within 10 business days on their plans to remediate and close open POA&M entries." The Department further stated, "A report of the responders has been sent to the Chief Information Security Officer for further action and escalation."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing the instructions for the bureaus to respond on their plans to remediate and close open POA&M entries and documentation showing that report of the responders has been sent to the Chief Information Security Officer for further action and escalation.

Finding J. Remote Access Policies and Procedures Need Improvement

Remote access controls can be improved. IRM/IA has a process in place to authorize remote access administration using Remote Desktop Protocol via Global OpenNet (GO) for administrators, which contradicts 12 FAM 680, which prohibits the use of remote administration. 12 FAM 680 is outdated because it does not reflect business requirements for remote administration. The FAM[39] states that remote access is only authorized for user-level privileges; remote administration/maintenance is prohibited. Remote access for system administration needs to be granted because of the time zone differences in the constituencies the Department of State serves overseas.

Additionally, supporting documentation was not provided and we were not able to test authorization requests for key fobs/tokens. Remedy tickets evidencing service requests for key fobs/tokens for remote access could not be located for 19 of 25 new employees selected for testing. The respective bureaus did not submit service requests for key fobs/tokens to the IT Service Center, and as such, Remedy tickets could not be provided.

Lack of supervisory approval for remote access increases the Department's risk for an insider to gain unauthorized remote access to the Department's systems. This would enable the performance of unauthorized activities, such as modifying Department sensitive data, improperly releasing sensitive data, or intentionally destroying sensitive data.

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

Management Response: The Department did not concur with this recommendation, stating that the "current 12 FAM policy is clear and unambiguous on this topic." The

[39] 12 FAM 682.2-3.

Department further stated that IRM/IA's policy on the exemption process "provides that each exemption is fully documented and available for review."

OIG Analysis: OIG considers the recommendation unresolved and open. The FAM, 12 FAM 680, prohibits remote administration/maintenance, which conflicts with IRM/IA's policy on the exemption process.

This recommendation can be closed when OIG reviews and approved documentation showing that 12 FAM 680 has been updated to reflect the current process of granting administrators the capabilities for remote administration.

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

Management Response: The Department did not concur with the recommendation, stating that it "is compliant with [OMB's] requirement to track fobs/tokens to identify the personnel who participate in telework opportunities."

OIG Analysis: OIG considers this recommendation unresolved and open. The correlation between users with key fobs/token and personnel who participate in telework opportunities could not be determined. Service requests to the Information Technology Service Center for key fobs/tokens are initiated by Telework Agreement Approvals. From a sample of 25 users with key fobs/tokens, service requests for 19 users could not be provided.

This recommendation can be closed when OIG reviews and approves the Department's actions for improving the process for submitting service requests as specified.

Finding K. The Continuity of Operations Program Needs To Be Improved

Contingency plans have been developed at the system level, bureau level, and even the national level; however, the COOP for communications and the infrastructure were not documented at the Department level (entity). Also, an entity-wide BIA had not been documented to ensure the coordination of the recovery prioritizations of critical mission/business processes and services in the event of a disruption at the Enterprise Service Operation Center.

According to NIST SP 800-34, Revision 1, Federal Continuity Directive 2 provides a required template for a process-based BIA to identify the information systems that support COOP functions for the process-based BIA.

IRM is focused on the Emergency Action Plan, which ensures the safety of Department employees and bureau readiness, instead of the COOP, which contributes to the continuation of communications and the network for the entire Department. The Department had not modified the FAM to provide guidance and direction for the COOP development. During fieldwork of the audit, the Department was in the process of developing the BIA.

Without a BIA, the Department increases the risks that it will not recover primary mission-critical functions based on established recovery priorities. Critical mission/business processes and services will not be restored in the required timeframe in the event of a disruption.

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

Management Response: The Department concurred with the recommendation, stating that it "is currently working with DS to update the FAM."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that the portion of the FAM described has been updated.

Recommendation 25. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, perform an entity-wide Business Impact Analysis and develop a strategy to prioritize recovery of the critical assets within the Department and align the Business Impact Analysis of the primary mission-critical functions with Information Resource Management's Maximum Tolerable Downtime for the network.

Management Response: The Department concurred with the recommendation, stating that it "has taken corrective actions to develop a Business Impact Analysis."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that the entity-wide Business Impact Analysis has been finalized.

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

Management Response: The Department concurred with the recommendation, stating that the Chief Information Officer and IRM/IA were developing a Continuity of Operations Plan for communications that "complies with the applicable NIST guidance and will include the standard elements of a Continuity of Operations Plan."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing the finalized Continuity of Operations Plan for communications that complies with the applicable NIST guidance and includes the standard elements of a Continuity of Operations Plan.

Finding L. Information System Contingency Plans Need To Be Improved

Although the Department had made some progress in addressing the prior years' audit findings for the information system contingency plans, weaknesses still existed as follows:

- Alternate processing site details were not documented in the Contingency Plans for five of 16 systems residing on OpenNet and four of 10 systems residing on ClassNet that we selected for testing. (Details are in Appendix H.)
- Annual Contingency Plan tests were not performed for FY 2012 on two of 16 systems residing on OpenNet and four of 10 systems residing on ClassNet that we selected for testing. (Details are in Appendix G.)

NIST [40] requires agencies to identify an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards and to conduct annual tests of backup information to verify media reliability and information integrity.

NIST[41] requires an organization to perform tests and/or exercises of the contingency plan for the information system. In addition, the IRM/IA Contingency Planning Toolkit requires testing contingency plans on an annual basis.

The Department had a decentralized process for developing and implementing a system's contingency plan and had not developed the processes to ensure bureaus comply with IRM/IA Contingency Planning Toolkit to perform annual contingency plan tests and provide required documentation to IRM/IA.

By inadequately documenting the contingency plan, the Department increases the risk of failing to maintain operations or to recover mission-critical systems in a timely manner in the event of a signification disruption in operations. As a result, the Department increases its risk of failing to meet its primary mission-critical functions and continue normal business activities of service to the public and abroad.

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

Management Response: The Department concurred with the recommendation, stating that IRM/IA had taken c"orrective actions to incorporate checklists questions regarding

[40] NIST SP 800-53, Rev. 3, CP-7, "Alternate Processing Site."
[41] NIST SP 800-53, Rev. 3, CP-4, "Contingency Plan Testing and Exercises."

the existence of alternate site locations, as well as procedures for accessing these facilities."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing the finalized checklist questions regarding the existence of alternate site locations, as well as procedures for accessing these facilities.

Finding M. Oversight of Contractor Systems and Extensions Needs Improvement

Efforts to strengthen the Department's oversight of contractor/government system and extension program had been made; however, weaknesses still existed as follows:

- The Gateway to State and Foreign Service Officer Test systems, each identified as Contractor Company Hosted Systems within the IT Asset Baseline system, had system security plans that were not compliant with NIST SP 800-53, Revision 3, requirements.

- Not all government extensions (older sites) had been documented (that is, an OpenNet extension that exists at the Broadcasting Board of Governors and authorization memoranda were not available or did not exist).

OMB[42] requires agencies to be fully responsible and accountable for ensuring contractor systems are compliant with FISMA. Agencies must ensure identical, not "equivalent," security procedures.

IRM did not publish the updated C&A Toolkit until December 2011, even though NIST SP 800-53, Revision 3, was finalized in August 2009. OMB requires compliance with new special publications within a year unless otherwise stated. For the OpenNet extensions, IRM only tracked extensions at contractor sites and did not consider other Government agencies as a contractor.

Without adequate oversight of contractor-hosted systems, government extensions, and contractor extensions, the Department cannot ensure that the contractor's information security controls are compliant with FISMA, OMB requirements, and NIST standards. Further, the Department increases the risk to the Department data for unauthorized access, use, disclosure, disruption, modification, or destruction that is collected, processed, and maintained by contractor-hosted systems, government extensions, and contractor extensions.

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

Management Response: The Department concurred with the recommendation, stating that it "will continue to ensure compliance with established schedules."

[42] OMB Memorandum M-12-20, Oct. 2, 2012.

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing the Department's progress in complying with established schedules.

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

Management Response: The Department concurred with the recommendation, stating that it "will continue to conduct the normal processing reviews to ensure compliance with NIST SP 800-53 rev. 3 and subsequent revisions."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing the contractor-hosted systems' compliance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

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

Management Response: The Department did not concur with the recommendation, stating that it "asserts the current process in practice are effective, periodic review of the process will be conducted and updates made when needed."

OIG Analysis: OIG modified the recommendation from the draft report to "continue" to implement procedures to coordinate security activities for tracking all extensions, since the procedures were recently implemented during the audit (FY2012).

OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing the tracking of all OpenNet and ClassNet extensions (that is, contractor sites and other government agencies via iPost).

Finding N. Security Capital Planning Requires Improvement

Our review of the business cases and OMB Exhibits 300 for the new enterprise level IT investments (Application Services, Data Center Services/Hosting, and Deployment, Maintenance & Refresh) found that the IRM exhibits were not complete because the IT investments were newly established Exhibits 300 this fiscal year. Specifically, we found that Investment level

Acquisition Plan, Earned Value, Integrated Program Team Charter, Investment Charter, Project Charters (as appropriate), and Risk Management Plan were incomplete within electronic Capital Planning Investment Control (eCPIC).[43] However, the IRM Portfolio Management Division was working with the respective Program Managers to ensure that these investments had up-to-date and complete eCPIC reporting for the next submission to OMB.

OMB[44] states that agencies must develop and maintain the following documents, all of which may be requested, and are subject to delivery within 10 business days: Investment Level Alternative Analysis, Investment Level Acquisition Plan, Earned Value Reports on large projects, Integrated Program Team Charter, Investment Charter; Project Charters (as appropriate), and Risk Management Plan.

According to officials in the Portfolio Management Division, the newly assigned IRM Service Line Program Manager did not have the time to gain the appropriate level of guidance, training, and understanding of the new eCPIC requirements to ensure complete Exhibits 300 and accurate identification and reporting of the resources required to protect the information systems.

Without providing proper justification for funds, IRM's accountability of the IT Infrastructure investment is not fully supported. OMB will not give the investment's Exhibit 300 a passing score if the Exhibits are incomplete. Failure to earn a passing score puts the investment's entire Exhibit 300 at risk for failing and for losing funding. These project charters and risk management plans are critical not only to investments' success but also to securing the funding necessary to acquire and operate IT investments.

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

Management Response: The Department concurred with the recommendation, stating that it was "identifying training opportunities to further understand the reporting requirements needed to ensure accurate reporting of Capital Planning Investment Control submissions."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation, showing that Information

[43] The Department of State's electronic Capital Planning Investment Control (eCPIC) portfolio management tool that is used for managing IT investments.

[44] "OMB Guidance on Exhibit 300 – Planning, Budgeting, Acquisition, and Management of Information Technology Capital Assets," Aug. 2011.

Technology Service Line Program Managers have been trained on the electronic Capital Planning Investment control tool.

List of Current Year Recommendations

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

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

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

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

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

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

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

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

Recommendation 9. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, revise the *Foreign Affairs Manual* to provide authority to the

Chief Information Officer to review and identify accounts not used within the past 90 days and to de-activate such accounts and require the bureaus and posts to recertify the user account prior to re-activating the account.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recommendation 25. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, perform an entity-wide Business Impact Analysis and develop a strategy to prioritize recovery of the critical assets within the Department and align the Business Impact Analysis of the primary mission-critical functions with Information Resource Management's Maximum Tolerable Downtime for the network.

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

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

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

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

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

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

Appendix A

Scope and Methodology

In order to fulfill its responsibilities related to the Federal Information Security Management Act (FISMA), 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 information security program and practices to determine the effectiveness of such programs and practices for FY 2012. The OIG and Williams, Adley & Company-DC, LLP, held an exit conference with management on November 15, 2012.

FISMA requires 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 or contractor or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

We performed the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), FISMA, OMB, and National Institute of Standards and Technology (NIST) Special Publications (SP) guidance. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Our fieldwork was completed before OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," October 2, 2012, was issued. This memorandum provided instructions for FY 2012 reporting requirements. We reviewed the memorandum and evaluated its impact on our results but determined that no changes were required to be made.

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

- OMB Memorandums M-02-01, M-04-04, M-06-19, and M-12-20.[1]
- DHS Federal Information Security Memorandum (FISM) 12-02.[2]

[1] OMB Memorandum 02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones"; OMB Memorandum 04-04, "E-Authentication Guidance for Federal Agencies"; OMB Memorandum 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"; OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," respectively.

[2] DHS Memorandum 12-02, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Feb. 15, 2012.

- Department policies and procedures such as the *Foreign Affairs Manual* (5 FAM and 12 FAM).[3]
- Federal laws, regulations, and standards such as FISMA, OMB Circular A-130, Appendix III,[4] and OMB Circular No. A-11.[5]
- NIST Special Publications (SP), Federal Information Processing Standards, other applicable NIST publications, and industry best practices.

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

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

The audit covered the period of October 1, 2011, to September 30, 2012. During the fieldwork, we took the following actions:

- 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 A-130, Appendix III, processes and reporting requirements; and NIST and Federal Information Processing Standards requirements.

- Reviewed all 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 reporting instructions from OMB Memorandum M-12-20.

- Assessed programs for monitoring of security policy and program compliance and responding to security events (that is, unauthorized changes detected by intrusion detection systems).

- Performed testing of major systems at the discretion of OIG. We tested 26 systems for our sample. (See Appendix E).

[3] 5 FAM, "Information Management" and 12 FAM, "Diplomatic Security."
[4] OMB Circular No. A-130 Revised Appendix III, "Security of Federal Automated Information Resources."
[5] OMB Circular No. A–11, "Preparation, Submission, and Execution of the Budget."

- Assessed the adequacy of internal controls related to the areas reviewed. Control deficiencies identified during the review are reported in the report.

- Evaluated the Department's remedial action taken to address the previously reported Information Security Program control weaknesses identified in OIG's report *Evaluation of Department of State Information Security Program* (AUD/IT-12-14, Nov. 2011).

Review of Internal Controls

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

- The Department had established an enterprise wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- The Department had established and was maintaining a security configuration management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- The Department had established and was maintaining an account and identity management program that was generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices.

- The Department had established and was maintaining an incident response and reporting program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- The Department had established a risk management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- The Department had established and was maintaining a security training program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- The Department had established a POA&M program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that tracked and monitored known information security weaknesses.

- The Department had established and was maintaining a remote access program that was generally consistent with NIST and OMB FISMA requirements.

- The Department had established and was maintaining an entity-wide business continuity/disaster recovery program that was generally consistent with NIST's and OMBFISMA requirements.

- The Department had established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization.

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

Use of Computer-Processed Data

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 Active Directory and the Department's human resources system to test user account management controls. We also reviewed data generated by software tools to determine the existence of security weaknesses that were identified during vulnerability assessments. We assessed the reliability of computer-generated data primarily by comparing selected data with source documents. We determined that the information was reliable for assessing the adequacy of related information security controls.

Appendix B

Follow-up of Recommendations From the FY 2011 FISMA Report

The audit team reviewed actions implemented by management to mitigate the findings identified in the FY 2011 FISMA report. The current status of each of the recommendations is as follows:

Recommendation 1. We recommend that the Information Security Steering Committee (ISSC) meet on a monthly basis to fulfill its purpose and responsibilities as required in ISSC charter.

2012 Status: Closed. As of March 2012, management updated the ISSC Charter to require the ISSC to meet only on an adhoc basis.

Recommendation 2. We recommend that the Information Security Steering Committee improve its risk management strategy at the organizational level for assessing, responding to, and monitoring information security risk as required in the Foreign Affairs Manual and the National Institute of Standards and Technology Special Publication 800-39.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 1 (Finding A) in the FY 2012 report.

Recommendation 3. We recommend that the Chief Information Officer:

- Improve oversight of the security assessment and authorization process for the Department’s information systems, especially the OpenNet General Support System (GSS) and ClassNet GSS as required by the National Institute of Standards and Technology (NIST) (SP) 800-37.
- Improve existing procedures to ensure security authorization packages are updated every 3 years or when a significant change occurs or develop a risk-based approach for implementing a continuous monitoring strategy as required by NIST SP 800-37.
- Improve existing procedures to ensure Systems Security Plans and Systems Assessment Reports are updated as required to comply with the security baseline controls contained in NIST SP 800-53 (Revision 3).
- Perform annual security assessments of a subset of a system’s security controls as required by NIST SP 800-37.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 17 and 18 (Finding G) in the FY 2012 report.

Recommendation 4. We recommend that the Chief Information Officer expedite the Information Resource Management, Operations, Enterprise Network Management and Diplomatic Security, Security Infrastructure, Office of Computer Security process to finalize and implement the elements within the Cyber Security Architecture draft target architecture and initiative for end-to–end configuration management and take immediate action to correct or mitigate the high risk vulnerabilities identified by the vulnerability scanning as required by the Foreign Affairs Manual and Diplomatic Security System Configuration Policy and Procedures.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 3 and 4 (Finding B) in the FY 2012 report.

Recommendation 5. We recommend that the Chief Information Officer and the Bureau of Diplomatic Security ensure, for significant security responsibility (SSR) training, that personnel designated as having SSR responsibilities receive the appropriate training as required by the Information Assurance Training Plan.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 20 (Finding H) in the FY 2012 report.

Recommendation 6. We recommend that the Chief Information Officer implement, for Security Awareness Training, automated methods to replace the current manual process to track and enforce the Department of State security awareness policy and to suspend a user's access to the network if the user has not taken the Cyber Security Awareness course within the required timeframe as required by the Information Assurance Training Plan.

2012 Status: Closed. As of March 2012, the Cybersecurity Tracking system updates the user's Active Directory account expiration date immediately after the student completes the Cyber Security Awareness (PS800) training. This Active Directory update extends the user's account expiration date by 368 days. If the user fails to retake the test in 368 days, the user's account expires and the user cannot access the system without manual intervention by an administrator.

Recommendation 7. We recommend that the Chief Information Officer:

- Implement a Plans of Action and Milestones (POA&M) tracking process for all ClassNet security weaknesses as required by Committee on National Security Systems Policy Number 22, Information Assurance Risk Management Policy for National Security Systems.
- Distribute the quarterly POA&M Grade Memorandums to the bureaus' and offices' senior management (executive director) as required by M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.
- Ensure that the POA&M completion dates and the required resources for OpenNet corrective actions are updated as required by OMB Memorandum M-04-25.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 21 (Finding I) in the FY 2012 report.

Recommendation 8. We recommend that the Chief Information Officer (CIO) develop and implement Department of State processes and procedures to resolve weaknesses in user accounts to ensure that unnecessary network user accounts are promptly removed by the bureaus and posts. Further, the CIO should develop and implement procedures to ensure that bureaus and organizational unit administrators annually review and recertify access privileges of users so that the number of guest, test, and temporary accounts are managed effectively as required by the Foreign Affairs Manual 12 FAM 622 and 12 FAM 629.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 8 – 10 (Finding E) in the FY 2012 report.

Recommendation 9. We recommend that the Chief Information Officer (CIO) ensure compliance with the account management process to make certain that user and administrator accounts are created, modified, and deleted in a manner consistent with Department of State policy. Further, the CIO needs to compare the terminated user listings provided by bureau and post personnel officers with information contained in the active directory on a quarterly basis to ensure that accounts for separated employees are removed timely, as required by NIST SP 800-53, Revision 3, August 2009, *Recommended Security Controls for Federal Information Systems and Organizations*, and the Foreign Affairs Manual (12 FAM 621.3).

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 11 – 15 (Finding F) in the FY 2012 report.

Recommendation 10. We recommend that the Information Security Steering Committee develop, document, and implement an enterprise-wide continuous monitoring strategy that addresses framing risk, assessing risk, responding to risk, and monitoring risk, as required by NIST SP 800-39, *Managing Information Security Risk*.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 1 (Finding A) in the FY 2012 report.

Recommendation 11. We recommend that the Chief Information Officer in accordance with the requirements in NIST SP 800-39, *Managing Information Security Risk*:

- Implement a continuous monitoring strategy at the enterprise-wide level.
- Obtain and use scanning software to enable effective scans of non-Windows operating systems, databases, firewalls, routers, and switches.
- Develop operating procedures to ensure the results are included in the Risk Scoring Program dashboard.
- Develop procedures to ensure that System Security Owners update the system security plans to include a continuous monitoring strategy to detail how system security controls is to be monitored.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 6 and 7 (Finding D) in the FY 2012 report.

Recommendation 12. We recommend that the Chief Information Officer, as required by NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems,* take the following actions:

- Update the Continuity of Operations Communication Plan annually or when changes occur to the organization, network hardware, systems, and applications and, if necessary, after Continuity Testing.

- Perform an entity-wide Business Impact Analysis and develop a strategy to prioritize recovery of the critical assets within the Department of State.
- Update the section of the Foreign Affairs Manual that contains guidance and direction for development and implementation of Continuity of Operations Communication Plan.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 24 – 26 (Finding K) in the FY 2012 report.

Recommendation 13. We recommend that the Bureau of Administration, Office of Emergency Management, in coordination with the Chief Information Officer, align the Business Impact Analysis of the Primary Mission Essential Functions with the Bureau of Information Resource Management's Maximum Tolerable Downtime for the network as required by NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 25 (Finding K) in the FY 2012 report.

Recommendation 14. As required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, and SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, we recommend that the Bureau of Information Resource Management, Office of Information Assurance, in coordination with the bureaus and system owners, take the following actions:

- Document and maintain alternate site locations and procedures for accessing an alternate site.
- Develop and maintain contingency plans for all major applications and general support systems.
- Maintain and update recovery and restoration procedures for all applications and general support systems.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 27 (Finding L) in the FY 2012 report.

Recommendation 15. As required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* and SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, we recommend that the Chief Information Officer:

- Revise the Information Resource Management/ Information Assurance Contingency Plan Test Review checklist to address the following items:

  - Recovery and damage assessment procedures
  - Alternate recovery site details
  - Back-up procedures
  - Back-up test results for moderate- and high-impact systems

- Revise the Contingency Plan Policy to include an organization-defined frequency for backup testing.

- Revise the *Foreign Affairs Manual* to require system owners to report to IRM/IA on the test results and updates to the contingency plans.

2012 Status: Closed. As of March 2012, the Information Resource Management/ Information Assurance (IRM/IA) Contingency Plan Test Review checklist had been updated, the Contingency Plan Policy now includes an organization-defined frequency for backup testing, and the Foreign Affairs Manual requires system owners to report to IRM/IA on the test results and updates to the contingency plans.

Recommendation 16. We recommend that the Chief Information Officer in accordance with the Foreign Affairs Manual (5 FAM 1065.3) and the National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems,* take the following actions:

- Ensure that the contractor oversight program complies with Office of Management and Budget, Federal Information Security Management Act, National Institute of Standards and Technology, and the Foreign Affairs Manual security policies, standards, and requirements for managing Contractor Owned Contractor Operated (COCO) systems; specifically, all security-related documentation for such systems should be retained.

- Implement a COCO system security program whereby COCOs are overseen by the Bureau of Information Resource Management/ Information Assurance.

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendations 28- 30 (Finding M) in the FY 2012 report.

Recommendation 17. We recommend that the Bureau of Diplomatic Security develop and implement new and enhanced security requirements to coordinate security activities for tracking all extensions (that is, contractor sites, other Government agencies, and third-party vendors) to OpenNet and ClassNet as required by the Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

2012 Status: Closed. This is a repeat recommendation from the FY 2011 report. It has become Recommendation 30 (Finding M) in the FY 2012 report.

Recommendation 18. We recommend that the Bureau of Diplomatic Security, in coordination with the Bureau of Administration, establish procedures to identify the total number of contractors who have access to Department of State systems, as required by the Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

2012 Status: Closed. Domestically, the number of contractors can be tracked through Centralized Emergency Notification System via the Data Capturing and Feeding (DCAF) system. For overseas contractors, Post Profiles can display the count of contractors as collected via WebPass.

Recommendation 19. We recommend that the Chief Information Officer, as required by Office of Management and Budget (OMB) Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* and OMB Circular No. A–11, *Preparation, Submission, and Execution of the Budget*:

- Ensure that the Bureau of Information Resource Management/ Business Management and Planning track all obligations and expenditures for information technology security investments.
- Provide a summary of non-major investments that make up the information technology-Infrastructure and other major investments.
- Include the Unique Project Identifier in the Department of State's Plans of Action and Milestones database.

2012 Status: Closed. As of August 2012, Unique Project Identifiers have been included in the Department of State's Plans of Action and Milestones database.

Appendix C

End-to-End Configuration Management Process Needs Improvement

Although the Department of State was taking actions to address the prior year noted weaknesses with the configuration management controls, the weaknesses within configuration management process still exist. During the independent vulnerability scanning analysis performed, we identified the following issues as shown in Tables 1 and 2.

Table 1. Systems Without Critical Patches Installed

No.	System Name	Classification	Total Number of Patch and Hot Fix Issues
1	NIV	Unclassified	7
2	ASTORM	Unclassified	0
3	ARS	Unclassified	157
4	CADSS	Unclassified	32
5	CRMSS	Unclassified	19
6	MCI	Unclassified	21
7	BMIS	Unclassified	0
8	LFMS	Unclassified	27
9	STMS	Unclassified	15
10	TOMIS	Unclassified	173
11	CRTS	Unclassified	13
12	IIP_PMOS	Unclassified	33
13	OPENNET	Unclassified	25
14	GO	Unclassified	242
15	Remedy 7.0	Unclassified	287
Total			1,051

System Name (Number of Servers Affected)	Third Party Patch Issues
ARS (6/10) BMIS (2/4) STMS (1/3) OPENNET(1/46) GO (1/76) Remedy (3/44)	Oracle Java Critical Patch missing
CADSS(2/4) GO (13/76)	Adobe Flash Player Multiple Vulnerabilities

Table 2. Systems Configured To Allow Unauthorized Users

System (Number of servers affected)	Risk	Description

NIV(1/4)
CRTS(1/12)
	Apache web server vulnerable to Denial of Service Attack	Apache httpd Ranges Header Field Memory Exhaustion (DoS)

CADSS (2/4) CRMS (1/3) MCI (1/2) STMS (2/3) TOMIS (2/14) CRTS (2/12) OPENNET (2/46) Remedy (1/44) ARS (1/10)	Confidentiality and Integrity can be violated.	Web Server Supports Weak SSL Encryption Certificates and SSL V2 protocol
CRMS (1/3) MCI (2/2) BMIS (1/4) LFMS (3/3) STMS(2/3) CRTS(1/12) GO(11/76) Remedy (5/44) ARS(1/10)	Unauthorized access	Administrator Users Password Never Expires

MCI (2/2)
BMIS(3/4)
GO(1/76)
Remedy (8/44)
	Buffer Overflow	IBM Tivoli Storage Manager Client JBB Functionality Buffer Overflow Privileges Escalation

STMS(2/3)
IIP_PMOS (3/14)
OPENNET(10/46)
GO(16/76)
Remedy (4/44)
	Access Bypass	HP System Management Homepage Multiple Vulnerabilities

TOMIS (3/14)	Confidentiality and Integrity can be violated.	Oracle Application Server multiple Vulnerabilities
TOMIS(3/14) Remedy (1/44)	Confidentiality and Integrity can be violated.	Tomcat Example Web Application Vulnerable to Cross-Site Scripting attack.
CRTS(4/12)	Denial of Service Attack	Symantec Veritas Backup Exec for Windows RPC Heap Overflow
CRTS(2/12)	Denial of Service Attack	IBM HTTP Server vulnerable to Denial Of Service

System (Number of servers affected)	Risk	Description
CRTS (2/12)	Privilege escalation	Oracle Database multiple vulnerabilities
IIP-PMOS(1/14)	Denial of Service Attack	IBM Lotus Notes Buffer Overflow
GO(4/76)	Access bypass and Denial of Service attack	Citrix XenApp multiple vulnerabilities
Remedy (1/44)	Denial of Service attack	MySQL Access Validation Denial Of Service Vulnerability
Remedy (1/44)	Confidentiality and Integrity can be violated.	SAP Crystal Reports Server Multiple Vulnerabilities

Appendix D

Weak Active Directory User Account Management

The Department of State needs to improve account management procedures and processes in Active Directory (AD) for OpenNet and ClassNet. In FY 2011, the Office of Inspector General reported deficiencies in account management. Although the Chief Information Officer is taking action, the audit identified deficiencies with account management controls covering Active Directory.

Table 1 lists stale user accounts, user accounts that were never logged on, and accounts with passwords that never expire and are not required.

Table 1. Count of Weak Active Directory User Account

AD Tab	Count of Stale User Account	Count of User Account that Never Logged On	Count of Passwords not required (All AD accounts)	Count of Passwords Never Expire (All AD accounts)
AF	909	521	2,123	11
Apps	10	6	1	121
CA	68	75	1,917	30
ConUS	40	23	82	3
DS	278	95	925	37
EAP	858	675	2,424	21
EUR	943	1,150	4,152	20
GFS	6	3	1	0
NEASA	1,112	773	2,224	71
OIG	12	28	103	12
SES	144	6	248	60
State	1	7	0	6
WashDC	705	1,742	2,045	106
WHA	1,183	613	3,090	31
Grand Total	**6,269**	**5,717**	**19,335**	**529**
Total User Accounts	**116,821**			
Total Service Accounts	**4,552**			
Total Shared Mailbox Accts	**329**			

Appendix E

Sample Selection of Information Systems Listed in Information Technology Asset Baseline Used for FY 2012 Audit – Vulnerability Assessment

The sample selection described in the title of this appendix is shown as follows:

Name	Acronym	Bureau	Classification	Categorization
Freedom of Information Document Management System	FREEDOMS	A	Classified	M|L|L
State Archiving System 2	SAS2	A	Classified	M|M|L
A Bureau Metastorm	ASTORM	A	Unclassified	Moderate
Consular Affairs Rational Tool Set	CRTS	CA	Unclassified	Moderate
Action Request System	ARS	CA	Unclassified	Moderate
Consular Affairs Domestic Support Suite	CADSS	CA	Unclassified	Moderate
Consular Affairs ClassNet Website	CACLI	CA	Classified	High
Non-Immigrant Visa System	NIV	CA	Unclassified	Moderate
electronic SAO Portal	eSP	CA	Classified	M|M|M
Technical Security Countermeasures	TSCM	DS	Classified	M|M|M
Counterintelligence Network Application	CINA	DS	Classified	M|H|H
The Office of Foreign Missions Information System	TOMIS	DS	Unclassified	High
Student Training Management System	STMS	FSI	Unclassified	Moderate
IIP Program Management and Outreach System	IIP-PMOS	IIP	Unclassified	Moderate
Local Financial Management System	LFMS	INL	Unclassified	Moderate
BMC Remedy IT Service Management Suite	Remedy 7.0	IRM	Unclassified	Moderate
ClassNet Public Key Infrastructure	CPKI	IRM	Classified	High
Global OpenNet	GO	IRM	Unclassified	Moderate
OpenNet Plus Transport GSS	OPENNET	IRM	Unclassified	Moderate
ClassNet	CN	IRM	Classified	M|M|M
Medical Capabilities Information database	MCI	MED	Unclassified	Moderate
Buildings Management Integrated System	BMIS	OBO	Unclassified	Moderate
Central Resource Management System	CRMS	RM	Unclassified	Moderate
Consolidated Reconciliation	CRS	RM	Unclassified	Moderate

System				
Secretariat Telegram Processing System (Second Edition)	STEPS II	S	Classified	M|H|H
Secretariat Tracking and Retrieval System	STARS	S	Classified	M|H|M

Legend

Bureaus	
A – Bureau of Administration	INL-Bureau of International Narcotics and Law Enforcement Affairs (INL)
CA – Bureau of Consular Affairs	IRM- Bureau of Information Resource Management
DS – Bureau of Diplomatic Security	MED – Office of Medical Services
FSI - Foreign Service Institute	OBO- Bureau of Overseas Building Operations
IIP – Office of International Information Programs	RM- Bureau of Resource Management
S- Office of the Secretary	

Appendix F

Missing NIST SP 800-53, Revision 3, Baseline Security Controls

Name	Acronym	Bureau	Classification	FIPS Categorization	NIST 800-53 rev 3
Electronic Passport Application Form Internet Website	2DB	CA	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Diplomatic Security Business Process Management System	BPMS	DS	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Consular Shared Tables	CST	CA	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Global Affairs Dashboard	Dashboard	RM	Unclassified	Low	AC-19; AC-22; AU-6; AU-12; CM-4; CM-7; CP-3; IA-8; IR-2; IR-5; IR-8; PM-1 to PM11; RA-5; SC-12; SC-15; SC-20; SI-12
Diversity Immigrant Visa Information System	DVIS	CA	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Enterprise Data Warehouse	EDW	IRM	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Electronic Visa Application Form	EVAF	CA	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Visa Opinion Information Service	VOIS	CA	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7
Resource and Budget Integration Tool	Web RABIT	RM	Unclassified	Moderate	AC-22; AU-12; CM-9; IA-8; IR-8; MP-3; PE-4; PM1 to PM11; SA-10; SC-28; SC-32; SI-7

Bureaus	SP 800-53 Control Family	
CA – Bureau of Consular Affairs	**AC – Access Controls**	**PE - Physical and Environmental Protection**
DS – Bureau of Diplomatic Security	**AU - Audit and Accountability**	**PM - Program Management**
IRM- Bureau of Information Resource Management	**CM - Configuration Management**	**RA - Risk Assessment**
RM- Bureau of Resource Management	**IA - Identification and Authentication**	**SA - System and Services Acquisition**
	IR - Incident Response	**SC - System and Communications Protection**
	MP - Media Protection	**SI - System and Information Integrity**

Appendix G

FISMA Reportable Systems That Have Not Completed the FY 2012 Contingency Plan Test

The systems described in the title of this appendix are shown as follows:

Name	Acronym	Bureau	Classification	Categorization
OpenNet Plus Transport GSS	OPENNET	IRM	Unclassified	Moderate
Global OpenNet	GO	IRM	Unclassified	Moderate
Freedom of Information Document Management System	FREEDOMS	A	Classified	M|L|L
Secretariat Telegram Processing System (Second Edition)	STEPS II	S	Classified	M|H|H
Secretariat Tracking and Retrieval System Bottom of Form	STARS	S	Classified	M|H|M
SPCD - (Classified)	SPCNet	OBO	Classified	M|H|H

Legend

Bureaus	
A – Bureau of Administration	OBO- Bureau of Overseas Building Operations
IRM- Bureau of Information Resource Management	S- Office of the Secretary

Appendix H

FISMA Reportable Systems Missing Alternate Processing Site Details

The systems described in the title of this appendix are shown as follows:

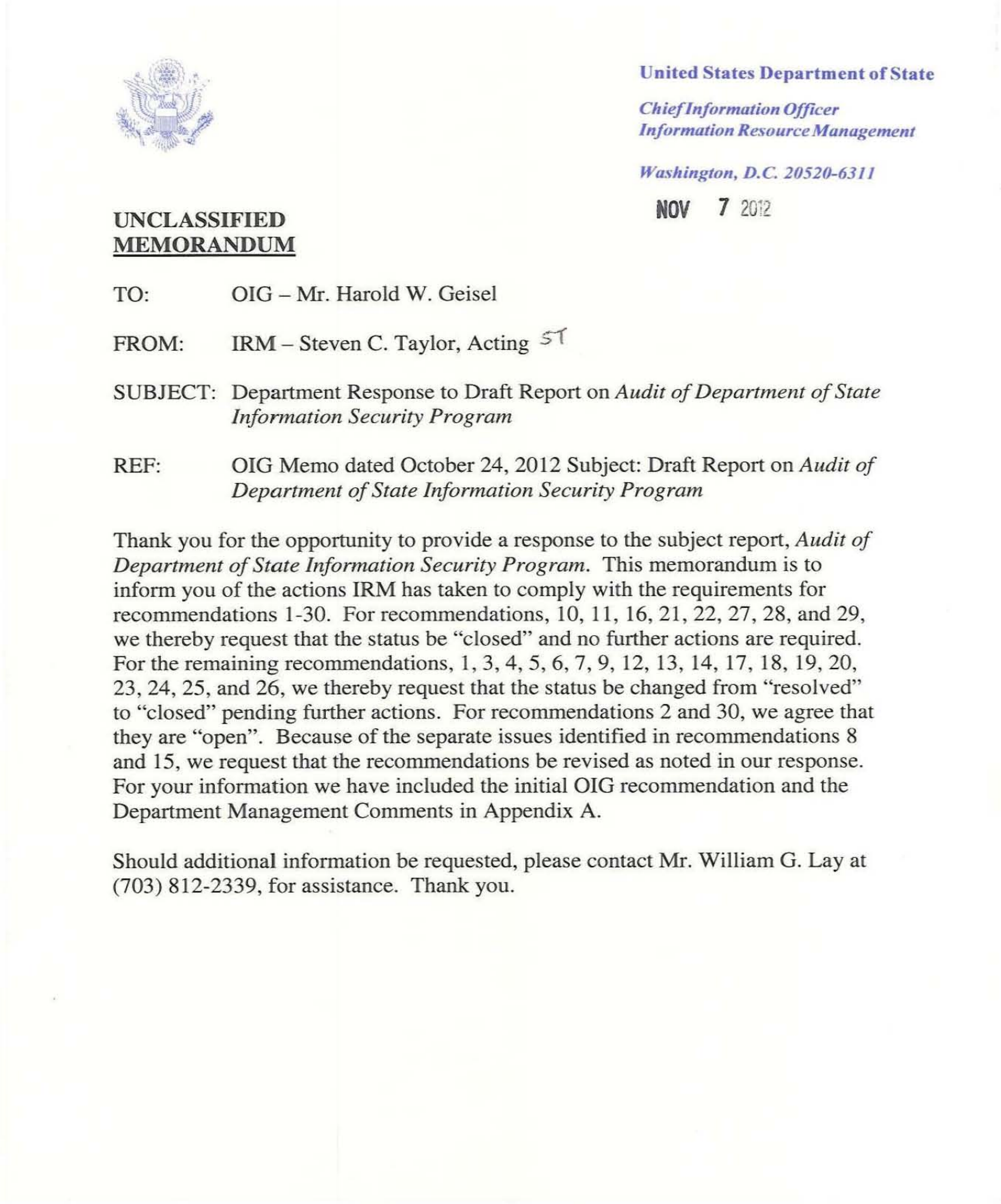
Name	Acronym	Bureau	Classification	Categorization
IIP Program Management and Outreach System	IIP-PMOS	IIP	Unclassified	Moderate
Global INL	GINL	INL	Unclassified	High
Airwing Information System	AWIS	INL	Unclassified	Moderate
OpenNet Plus Transport GS**S**	OPENNET	IRM	Unclassified	Moderate
Global OpenNet	GO	IRM	Unclassified	Moderate
Freedom of Information Document Management System	FREEDOMS	A	Classified	M|L|L
Secretariat Telegram Processing System (Second Edition)	STEPS II	S	Classified	M|H|H
Secretariat Tracking and Retrieval System Bottom of Form	STARS	S	Classified	M|H|M
SPCD - (Classified)	SPCNet	OBO	Classified	M|H|H

Legend

Bureaus	
A – Bureau of Administration	IRM- Bureau of Information Resource Management
IIP – Office of International Information Programs	OBO- Bureau of Overseas Building Operations
INL-Bureau of International Narcotics and Law Enforcement Affairs (INL)	S- Office of the Secretary

Appendix I

Department of State Response



United States Department of State

Chief Information Officer
Information Resource Management

Washington, D.C. 20520-6311

NOV 7 2012

UNCLASSIFIED
MEMORANDUM

TO: OIG – Mr. Harold W. Geisel

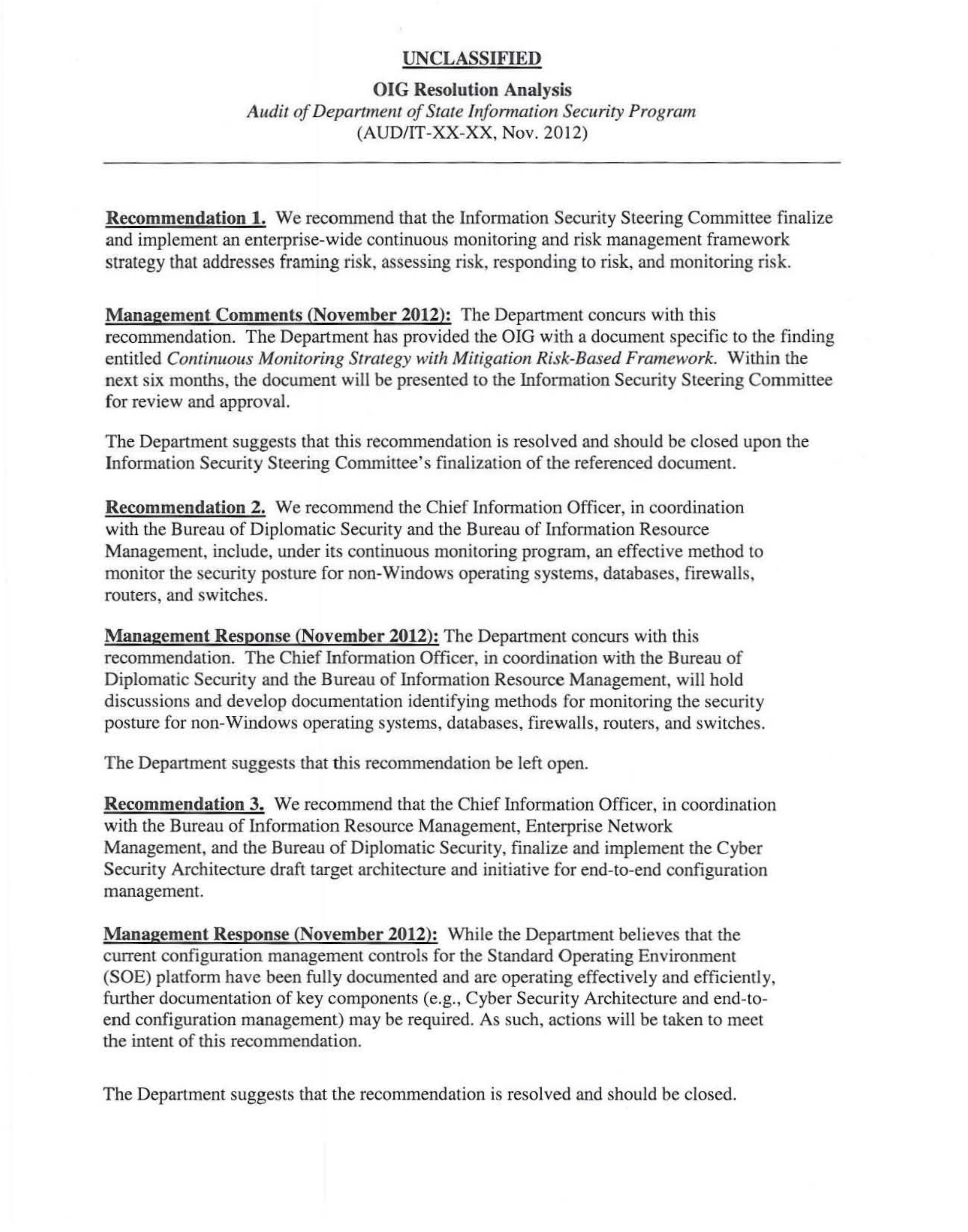
FROM: IRM – Steven C. Taylor, Acting ST

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

REF: OIG Memo dated October 24, 2012 Subject: Draft Report on *Audit of Department of State Information Security Program*

Thank you for the opportunity to provide a response to the subject report, *Audit of Department of State Information Security Program*. This memorandum is to inform you of the actions IRM has taken to comply with the requirements for recommendations 1-30. For recommendations, 10, 11, 16, 21, 22, 27, 28, and 29, we thereby request that the status be "closed" and no further actions are required. For the remaining recommendations, 1, 3, 4, 5, 6, 7, 9, 12, 13, 14, 17, 18, 19, 20, 23, 24, 25, and 26, we thereby request that the status be changed from "resolved" to "closed" pending further actions. For recommendations 2 and 30, we agree that they are "open". Because of the separate issues identified in recommendations 8 and 15, we request that the recommendations be revised as noted in our response. For your information we have included the initial OIG recommendation and the Department Management Comments in Appendix A.

Should additional information be requested, please contact Mr. William G. Lay at (703) 812-2339, for assistance. Thank you.



UNCLASSIFIED

OIG Resolution Analysis
Audit of Department of State Information Security Program
(AUD/IT-XX-XX, Nov. 2012)

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

Management Comments (November 2012): The Department concurs with this recommendation. The Department has provided the OIG with a document specific to the finding entitled *Continuous Monitoring Strategy with Mitigation Risk-Based Framework.* Within the next six months, the document will be presented to the Information Security Steering Committee for review and approval.

The Department suggests that this recommendation is resolved and should be closed upon the Information Security Steering Committee's finalization of the referenced document.

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

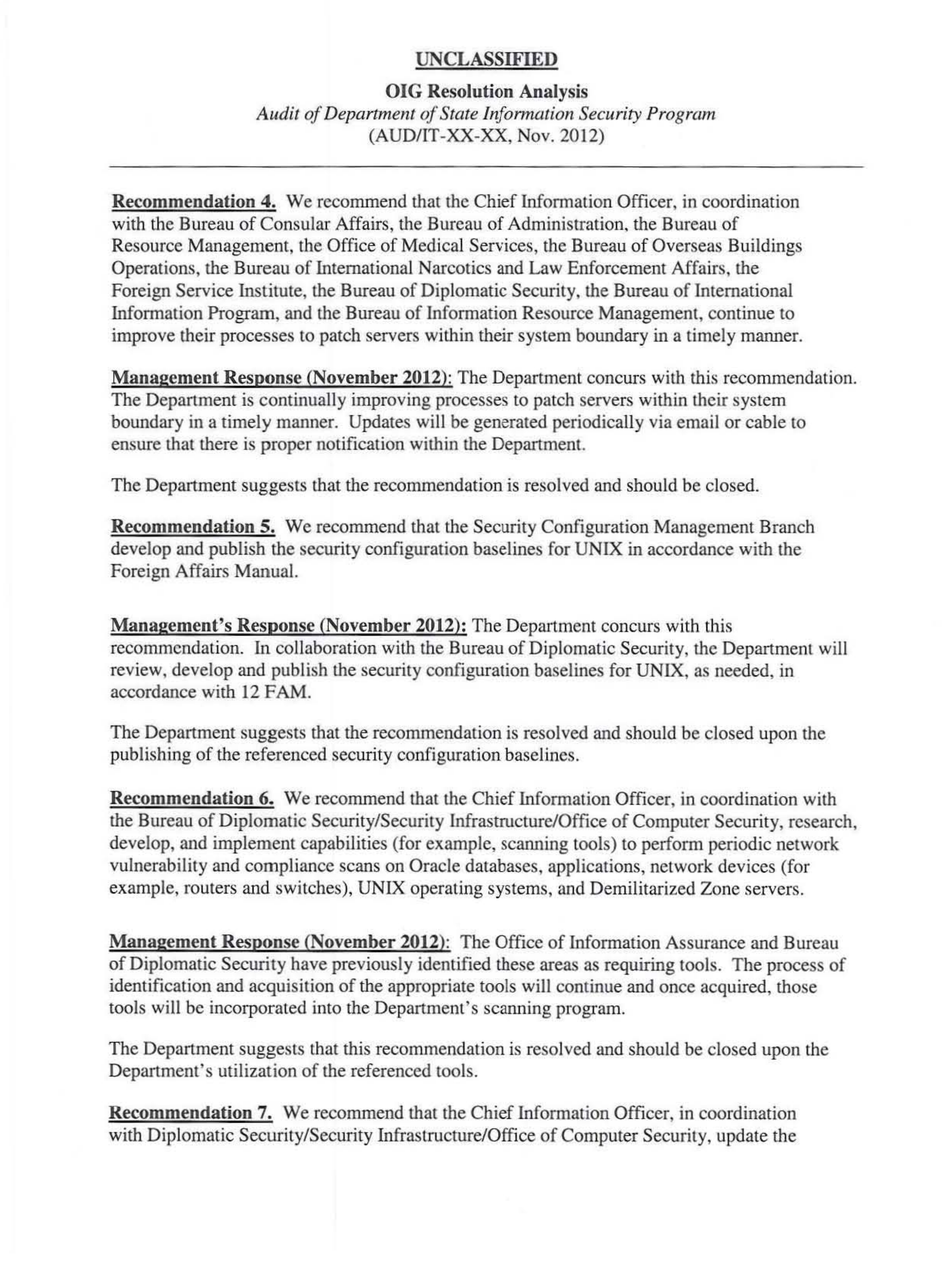
Management Response (November 2012): The Department concurs with this recommendation. The Chief Information Officer, in coordination with the Bureau of Diplomatic Security and the Bureau of Information Resource Management, will hold discussions and develop documentation identifying methods for monitoring the security posture for non-Windows operating systems, databases, firewalls, routers, and switches.

The Department suggests that this recommendation be left open.

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

Management Response (November 2012): While the Department believes that the current configuration management controls for the Standard Operating Environment (SOE) platform have been fully documented and are operating effectively and efficiently, further documentation of key components (e.g., Cyber Security Architecture and end-to-end configuration management) may be required. As such, actions will be taken to meet the intent of this recommendation.

The Department suggests that the recommendation is resolved and should be closed.



UNCLASSIFIED

OIG Resolution Analysis

Audit of Department of State Information Security Program

(AUD/IT-XX-XX, Nov. 2012)

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

Management Response (November 2012): The Department concurs with this recommendation. The Department is continually improving processes to patch servers within their system boundary in a timely manner. Updates will be generated periodically via email or cable to ensure that there is proper notification within the Department.

The Department suggests that the recommendation is resolved and should be closed.

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

Management's Response (November 2012): The Department concurs with this recommendation. In collaboration with the Bureau of Diplomatic Security, the Department will review, develop and publish the security configuration baselines for UNIX, as needed, in accordance with 12 FAM.

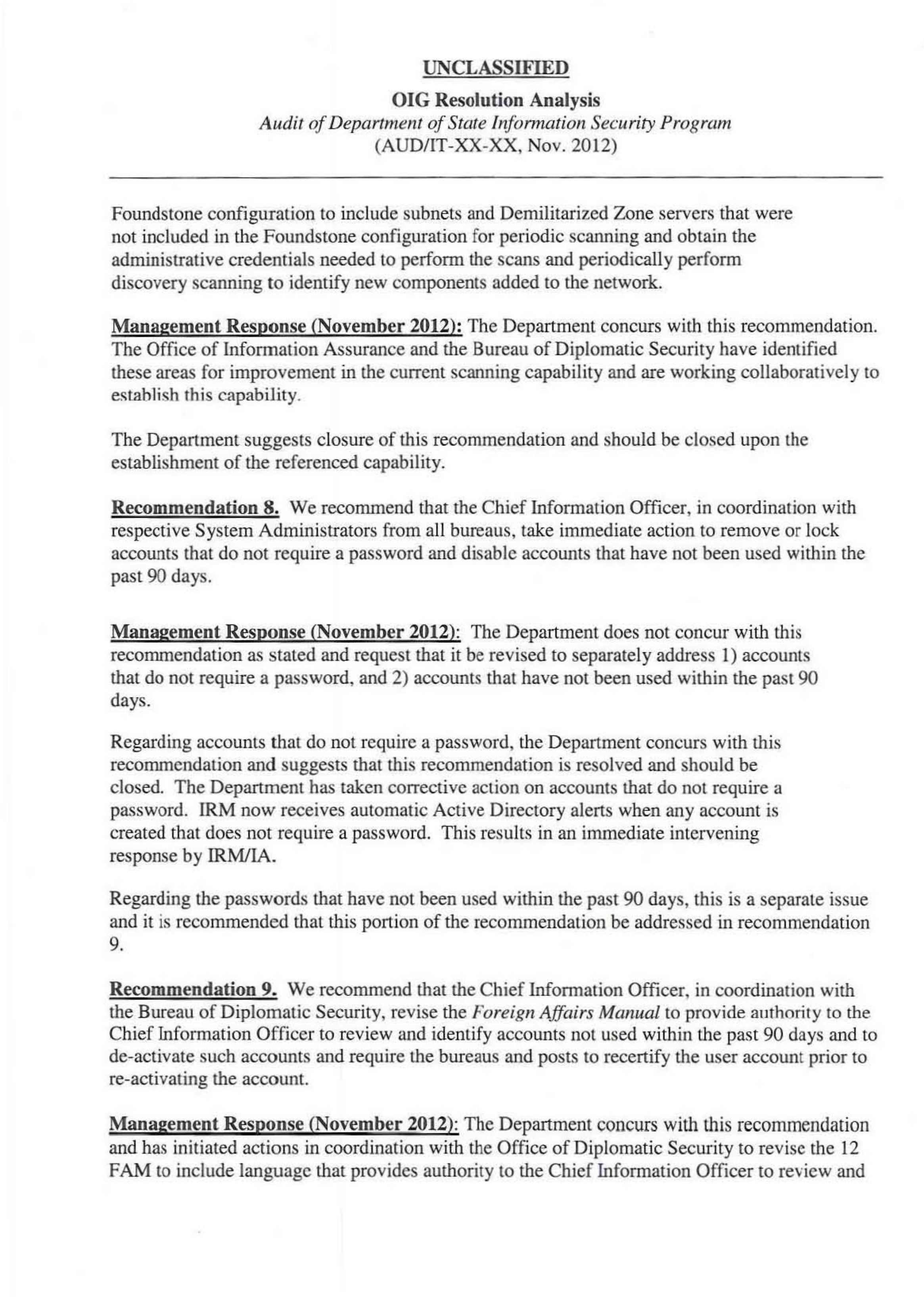
The Department suggests that the recommendation is resolved and should be closed upon the publishing of the referenced security configuration baselines.

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

Management Response (November 2012): The Office of Information Assurance and Bureau of Diplomatic Security have previously identified these areas as requiring tools. The process of identification and acquisition of the appropriate tools will continue and once acquired, those tools will be incorporated into the Department's scanning program.

The Department suggests that this recommendation is resolved and should be closed upon the Department's utilization of the referenced tools.

Recommendation 7. We recommend that the Chief Information Officer, in coordination with Diplomatic Security/Security Infrastructure/Office of Computer Security, update the



OIG Resolution Analysis

Audit of Department of State Information Security Program

(AUD/IT-XX-XX, Nov. 2012)

Foundstone configuration to include subnets and Demilitarized Zone servers that were not included in the Foundstone configuration for periodic scanning and obtain the administrative credentials needed to perform the scans and periodically perform discovery scanning to identify new components added to the network.

Management Response (November 2012): The Department concurs with this recommendation. The Office of Information Assurance and the Bureau of Diplomatic Security have identified these areas for improvement in the current scanning capability and are working collaboratively to establish this capability.

The Department suggests closure of this recommendation and should be closed upon the establishment of the referenced capability.

Recommendation 8. We recommend that the Chief Information Officer, in coordination with respective System Administrators from all bureaus, take immediate action to remove or lock accounts that do not require a password and disable accounts that have not been used within the past 90 days.

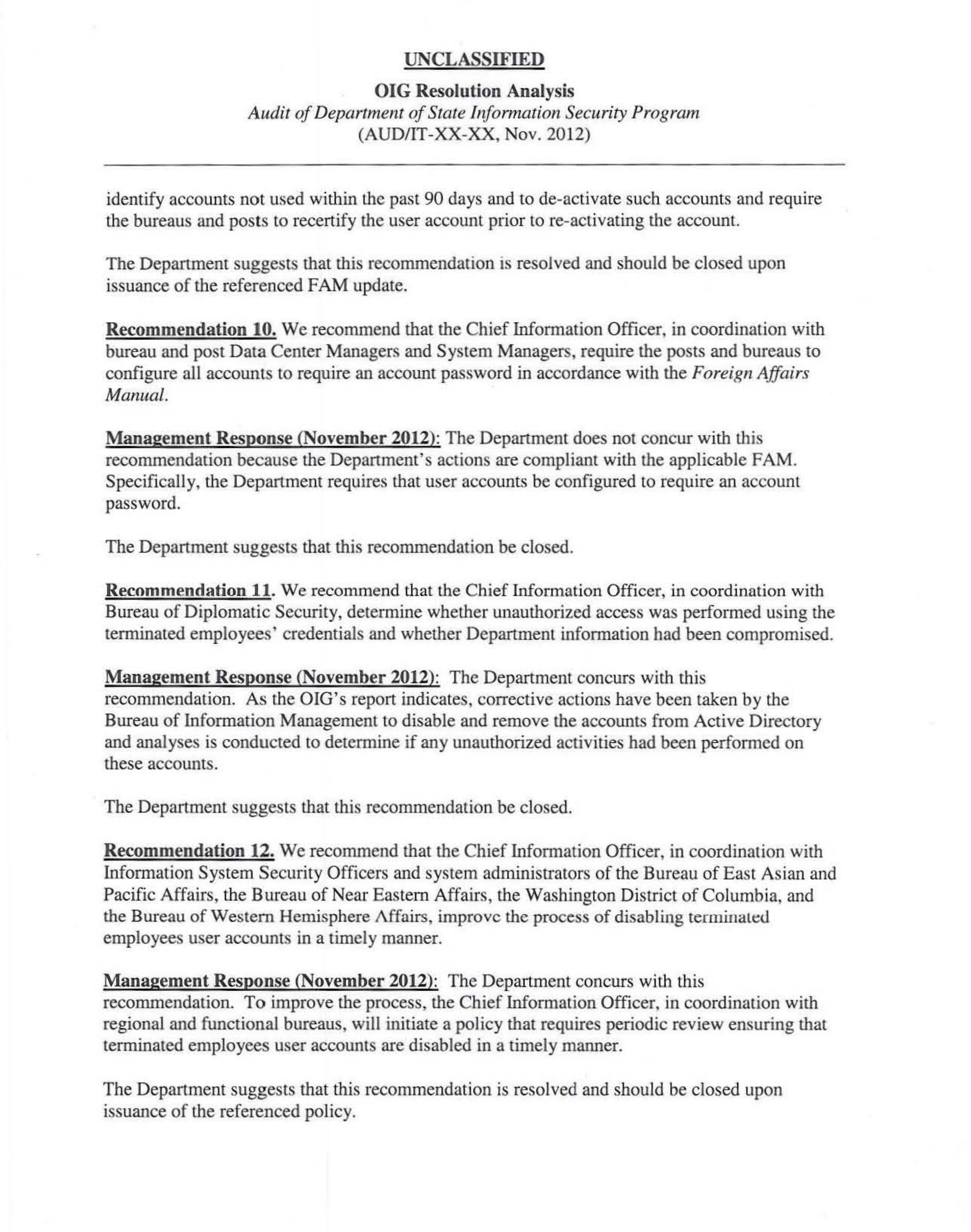
Management Response (November 2012): The Department does not concur with this recommendation as stated and request that it be revised to separately address 1) accounts that do not require a password, and 2) accounts that have not been used within the past 90 days.

Regarding accounts that do not require a password, the Department concurs with this recommendation and suggests that this recommendation is resolved and should be closed. The Department has taken corrective action on accounts that do not require a password. IRM now receives automatic Active Directory alerts when any account is created that does not require a password. This results in an immediate intervening response by IRM/IA.

Regarding the passwords that have not been used within the past 90 days, this is a separate issue and it is recommended that this portion of the recommendation be addressed in recommendation 9.

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

Management Response (November 2012): The Department concurs with this recommendation and has initiated actions in coordination with the Office of Diplomatic Security to revise the 12 FAM to include language that provides authority to the Chief Information Officer to review and



identify accounts not used within the past 90 days and to de-activate such accounts and require the bureaus and posts to recertify the user account prior to re-activating the account.

The Department suggests that this recommendation is resolved and should be closed upon issuance of the referenced FAM update.

Recommendation 10. We recommend that the Chief Information Officer, in coordination with bureau and post Data Center Managers and System Managers, require the posts and bureaus to configure all accounts to require an account password in accordance with the *Foreign Affairs Manual*.

Management Response (November 2012): The Department does not concur with this recommendation because the Department's actions are compliant with the applicable FAM. Specifically, the Department requires that user accounts be configured to require an account password.

The Department suggests that this recommendation be closed.

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

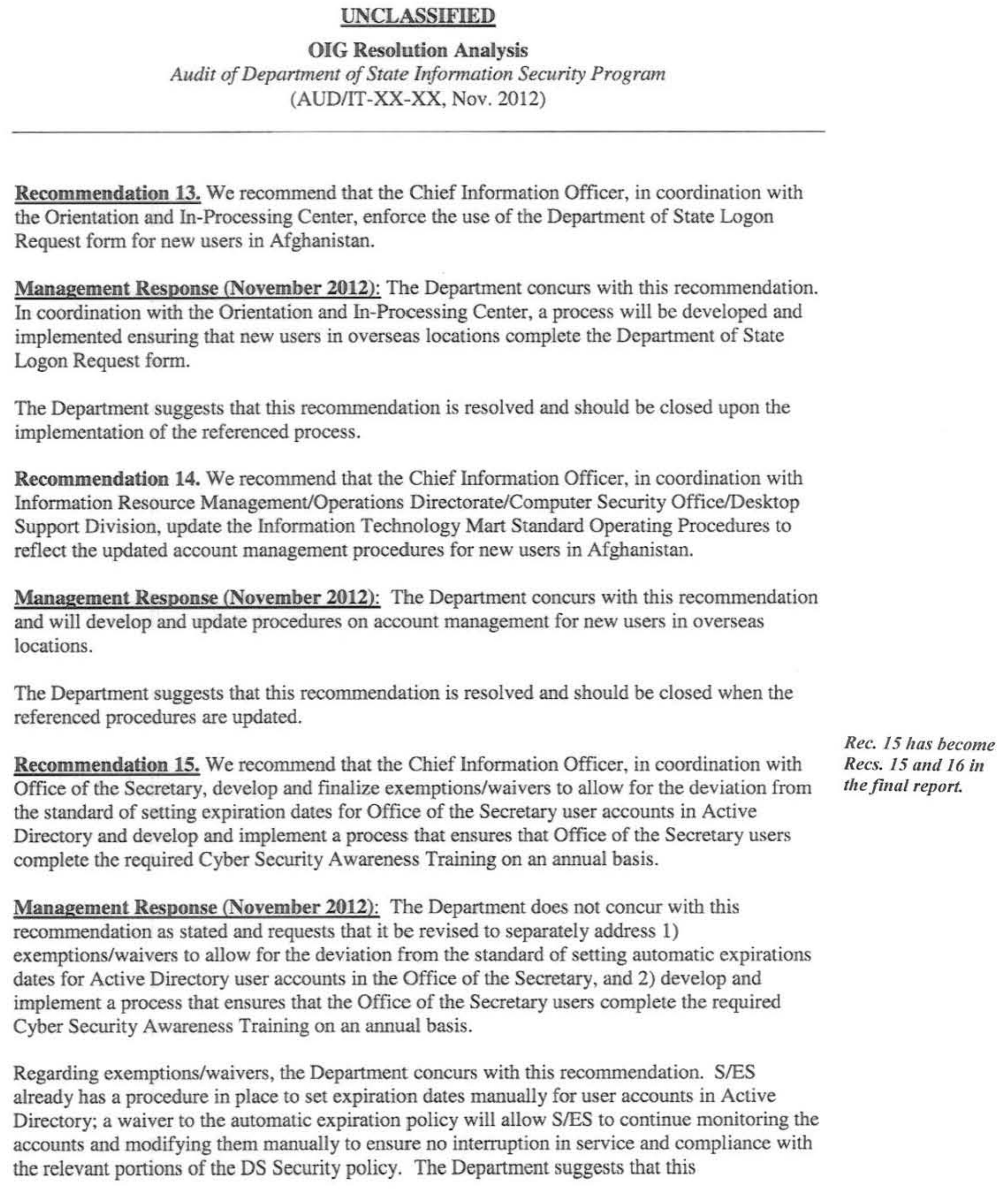
Management Response (November 2012): The Department concurs with this recommendation. As the OIG's report indicates, corrective actions have been taken by the Bureau of Information Management to disable and remove the accounts from Active Directory and analyses is conducted to determine if any unauthorized activities had been performed on these accounts.

The Department suggests that this recommendation be closed.

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

Management Response (November 2012): The Department concurs with this recommendation. To improve the process, the Chief Information Officer, in coordination with regional and functional bureaus, will initiate a policy that requires periodic review ensuring that terminated employees user accounts are disabled in a timely manner.

The Department suggests that this recommendation is resolved and should be closed upon issuance of the referenced policy.



UNCLASSIFIED

OIG Resolution Analysis

Audit of Department of State Information Security Program

(AUD/IT-XX-XX, Nov. 2012)

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

Management Response (November 2012): The Department concurs with this recommendation. In coordination with the Orientation and In-Processing Center, a process will be developed and implemented ensuring that new users in overseas locations complete the Department of State Logon Request form.

The Department suggests that this recommendation is resolved and should be closed upon the implementation of the referenced process.

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

Management Response (November 2012): The Department concurs with this recommendation and will develop and update procedures on account management for new users in overseas locations.

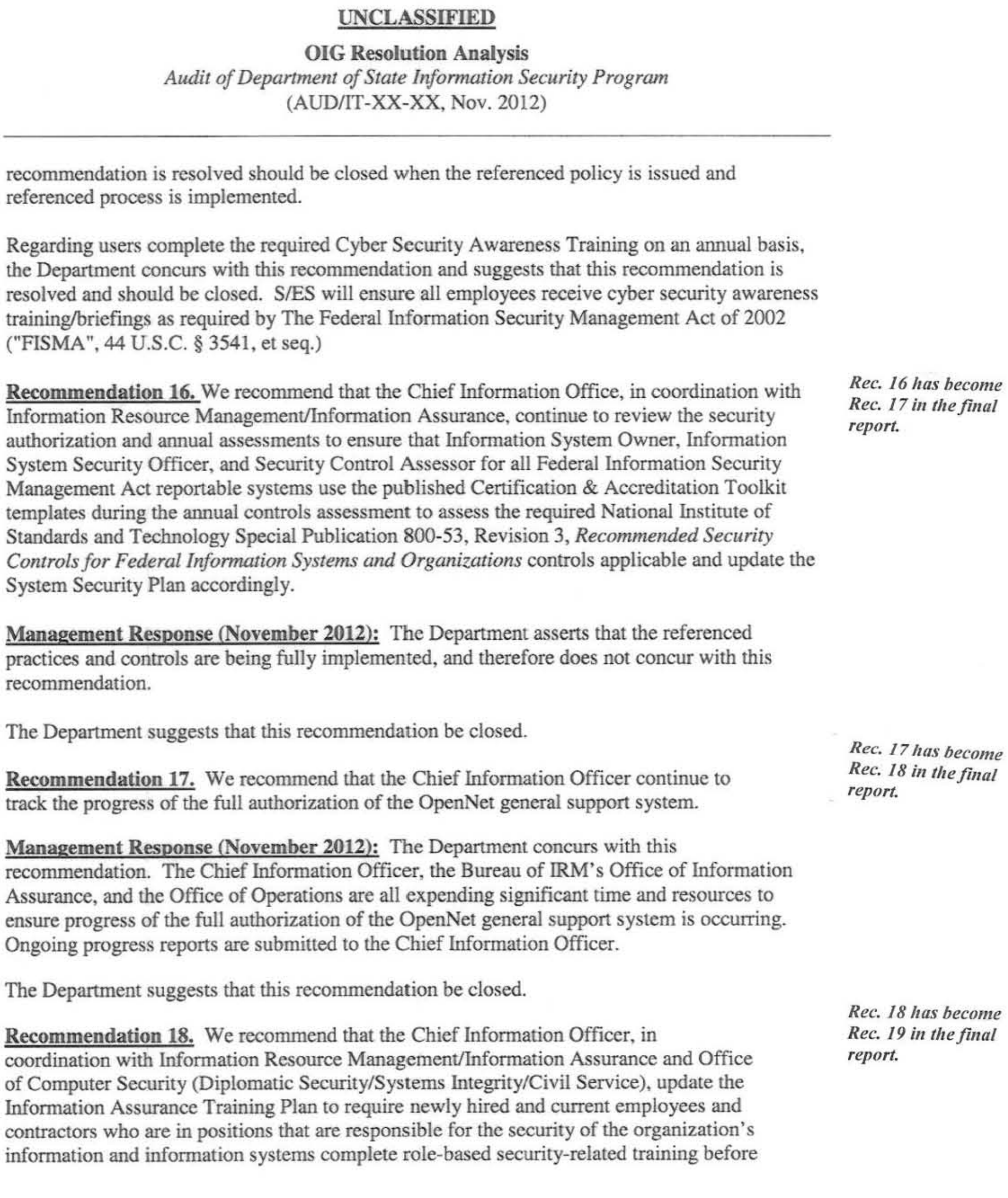
The Department suggests that this recommendation is resolved and should be closed when the referenced procedures are updated.

Recommendation 15. We recommend that the Chief Information Officer, in coordination with Office of the Secretary, develop and finalize exemptions/waivers to allow for the deviation from the standard of setting expiration dates for Office of the Secretary user accounts in Active Directory and develop and implement a process that ensures that Office of the Secretary users complete the required Cyber Security Awareness Training on an annual basis.

Rec. 15 has become Recs. 15 and 16 in the final report.

Management Response (November 2012): The Department does not concur with this recommendation as stated and requests that it be revised to separately address 1) exemptions/waivers to allow for the deviation from the standard of setting automatic expirations dates for Active Directory user accounts in the Office of the Secretary, and 2) develop and implement a process that ensures that the Office of the Secretary users complete the required Cyber Security Awareness Training on an annual basis.

Regarding exemptions/waivers, the Department concurs with this recommendation. S/ES already has a procedure in place to set expiration dates manually for user accounts in Active Directory; a waiver to the automatic expiration policy will allow S/ES to continue monitoring the accounts and modifying them manually to ensure no interruption in service and compliance with the relevant portions of the DS Security policy. The Department suggests that this



recommendation is resolved should be closed when the referenced policy is issued and referenced process is implemented.

Regarding users complete the required Cyber Security Awareness Training on an annual basis, the Department concurs with this recommendation and suggests that this recommendation is resolved and should be closed. S/ES will ensure all employees receive cyber security awareness training/briefings as required by The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.)

Rec. 16 has become Rec. 17 in the final report.

Recommendation 16. We recommend that the Chief Information Office, in coordination with Information Resource Management/Information Assurance, continue to review the security authorization and annual assessments to ensure that Information System Owner, Information System Security Officer, and Security Control Assessor for all Federal Information Security Management Act reportable systems use the published Certification & Accreditation Toolkit templates during the annual controls assessment to assess the required National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* controls applicable and update the System Security Plan accordingly.

Management Response (November 2012): The Department asserts that the referenced practices and controls are being fully implemented, and therefore does not concur with this recommendation.

The Department suggests that this recommendation be closed.

Rec. 17 has become Rec. 18 in the final report.

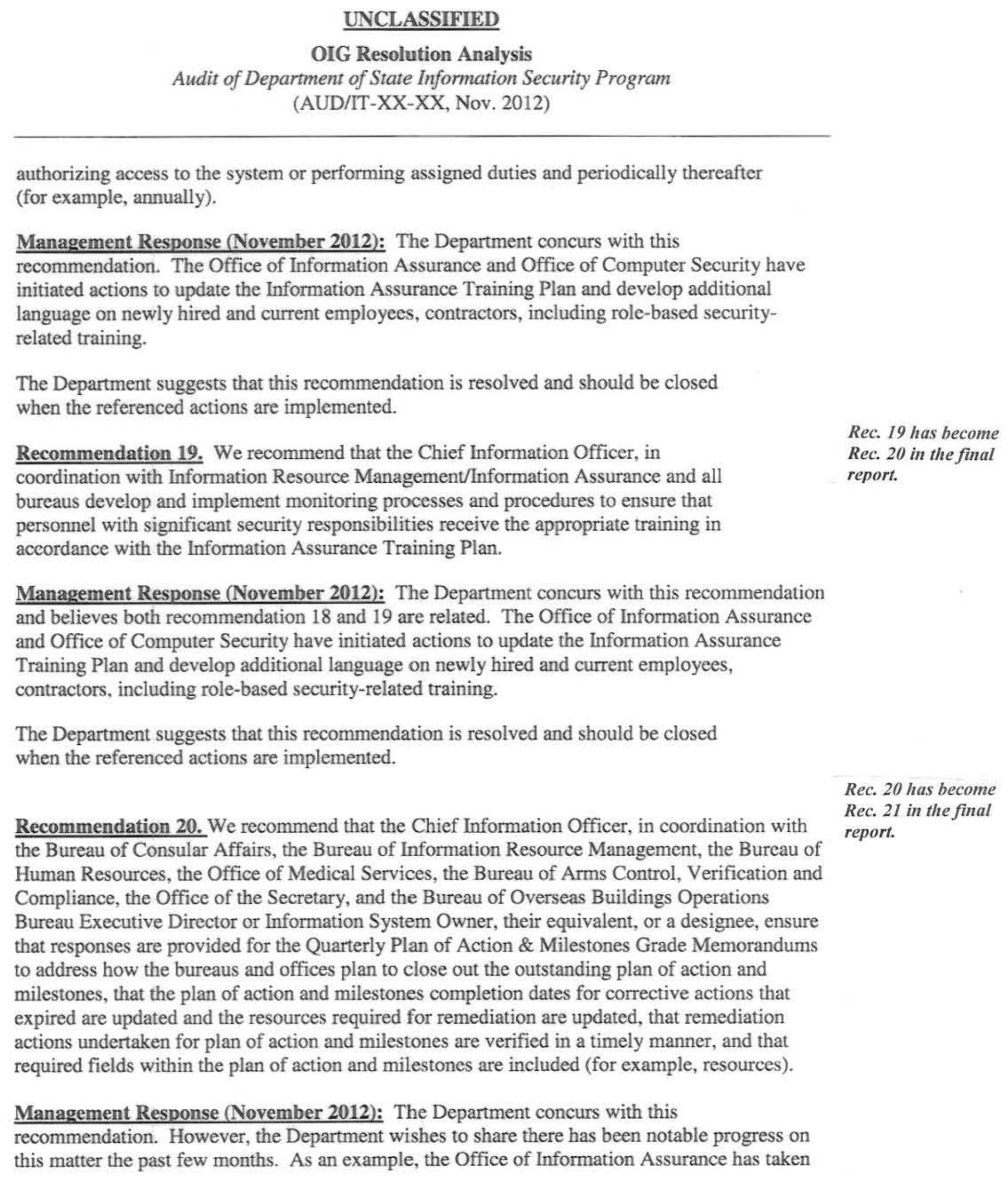
Recommendation 17. We recommend that the Chief Information Officer continue to track the progress of the full authorization of the OpenNet general support system.

Management Response (November 2012): The Department concurs with this recommendation. The Chief Information Officer, the Bureau of IRM's Office of Information Assurance, and the Office of Operations are all expending significant time and resources to ensure progress of the full authorization of the OpenNet general support system is occurring. Ongoing progress reports are submitted to the Chief Information Officer.

The Department suggests that this recommendation be closed.

Rec. 18 has become Rec. 19 in the final report.

Recommendation 18. We recommend that the Chief Information Officer, in coordination with Information Resource Management/Information Assurance and Office of Computer Security (Diplomatic Security/Systems Integrity/Civil Service), update the Information Assurance Training Plan to require newly hired and current employees and contractors who are in positions that are responsible for the security of the organization's information and information systems complete role-based security-related training before



UNCLASSIFIED

OIG Resolution Analysis

Audit of Department of State Information Security Program

(AUD/IT-XX-XX, Nov. 2012)

authorizing access to the system or performing assigned duties and periodically thereafter (for example, annually).

Management Response (November 2012): The Department concurs with this recommendation. The Office of Information Assurance and Office of Computer Security have initiated actions to update the Information Assurance Training Plan and develop additional language on newly hired and current employees, contractors, including role-based security-related training.

The Department suggests that this recommendation is resolved and should be closed when the referenced actions are implemented.

Rec. 19 has become Rec. 20 in the final report.

Recommendation 19. We recommend that the Chief Information Officer, in coordination with Information Resource Management/Information Assurance and all bureaus develop and implement monitoring processes and procedures to ensure that personnel with significant security responsibilities receive the appropriate training in accordance with the Information Assurance Training Plan.

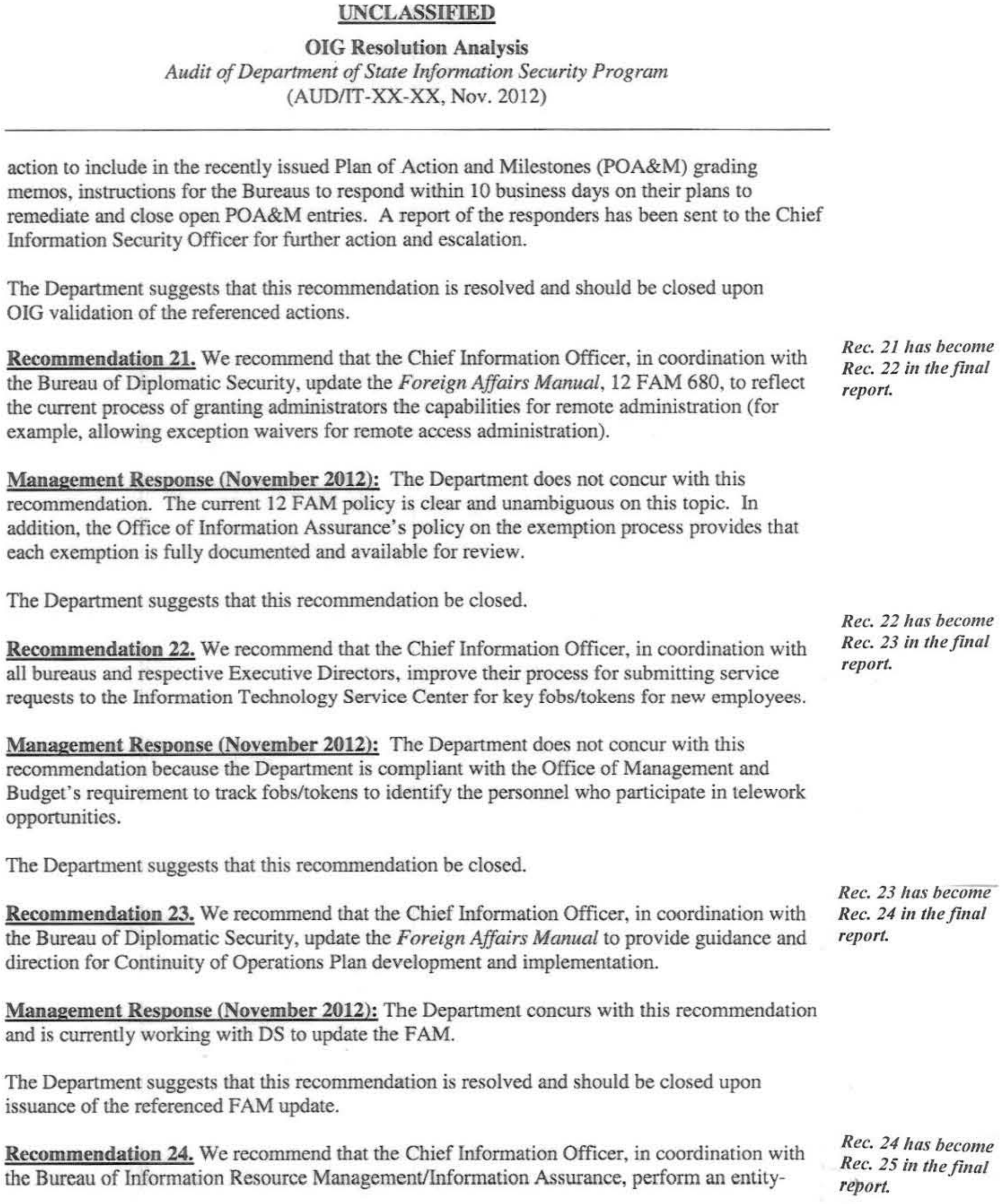
Management Response (November 2012): The Department concurs with this recommendation and believes both recommendation 18 and 19 are related. The Office of Information Assurance and Office of Computer Security have initiated actions to update the Information Assurance Training Plan and develop additional language on newly hired and current employees, contractors, including role-based security-related training.

The Department suggests that this recommendation is resolved and should be closed when the referenced actions are implemented.

Rec. 20 has become Rec. 21 in the final report.

Recommendation 20. We recommend that the Chief Information Officer, in coordination with the Bureau of Consular Affairs, the Bureau of Information Resource Management, the Bureau of Human Resources, the Office of Medical Services, the Bureau of Arms Control, Verification and Compliance, the Office of the Secretary, and the Bureau of Overseas Buildings Operations Bureau Executive Director or Information System Owner, their equivalent, or a designee, ensure that responses are provided for the Quarterly Plan of Action & Milestones Grade Memorandums to address how the bureaus and offices plan to close out the outstanding plan of action and milestones, that the plan of action and milestones completion dates for corrective actions that expired are updated and the resources required for remediation are updated, that remediation actions undertaken for plan of action and milestones are verified in a timely manner, and that required fields within the plan of action and milestones are included (for example, resources).

Management Response (November 2012): The Department concurs with this recommendation. However, the Department wishes to share there has been notable progress on this matter the past few months. As an example, the Office of Information Assurance has taken



action to include in the recently issued Plan of Action and Milestones (POA&M) grading memos, instructions for the Bureaus to respond within 10 business days on their plans to remediate and close open POA&M entries. A report of the responders has been sent to the Chief Information Security Officer for further action and escalation.

The Department suggests that this recommendation is resolved and should be closed upon OIG validation of the referenced actions.

Recommendation 21. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, update the *Foreign Affairs Manual*, 12 FAM 680, to reflect the current process of granting administrators the capabilities for remote administration (for example, allowing exception waivers for remote access administration).

Rec. 21 has become Rec. 22 in the final report.

Management Response (November 2012): The Department does not concur with this recommendation. The current 12 FAM policy is clear and unambiguous on this topic. In addition, the Office of Information Assurance's policy on the exemption process provides that each exemption is fully documented and available for review.

The Department suggests that this recommendation be closed.

Recommendation 22. We recommend that the Chief Information Officer, in coordination with all bureaus and respective Executive Directors, improve their process for submitting service requests to the Information Technology Service Center for key fobs/tokens for new employees.

Rec. 22 has become Rec. 23 in the final report.

Management Response (November 2012): The Department does not concur with this recommendation because the Department is compliant with the Office of Management and Budget's requirement to track fobs/tokens to identify the personnel who participate in telework opportunities.

The Department suggests that this recommendation be closed.

Recommendation 23. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, update the *Foreign Affairs Manual* to provide guidance and direction for Continuity of Operations Plan development and implementation.

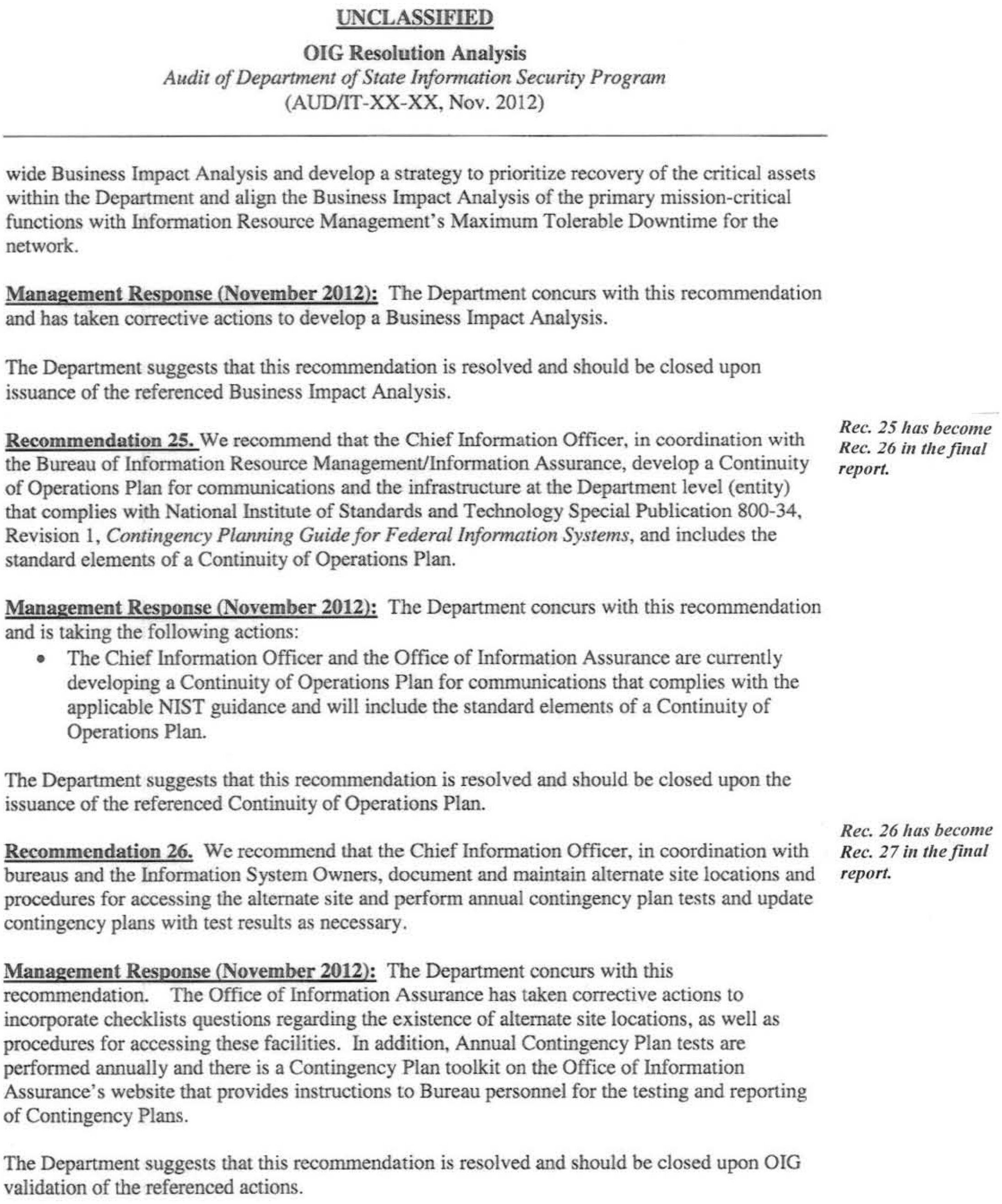
Rec. 23 has become Rec. 24 in the final report.

Management Response (November 2012): The Department concurs with this recommendation and is currently working with DS to update the FAM.

The Department suggests that this recommendation is resolved and should be closed upon issuance of the referenced FAM update.

Recommendation 24. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, perform an entity-

Rec. 24 has become Rec. 25 in the final report.



wide Business Impact Analysis and develop a strategy to prioritize recovery of the critical assets within the Department and align the Business Impact Analysis of the primary mission-critical functions with Information Resource Management's Maximum Tolerable Downtime for the network.

Management Response (November 2012): The Department concurs with this recommendation and has taken corrective actions to develop a Business Impact Analysis.

The Department suggests that this recommendation is resolved and should be closed upon issuance of the referenced Business Impact Analysis.

Recommendation 25. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, develop a Continuity of Operations Plan for communications and the infrastructure at the Department level (entity) that complies with National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, and includes the standard elements of a Continuity of Operations Plan.

Rec. 25 has become Rec. 26 in the final report.

Management Response (November 2012): The Department concurs with this recommendation and is taking the following actions:

- The Chief Information Officer and the Office of Information Assurance are currently developing a Continuity of Operations Plan for communications that complies with the applicable NIST guidance and will include the standard elements of a Continuity of Operations Plan.

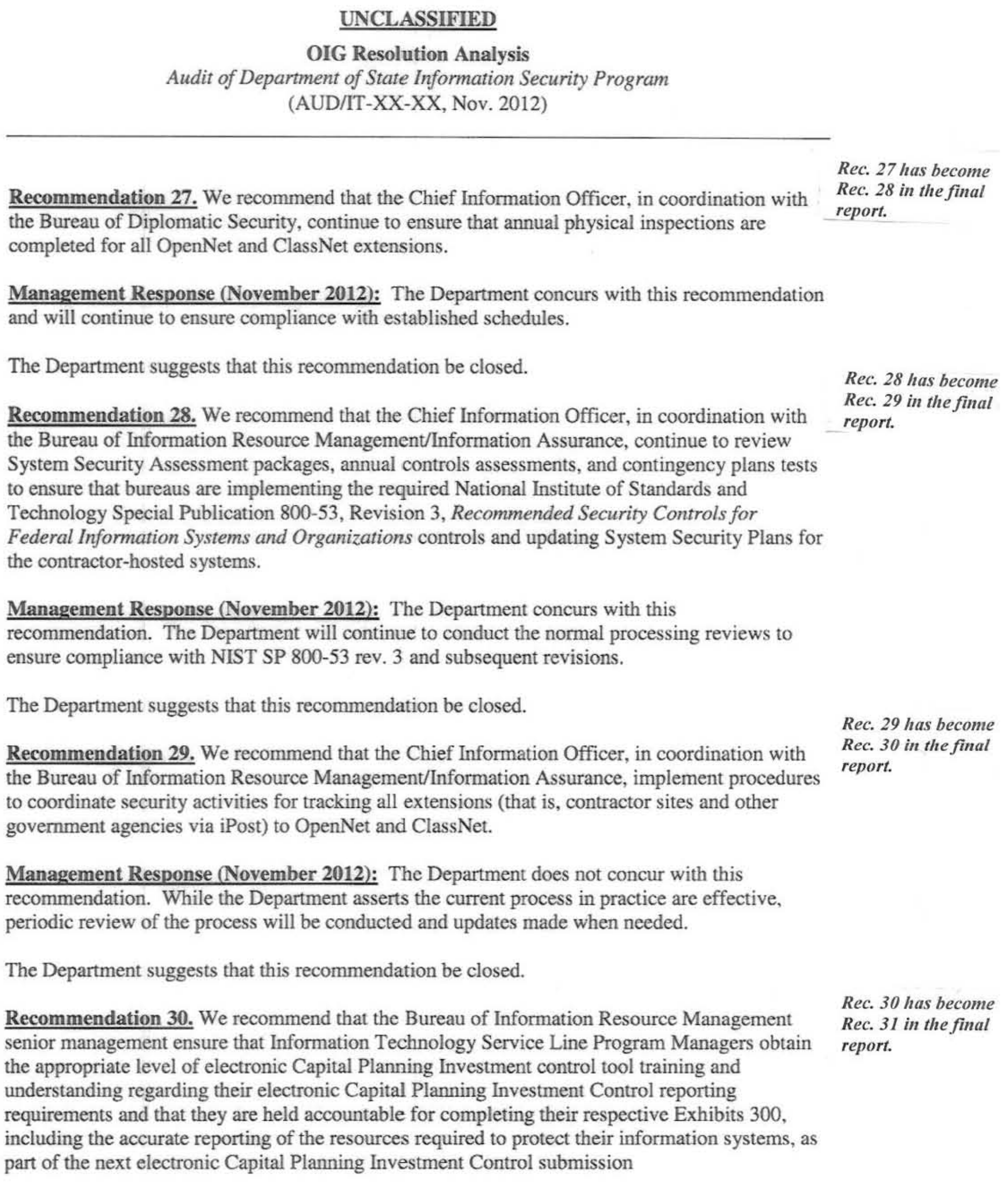
The Department suggests that this recommendation is resolved and should be closed upon the issuance of the referenced Continuity of Operations Plan.

Recommendation 26. We recommend that the Chief Information Officer, in coordination with bureaus and the Information System Owners, document and maintain alternate site locations and procedures for accessing the alternate site and perform annual contingency plan tests and update contingency plans with test results as necessary.

Rec. 26 has become Rec. 27 in the final report.

Management Response (November 2012): The Department concurs with this recommendation. The Office of Information Assurance has taken corrective actions to incorporate checklists questions regarding the existence of alternate site locations, as well as procedures for accessing these facilities. In addition, Annual Contingency Plan tests are performed annually and there is a Contingency Plan toolkit on the Office of Information Assurance's website that provides instructions to Bureau personnel for the testing and reporting of Contingency Plans.

The Department suggests that this recommendation is resolved and should be closed upon OIG validation of the referenced actions.



UNCLASSIFIED

OIG Resolution Analysis
Audit of Department of State Information Security Program
(AUD/IT-XX-XX, Nov. 2012)

Rec. 27 has become Rec. 28 in the final report.

Recommendation 27. We recommend that the Chief Information Officer, in coordination with the Bureau of Diplomatic Security, continue to ensure that annual physical inspections are completed for all OpenNet and ClassNet extensions.

Management Response (November 2012): The Department concurs with this recommendation and will continue to ensure compliance with established schedules.

The Department suggests that this recommendation be closed.

Rec. 28 has become Rec. 29 in the final report.

Recommendation 28. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, continue to review System Security Assessment packages, annual controls assessments, and contingency plans tests to ensure that bureaus are implementing the required National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* controls and updating System Security Plans for the contractor-hosted systems.

Management Response (November 2012): The Department concurs with this recommendation. The Department will continue to conduct the normal processing reviews to ensure compliance with NIST SP 800-53 rev. 3 and subsequent revisions.

The Department suggests that this recommendation be closed.

Rec. 29 has become Rec. 30 in the final report.

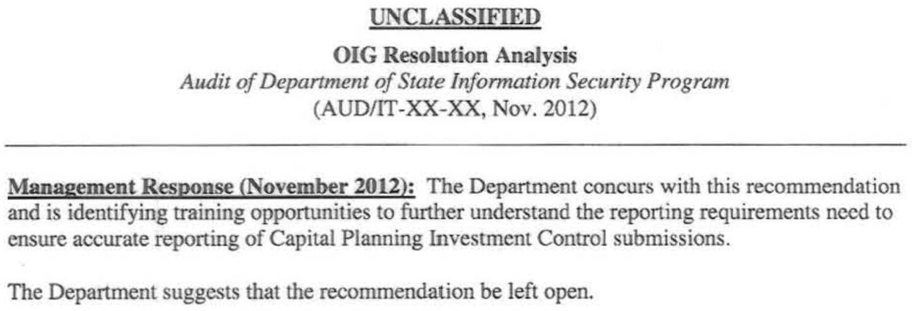
Recommendation 29. We recommend that the Chief Information Officer, in coordination with the Bureau of Information Resource Management/Information Assurance, implement procedures to coordinate security activities for tracking all extensions (that is, contractor sites and other government agencies via iPost) to OpenNet and ClassNet.

Management Response (November 2012): The Department does not concur with this recommendation. While the Department asserts the current process in practice are effective, periodic review of the process will be conducted and updates made when needed.

The Department suggests that this recommendation be closed.

Rec. 30 has become Rec. 31 in the final report.

Recommendation 30. We recommend that the Bureau of Information Resource Management senior management ensure that Information Technology Service Line Program Managers obtain the appropriate level of electronic Capital Planning Investment control tool training and understanding regarding their electronic Capital Planning Investment Control reporting requirements and that they are held accountable for completing their respective Exhibits 300, including the accurate reporting of the resources required to protect their information systems, as part of the next electronic Capital Planning Investment Control submission



UNCLASSIFIED

OIG Resolution Analysis

Audit of Department of State Information Security Program

(AUD/IT-XX-XX, Nov. 2012)

Management Response (November 2012): The Department concurs with this recommendation and is identifying training opportunities to further understand the reporting requirements need to ensure accurate reporting of Capital Planning Investment Control submissions.

The Department suggests that the recommendation be left open.

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