



Office of Inspector General

UNCLASSIFIED

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

**Office of Audits**

**Evaluation of Department of State  
Information Security Program**

**Report Number AUD/IT-12-14, November 2011**

**~~Important Notice~~**

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

UNCLASSIFIED



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 a review of the Department of State Information Security Program for FY 2011. To perform this review, 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, 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.

A handwritten signature in black ink, appearing to read "H. W. Geisel", written in a cursive style.

Harold W. Geisel  
Deputy Inspector General

**UNCLASSIFIED**



Evaluation of Department of State Information Security Program

November 7, 2011

Office of Inspector General  
U.S. Department of State  
2201 C St., NW  
Washington, D.C. 20520

Williams, Adley & Company, LLP (referred to as “we” in this letter), is pleased to provide the Office of Inspector General (OIG) the results of the evaluation of the Department of State (Department) Information Security Program for FY 2011. We evaluated the Department’s Information Security Program performance in compliance with the Federal Information Security Management Act, Office of Management and Budget (OMB), and National Institute of Standards and Technology regulations, standards, and requirements. Additionally, the evaluation was performed to provide sufficient support for OIG in providing responses to OMB in accordance with OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

This evaluation, performed under Contract No. SAQMMA10F2159, was designed to meet the objectives identified in Appendix A, “Objectives, Scope, and Methodology,” of the report. We communicated the results of our review and the related findings and recommendations to the Department’s management.

We appreciate the cooperation provided by Department personnel during the evaluation. Should you have any questions, or if we can be of further assistance, please contact either [REDACTED]

(b) (6)

*Williams Adley & Company, LLP*

WILLIAMS, ADLEY & COMPANY-DC, LLP  
Certified Public Accountants / Management Consultants  
1030 15<sup>th</sup> Street, NW, Suite 300W • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161  
[www.williamsadley.com](http://www.williamsadley.com)

**UNCLASSIFIED**

**UNCLASSIFIED**

---

**Acronyms**

AD	Active Directory
ATO	Authority to Operate
BEAP	Bureau Emergency Action Plan
BIA	Business Impact Assessment
BIMC	Beltsville Information Management Center
CCP	COOP Communications Plan
CIO	Chief Information Officer
CM	Configuration Management
CMS	Content Management System
CNSS	Committee on National Security Systems
COCO	Contractor Owned Contractor Operated
COOP	Continuity of Operations Plan
CP	Contingency Plan
CPIC	Capital Planning and Investment Control
CPM	Central Patch Management
CVE	Common Vulnerability Exposure
Department	U.S. Department of State
DHS	Department of Homeland Security
DS	Bureau of Diplomatic Security
DS/EV	Diplomatic Security/Enterprise Vulnerability
DS/SI/CS	Diplomatic Security/Security Infrastructure/Office of Computer Security
ENM	IRM/Enterprise Network Management
ESOC	Enterprise Service Operation Center
FAM	Foreign Affairs Manual
FCD	Federal Continuity Directive
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTE	full time equivalent
GAO	Government Accountability Office
GSS	General Support System
IA	Information Assurance
IBWC	International Boundary and Water Commission
IRM/ENM	Bureau of Information Resource Management, Enterprise Network Management
IRM/IA	Bureau of Information Resource Management, Office of Information Assurance
ISCP	Information System Contingency Plan
ISP	Internet Service Provider
ISSC	Information Security Steering Committee
ISSO	Information System Security Officer

**UNCLASSIFIED**

**UNCLASSIFIED**

IT	information technology
ITAB	Information Technology Asset Baseline
ITSP	Information Technology Strategic Plan
MSDC	Main State Data Center
NIST	National Institute of Standards and Technology
OEM	Office of Emergency Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONE	OpenNet Everywhere
PB	Program Board
PIA	Privacy Impact Assessment
PMEF	Primary Mission Essential Functions
POA&M	Plans of Action and Milestones
RBAC	Role Based Access Controls
RMF	Risk Management Framework
SARs	Security Assessment Reports
SMART	State Messaging and Archive Retrieval Toolset
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan
SSR	Significant Security Responsibilities
TDS	DOS Telegram Delivery
UPI	Unique Project Identifier
USEVI	United States Embassy Vienna Internet
WEBPASS	Web Post Administrative Software Suite
WINAD	OpenNet Windows Active Directory

**UNCLASSIFIED**

**Table of Contents**

**EXECUTIVE SUMMARY .....1**

**BACKGROUND .....6**

**RESULTS OF REVIEW .....7**

**A. RISK MANAGEMENT FRAMEWORK NEEDS IMPROVEMENT .....7**

**B. SECURITY CONFIGURATION MANAGEMENT NEEDS IMPROVEMENT .....11**

**C. INFORMATION SECURITY TRAINING REQUIREMENTS WERE NOT ENFORCED .....13**

**D. PLANS OF ACTION AND MILESTONES ARE NOT EFFECTIVE .....15**

**E. ACCOUNT MANAGEMENT PROCESSES IN ACTIVE DIRECTORY NEED TO BE IMPROVED .....17**

**F. THE USER PROVISIONING PROCESS FOR CREATING, MODIFYING, AND DISABLING USERS' ACCOUNTS REQUIRES SIGNIFICANT IMPROVEMENT .....19**

**G. CONTINUOUS MONITORING PROGRAM NEEDS TO BE IMPROVED .....21**

**H. THE CONTINUITY OF OPERATIONS PROGRAM NEEDS TO BE IMPROVED .....24**

**I. INFORMATION SYSTEM CONTINGENCY PLANS NEEDS TO BE IMPROVED .....26**

**J. OVERSIGHT OF CONTRACTOR SYSTEMS AND EXTENSIONS NEEDS IMPROVEMENT .....29**

**K. CAPITAL PLANNING REQUIRES IMPROVEMENT .....31**

**LIST OF CURRENT YEAR RECOMMENDATIONS .....36**

**APPENDIX A. OBJECTIVES, SCOPE, AND METHODOLOGY .....41**

**APPENDIX B. FOLLOWUP OF RECOMMENDATIONS FROM THE FY 2010 FISMA REPORT .....44**

**APPENDIX C. SYSTEMS WITH INVALID AUTHORITY TO OPERATE .....47**

**APPENDIX D. SYSTEMS WITH OUTDATED SECURITY BASELINE CONTROLS .....48**

**APPENDIX E. VULNERABILITY ASSESSMENT .....50**

**UNCLASSIFIED**

**APPENDIX F. SYSTEMS WITHOUT ANNUAL BACKUP PLAN TESTING .....55**

**APPENDIX G. SERVERS WITHOUT CRITICAL PATCHES .....56**

**APPENDIX H. SUMMARY OF DEPARTMENT OF STATE’S CONTINUOUS  
MONITORING CONTROLS COMPLIANCE WITH FEDERAL GUIDANCE....57**

**APPENDIX I. SAMPLE SELECTION OF INFORMATION SYSTEMS LISTED IN  
INFORMATION TECHNOLOGY ASSET BASELINE USED FOR FY2011  
EVALUATION .....59**

**APPENDIX J. DEPARTMENT OF STATE RESPONSE .....61**

## **Executive Summary**

In accordance with the Federal Information Security Management Act of 2002 (FISMA),<sup>1</sup> the Office of Inspector General (OIG) contracted with Williams, Adley & Company, LLP (referred to as “we” in this report), to perform an independent evaluation 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 OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

Overall, we found that the Department had implemented an information security program, but we identified weaknesses that significantly impact the information security program controls. If these control weaknesses are exploited, the Department could be exposed to additional security breaches. Collectively, these control weaknesses represent a significant deficiency, as defined by the Office of Management and Budget M-11-33, 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 taken corrective action to remediate all of the control weaknesses identified in the FY2010 FISMA report. 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 following control weaknesses:

### **A. Risk Management Program**

The Department’s risk management program for information security needs improvement at both the organization and the system levels. At the organizational level, the Department had not implemented an effective risk management strategy, and the Information Security Steering Committee (ISSC) did not meet during the fiscal year. At the system level, we noted several deficiencies in the Department’s documentation in the security assessment and authorization packages. More importantly, the security authorization process was not properly managed for nine of 30 of the Department’s information systems, including extensions for security authorizations (formerly authority to operate [ATO]) on the Department’s primary general support systems (GSS) for classified and unclassified systems. These deficiencies weaken the Department’s risk management framework and its ability to assess, respond to, and monitor information security risk.

### **B. Security Configuration Management**

Although the Chief Information Officer (CIO) is 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

---

<sup>1</sup> Public Law No. 107-347, title III.

## UNCLASSIFIED

patches within required timeframes and enabling mandatory security settings from the Bureau of Diplomatic Security (DS) Configuration Guidelines.

### **C. Security Awareness and Role-Based Training**

The Department needs to improve its process and procedures for general information security awareness and role-based training. The Department is not tracking and documenting Significant Security Responsibilities (SSR) training attendance. The evaluation found that nine of 30 employees and contractors hired during FY 2011 had not taken the PS800 training (general security awareness training) within 10 days after being hired. Additionally, five of 30 Department information system users had not taken the annual PS800 training.

### **D. Plans of Action and Milestones**

The Department's Plans of Actions and Milestones (POA&M) process had not been fully and effectively implemented, and the program is not compliant with FISMA and OMB requirements. The Department had not implemented a POA&M process to address and resolve security weaknesses identified on the ClassNet GSS. In addition, the evaluation found the Department had not implemented effective corrective actions to address the POA&M control weaknesses within the OpenNet GSS identified in the FY 2010 FISMA report on the Department's information security program.

### **E. Account and Identity Management Program**

The Department needs to improve account management processes in Active Directory<sup>2</sup> (AD) for OpenNet and ClassNet. From a population of approximately 128,000 OpenNet Active Directory user accounts, we identified approximately 400 guest, test, and temporary accounts; 9,000 accounts that had not been used (never logged on); 400 accounts with passwords set "not to expire"; and 300 Install Accounts.<sup>3</sup> Then, from a population of approximately 36,000 ClassNet AD accounts, we identified approximately 200 guest, test, and temporary accounts; 4,000 accounts that had not been used (never logged on); 900 accounts with passwords set "not to expire"; and 200 software installation accounts (Install Accounts).

### **F. User Provisioning Process**

The Department's user provisioning process for creating, modifying, and disabling users' accounts is not in compliance with the Department's *Foreign Affairs Manual* (FAM). The Department did not require two of 25 ClassNet Domain Administrators' accounts to have individual user accounts, which may result in Domain Administrators' accounts being used for non-administrator functions and susceptible to cyber attacks. The Department had not removed in a timely manner 294 of 894

---

<sup>2</sup> Active Directory is a technology created by Microsoft that provides a variety of network services such as identification and authentication, directory access, and other network services.

<sup>3</sup> Install accounts are those accounts created for Department of State personnel to install software within the different domains (for the bureaus and offices).

## UNCLASSIFIED

accounts for separated Full Time Equivalent employee accounts, and 104 of those accounts had Department issued security tokens<sup>4</sup> for remote access. Documentation (Password/Receipt Form) had not been received for all of 25 new user accounts created within the past fiscal year and documentation had not been received for all seven Network Administrators' accounts created within the past fiscal year. The Department permitted one of 25 OpenNet Domain Administrators/Administrators' accounts to be used as a group account.

These control weaknesses increase the potential that unauthorized activities can occur without timely detection, which adversely impacts confidentiality, integrity, and availability of the data on OpenNet and ClassNet.

### **G. Continuous Monitoring**

The Department does not have an effective means of implementing continuous monitoring at the organization level or the system level, and the Department had not taken action to resolve the continuous monitoring control weaknesses identified in the FY 2010 FISMA report on the Department's information security program. The ISSC had not developed a formal continuous monitoring strategy that addresses framing risk, assessing risk, responding to risk, and monitoring risk, all of which are required by NIST Special Publication (SP) 800-39, *Managing Information Security Risk*.

Also, based on our review of the actions taken by the Department regarding weaknesses identified in the FY 2010 FISMA report on the Department's information security program, we found the following repeat deficiencies:

- 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;<sup>5</sup> therefore, the results were not used in risk scoring.

### **H. The Continuity of Operations Program Needs to Be Improved**

The Department's Continuity of Operations Program is not operating effectively and is not documented in accordance with NIST SP 800-34 and Federal Continuity Directive (FCD)-2. 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.

---

<sup>4</sup> A token (sometimes called a security token) is an object that controls access to a digital asset. It is a small device used in a networked environment to create a one-time password that the owner enters into a login screen along with a user identification and a personal identification number.

<sup>5</sup> 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.

## **UNCLASSIFIED**

We found that the Continuity of Operations Plan (COOP) Communication Plan (CCP) for emergency communications and the network had not been updated with significant changes since 2008. The COOP CCP was not updated in accordance with NIST SP 800-34 because the Bureau of Information Resource Management (IRM) is focused on the Bureau Emergency Action Plan (BEAP) instead of the COOP CCP that contributes to the continuation of communications and the network for the entire Department.

### **I. Information Systems Contingency Planning**

The Department needs to improve the information system contingency planning program. An effective contingency planning program is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability.

From a sample of 25 information system contingency plans tested, we found several deficiencies. For example, three systems' (OpenNet, WebPass, and TDS) Contingency Plans did not document the alternate recovery site information.

### **J. Oversight of Contractor Systems**

The Department had not implemented an effective oversight program of its contractor systems and contractor extensions. All five Contractor-Owned Contractor-Operated (COCO) systems reviewed did not have contract agreements or security-related documentation available for review. For four of five COCO systems, IRM did not provide ATO memorandums after several requests.

We also found that the Department did not have an effective mechanism in place to identify the total number of contractors' personnel who had access to and privileges within the Department's network, applications, databases, and data.

### **K. Capital Planning**

Information security is not fully integrated into the Department's Capital Planning and Investment Control (CPIC) process. IRM needs to strengthen its oversight process of information technology (IT) investments. For four of 10 appropriated IT security investments reviewed, the Department did not provide evidence of documentation showing obligations and expenditures. The Department does not provide OMB with all investments that have significant dependency for the IT Infrastructure major investment. For a sample of 10 non-major investments that make up the IT Infrastructure major investment, we found that none of the 10 were identified as required by OMB in Exhibit 300.

Also, IT security costs from the Department's POA&Ms are not captured in the capital planning process. Specifically, Department implementation of the POA&M process does not reflect the unique project identifiers (UPI), which tie security correction action plans into the CPIC process. The lack of integration between the POA&M process and capital planning process negatively affects the funding prioritization

## UNCLASSIFIED

among the IT investments. Ultimately, inadequate oversight increases the risk of unapproved investments being funded.

Although this report contains 19 recommendations to the Department, 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).

We reviewed the Department's remedial actions taken to address the 2010 reported information security program control weaknesses identified in the FY 2010 FISMA report *Review of the Information Security Program at the Department of State* (AUD/IT-11-07, November 2010). (The statuses of the recommendations from the FY 2010 review of the information security program are in Appendix B.) Since FY 2010, the Department has taken actions to improve management controls to include the following:

- Updated and verified the FISMA systems inventory list to the Information Technology Asset Baseline (ITAB) to ensure that all information technology (IT) systems are accurately accounted for.
- Defined and identified personnel who have significant security responsibilities in its Information Assurance (IA) Training Plan.
- Ensured that personally identifiable information (PII) data incidents are reported to the U.S. Computer Emergency Response Team within the required 1-hour timeframe.
- Updated its contracts to include Department of State Acquisition Regulations information security language.

**Management Comments.** In its November 2, 2011, response to the draft report (see Appendix J), the Department stated that it “disagrees” on whether continuous monitoring, as currently conducted, produces a lower risk than a traditional C&A program, and on the relative importance of completeness and compliance vs. timeliness and risk-based prioritization.” The Department further stated, “Having carefully considered these factors, the Department is convinced its continuous monitoring program, which is 300 times more timely than traditional three-year reauthorizations, produces significantly lower security risk [Department footnote states: “Neither produce zero risk, and achieving zero risk in not foreseeable.”] on its networks.”

Although OIG agrees that the continuous monitoring concept, if properly implemented and documented, allows for more rapid identification of security weaknesses, OIG is unable to provide an opinion on the effectiveness of the continuous monitoring strategy because the Bureau of Information Resource Management (IRM) did not provide a strategy, but the concept of continuous monitoring is designed to provide results in a more timely fashion. The collective weaknesses in the information security program, including IRM's lack of strategies for risk management and continuous monitoring, leave a weakness in the approach to assessing risk and taking actions to correct identified vulnerabilities. Furthermore, IRM's approach cannot establish responsibility and accountability for information systems security controls and leaves a vacuum between the current state of information security controls and any planned

## **UNCLASSIFIED**

improvements regarding the protection of the Department's information and information systems, because the Department relies heavily on iPost results to determine the current security posture of information systems and to initiate corrective actions. However, IRM could not provide documentation to support the strategy used or present historical or trend analysis during the annual evaluation. OIG identified weaknesses that should have been addressed or corrected based on the approach IRM presented verbally during the course of the FISMA evaluation. The identification of account management weaknesses by OIG's FISMA and financial statement auditors, the failure to install critical patches on servers, and the increasing trend of Common Vulnerabilities and Exposures (CVE) since 2007 indicates that the approach in place is not addressing information security risks in the Department's information and information systems.

In its response to the report's 19 recommendations, the Department generally agreed or agreed with portions of 10 recommendations, did not agree with five recommendations, and did not indicate agreement or disagreement with four recommendations. Based on the response, OIG considers 10 recommendations resolved, pending further action, and nine recommendations unresolved.

Management's responses to the recommendations and OIG's analyses of the responses are presented after each recommendation. Also, OIG has provided additional comments to the Department's response in the section "Management Comments and OIG Analyses."

### **Background**

FISMA 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 information technology (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.

## UNCLASSIFIED

On an annual basis, OMB provides guidance with reporting categories and questions for meeting the current year's reporting requirements.<sup>6</sup> OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

### **Results of Review**

Overall, we found that the Department had implemented an information security program, but we identified weaknesses that significantly impact the information security program controls. If these control weaknesses are exploited, the Department could be exposed to additional security breaches. Collectively, these control weaknesses represent a significant deficiency, as defined by the Office of Management and Budget M-11-33, 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 FY2010 FISMA report. 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 following control weaknesses:

#### **A. Risk Management Framework Needs Improvement**

The Department needs to improve its risk management program for information security at both the organization and the system levels. We found that the Department had not taken adequate remedial actions to resolve control weaknesses reported in the FY 2010 OIG FISMA report and that the Department continues to experience control deficiencies at both the organizational and information systems levels of the Risk Management Framework (RMF). The RMF is important because NIST SP 800-37<sup>7</sup> requires an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy, instead of sole reliance on security authorizations at the system level.

At the organizational level, the Department had not implemented an effective risk management strategy addressing how it intends to assess, respond to, and monitor information security risk as required by NIST 800-39.<sup>8</sup> As of June 30, 2011, the ISSC,<sup>9</sup> a key component of the Department's cyber security governance structure, had not met during FY 2011. The committee chose to meet only during emergency events and not regularly, as specified in its charter. Key members of the ISSC consist of the Chief Information Security Officer, the Senior Coordinator for Security Infrastructure; Co-Executive Secretaries from the Office Information Resource Management/Information Assurance/Policy Liaison and Reporting (IRM/IA/PLR) and

---

<sup>6</sup> OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated Sept.14, 2011.

<sup>7</sup> NIST SP 800-37, rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Feb. 2010.

<sup>8</sup> NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

<sup>9</sup> According to the ISSC charter, members will meet on a monthly basis; more or less frequent meetings may be scheduled at the request of any member, given a majority agreement of the ISSC. Among its responsibilities, the ISSC shall: (a) Develop priorities and determine availability of resources for security of Department information systems; (b) coordinate strategic direction of the Department's information security efforts; and (c) support Department funding and budget mechanisms as they relate to information security.

**UNCLASSIFIED**

Diplomatic Security/Security Infrastructure/Office of Computer Security (DS/SI/CS), and permanent bureau members. Further, because the risk management strategy had not been fully implemented at the organizational level, communication of operations at the system level is negatively affected, along with business decisions such as funding allocation, because management is not fully aware of security vulnerabilities that exist.

At the information system level, we found deficiencies in the Security Assessment and Authorization documentation (formerly Certification & Accreditation) as follows:

1. For the authorities to operate (ATO), which provide proof that an authorizing official has accepted the identified risk, we found that nine of 30 systems (see Appendix I) tested did not have a full security assessment and authorization performed. The most notable examples identified were that the designated approving authority provided only memorandums granting extensions of ATOs for OpenNet and ClassNet general support systems (GSS) rather than completing a full security assessment and authorization. Because the OpenNet system did not have a legitimate ATO for the unclassified systems, we requested the ClassNet ATO for the classified systems. OMB<sup>10</sup> requires agencies to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. However, we found control deficiencies in the Department's continuous monitoring program (see Finding G - Continuous Monitoring Program Needs To Be Improved). The nine systems, in addition to ClassNet, where the ATOs were not valid, not available or outdated, are presented in Appendix C.
2. For thirty System Security Plans (SSP) tested, which document the security controls for the system, we found the following:
  - The security baseline controls for 24 systems had not been updated to comply with NIST SP 800-53 Revision 3,<sup>11</sup> (see Appendix D).
  - Four systems' SSPs (OpenNet Transport, OpenNet Windows Active Directory [WINAD], Extranet, and the United States Embassy Vienna Internet [USEVI]) had not been updated within 3 years or updated because of a major change, as required by OMB Circular A-130 Appendix III and NIST SP 800-37.
3. For thirty Security Assessment Reports (SAR) supporting the independent assessor's evaluation of management, operational, and technical controls, we found the following:
  - For five systems (OpenNet, Windows Active Directory [WINAD], Extranet, USEVI, and the Web Post Administrative Application Software Suite [WebPASS]), the SAR either was not available or was outdated.
  - Two systems (WebPASS and State Messaging and Archiving Retrieval Tool – Classified [SMART-C]) did not have an annual assessment of security controls performed as part of their continuous monitoring of annual controls.

---

<sup>10</sup> OMB Memorandum M-11-33.

<sup>11</sup> NIST SP 800-53, rev.3, *Recommended Security Controls for Information Systems*, Aug. 2009.

## UNCLASSIFIED

The Department did not properly follow NIST SP 800-37 guidelines for properly managing the documentation included in the security assessment and authorization packages. Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), officials stated that they were aware that the contents were sometimes outdated or were unavailable but explained that the USEVI Web site has a foreign IP address that does not belong to the Department. The officials acknowledged, however, that OIG had informed them that USEVI needs to be included in their system inventory.

At the system level, not performing the security assessment and authorization for OpenNet and ClassNet is a vulnerability that not only could eventually lead to a threat for these systems but also for all other GSSs and major applications that are dependent on common controls from ClassNet and OpenNet.

**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.

**Management Response:** The Department did not agree with this recommendation, stating that the lack of meetings does not pose a material risk to Department security. The Department further stated: “Moreover, there is no requirement that this voluntarily created internal group [ISSC] meet with recurring frequency. The Department exercised its valid authority [OMB Memorandum 11-33] to conclude there was no need to meet . . . The ISSC chairpersons will survey the ISSC membership on reasons to meet, and conduct meetings accordingly.”

**OIG Analysis:** OIG considers this recommendation unresolved. The Department’s ISSC charter states that the committee will meet on a monthly basis. Further, OIG is of the opinion that the ISSC should meet on a more frequent basis to mitigate organizational vulnerabilities, as the cyber threat environment to the Department is dynamic. This recommendation can be resolved when the Department agrees to have the ISSC meet monthly to fulfill its purpose and responsibilities, as required in the ISSC charter.

**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.

**Management Response:** The Department stated that it “agree[d] that some increased level of documentation in this area could be beneficial” but noted that under OMB Memorandum M-11-33, “it is the Department’s judgment that shall decide how much documentation is needed to reduce risk.” The Department further stated that its “Designated Authorizing Authority . . . will determine the level of documentation adequate to manage risk.”

**OIG Analysis:** OIG considers this recommendation resolved. The recommendation can be closed when OIG reviews and accepts documentation showing that the Department has implemented a risk management strategy at the organizational level showing how the

## UNCLASSIFIED

Department's risk management strategy addresses how the Department will assess, respond to, and monitor information security risk.

**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) Special Publication (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.

**Management Response:** The Department did not agree with the recommendation, stating that based on OMB Memorandum M-11-33, security reauthorizations are not required every 3 years but through "ongoing authorizations" via implementation of a continuous monitoring program. The Department also did not agree that security assessments and authorizations had to be improved, stating that NIST SP 800-53 guidance "was not fully implemented until June 2010." The Department also stated that a "new NIST 800-53A was needed to implement the new 800-53, and was not published until June 2010." Therefore, according to the Department, "compliance was not required for C&As starting before June 2011" but, as of June 2011, the Department "will comply with the new version of NIST 800-53/53A." The Department further stated that its C&A Toolkit "has been fully updated to implement this change" and that it "performs such annual testing on all its systems, except in rare cases that are vigorously pursued."

**OIG Analysis:** OIG considers this recommendation unresolved. The evaluation of the Department's continuous monitoring program determined that several control deficiencies were identified (see Appendix H), therefore weakening the reliance on the continuous monitoring program. NIST SP 800-53, Revision 3, guidance was issued in August 2009, and OMB Memorandum M-11-33 states that "agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB." Although the Department stated that it had performed annual security assessments on all of its controls, testing results showed that the Department was not testing all of the security controls and could not support the control baselines necessary to define the testing level. This recommendation can be considered resolved when OIG reviews and accepts documentation showing that the Department has agreed to address these risk management recommendations and the actions it will take to address these actions.

## **B. Security Configuration Management Needs Improvement**

In FY 2011, we inquired about the progress of the Central Patch Management (CPM) project and the Initiative for End-to-End Configuration Management (CM) identified in the FY 2010 FISMA report on the Department's information security program. According to IRM/Operations/Enterprise Network Management (IRM/OPS/ENM) officials, the CPM project is in the deployment phase. Although the CIO is taking actions to address the prior year's weaknesses with the CM controls and IRM/OPS/ENM has set a patch installation benchmark rate of 100 percent, which is in accordance with the FAM,<sup>12</sup> we found the following deficiencies:

- Critical security patches were not installed within the required timeframes. From a sample of 25 Windows servers, we found that 17 servers did not have critical patches installed. (Details of missing critical patches are in Appendix G.)
- All mandatory security settings were not reported by iPost. The scan results are submitted to IRM/IA to upload to iPost. Based on our comparison of a sample of 25 mandatory security settings from the DS Configuration Guidelines (Windows 2003 and 2008) and the McAfee Foundstone Benchmarks, which are run by the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security, Enterprise Vulnerability Scanning (DS/SI/CS/EV) Branch, we found that the following settings were not enabled during the vulnerability scans:
  - Security Options: Network Access: Restrict anonymous access to named pipes and shares.
  - Securing System Services: DFS Replication.
  - Restricting Access to Windows Server 2003 System Folders.
  - Windows (2008) Update Services: PKI Interoperability.
- We performed a vulnerability analysis and identified 8,520 high risk deficiencies. Some of the deficiencies identified are as follows (the vulnerability analysis is in Appendix E):
  - Systems, operating systems, and applications with critical system and security patches that had not been applied by the Department.
  - Systems that did not meet the standards set forth in the DS System Configuration Policy and Procedures.
  - Systems that allowed access to system resources via anonymous logins and passwords, default credentials, and unsecured access points.

Responsibility for the implementation of CM controls for the systems, operating systems, databases, and network is distributed among the various system owners, database administrators, and network administrators without sufficient centralized governance controls to oversee

---

<sup>12</sup> 5 FAM 1067.3(b)(1), "Patch Management Compliance Program."

## UNCLASSIFIED

performance. For example, the Information System Security Officers (ISSO) have not established and implemented a reporting process to verify that the responsible groups have implemented the security configuration patches and software updates identified by DS and IRM. Although system owners are responsible for the systems' operations and compliance, DS and IRM did not establish reporting procedures to obtain, between each other, assurance that patches were actually installed. To correct these weaknesses, IRM/OPS/ENM is implementing the end-to-end CM initiative, which includes a standard operating environment to support development of effective CM plans for the computing environments commonly used throughout the Department.

Without effective configuration management controls, the Department increases the risks that Department-sensitive data, systems, and hardware may 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 CM 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 Department bureaus and system owners in a timely manner.

**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 initiatives 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.

**Management Response:** The Department stated the following:

In general, the OIG is using a criterion focused upon completeness, and overlooking timeliness. This is a "compliance-based" approach not consistent with FY2011 FISMA reporting instructions that require both the Department and OIG to assess risk and make judgments of how to best achieve security.

More specifically, the OIG asserts the Department is not checking 100% of configuration settings within the "required" three-year timeframe. Utilizing a risk-based approach, the Department is applying the analysis conducted by MIT Lincoln Labs examining the tradeoff between completeness and timeliness of testing. This study shows the following two conditions have approximately equal risk [Chart in Department response: "100% completeness every year = 17% completeness every two months"].

Because the Department checks nearly 90% of configuration settings every three days, the Department's risk is significantly lower than the traditional C&A requirement (100% completeness every three years). In this case, evidence shows timeliness trumps completeness in lowering risk.

## UNCLASSIFIED

The Department examined each of the three OIG findings and determined the findings do not reflect a material increase of risk for reasons documented elsewhere [Footnote in Department response: “Available for auditor inspection.”]. The Department will continue to assess risk in these areas, and if a material risk to the security of the Department is found, the Department will take appropriate steps.

**OIG Analysis:** OIG considers this recommendation unresolved. During the analysis of vulnerability scan results analysis, the evaluation determined that a total of 15,288 critical, high, medium, and low patches have not been applied for 16 general support systems/major applications. Further, there were critical patches that were 7 years overdue. For the 16 systems tested, the vulnerability scan results analyses displayed a rising trend of non-remediation of Common Vulnerabilities Exposures (CVE) since 2007, with some being identified as early as 1999. Thus there are vulnerabilities that have not been remediated and that can possibly threaten the security posture of the network infrastructure. (See Appendix E, “Vulnerability Assessments,” Table 4, “Total Number of Vulnerabilities by CVE and Year.”) This recommendation can be resolved, when the Department agrees to finalize and implement the elements within the Cyber Security Architecture draft target architecture and initiatives for end-to-end configuration management and take immediate action to correct or mitigate the high risk vulnerabilities identified by the vulnerability scanning.

### **C. Information Security Training Requirements Were Not Enforced**

The Department’s security training program needs to improve processes and procedures within the general information security awareness and role-based training. OMB<sup>13</sup> mandates agencies provide periodic computer security awareness to all users as well as specialized training for individuals who have significant security responsibilities. Training ensures that all users are knowledgeable of the rules of the system. In the FY 2010 FISMA report, OIG reported that the Department did not identify employees with significant security responsibilities (SSR).

The FY 2011 evaluation found that the Department had established controls to identify SSR positions and required role-based training in the IA Training Plan; however, the Department is not tracking and documenting SSR training attendance. From a sample of 25 full-time-equivalent (FTE) employees with SSRs, we found 20 employees had not completed role-based training within the past 3 years.

We also found the following control deficiencies:

- From a sample of 25 newly hired personnel (contractor, FTE, and locally employed staff), we identified nine users who had not completed the initial PS800<sup>14</sup> training within 10 days of gaining access to the system. The IA Training Plan requires first-time users to complete the course within 2 weeks of being granted access to the system.

---

<sup>13</sup> OMB Circular A-130, revised app. III, “Security of Federal Automated Information Resources.”

<sup>14</sup> The PS800 online user awareness training is required for all network users, domestic and abroad.

## UNCLASSIFIED

- From a sample of 25 personnel (contractor, FTE employees, and locally employed staff), five users had not taken the annual PS800 refresher training.

The control deficiencies with the new user and annual refresher PS800 training occurred because the Department had not implemented new automated methods to suspend the employees' access to the networks for those employees who have not completed the PS800 training. Currently, the Department relies on ISSOs to set expiration dates on user accounts, which are contingent on the completion of the PS800 training. As a result, all employees (users and non-users) need to be properly trained on how to protect classified information. Employees who are not properly trained create a risk for the Department because they may cause vulnerabilities or security breaches.

**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.

**Management's Response:** The Department stated that it "agrees with this recommendation" and that it "will develop a method of tracking of who needs and who has received role-based training; comparable to what is available for awareness training (including risk scoring in iPost)."

**OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department has developed a method for tracking individuals who have received role-based training.

**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.

**Management Response:** The Department did not indicate concurrence or nonconcurrence with this recommendation. It stated that it will "conduct a complete assessment of compliance in this area and take appropriate action if a material level of non-compliance is indicated."

Regarding the Cyber Security Awareness course (PS-800), the Department stated that a preliminary study of compliance with annual completion of the course shows that "nearly 100% of those who require training receive training within 30 days of the due date" and that it "does not consider this level of non-compliance to be a material risk to the security of the Department." The Department further stated that this is "especially true, considering there are several other sources of awareness training including the daily awareness program at login, as well as weekly and quarterly sources." Regarding OIG's "proposal to automatically suspend account access (without human intervention)," the

## UNCLASSIFIED

Department stated that this proposal “has a high risk of creating serious denial-of-service issues and as such, itself poses risks to the security of the Department.”

**OIG Analysis:** OIG considers this recommendation unresolved. The testing that was performed during the evaluation was a control-based test of the IA Training Plan, which states, “First time users must complete the course within 2 weeks of being granted access to the system. Thereafter, annual refresher training is required. Users should take the course within ten working days of the expiration of the course completion certificate received the previous year.” This recommendation can be resolved when the Department agrees to follow its internal procedures or change its procedures to train first-time users.

### **D. Plans of Action and Milestones Are Not Effective**

The Department’s Plans of Action and Milestones (POA&M) process is not fully and effectively implemented, and the program is not compliant with FISMA and OMB requirements. The POA&M is used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems.

The Department had not implemented a POA&M process to address and resolve security weaknesses identified on ClassNet GSS. For example, ClassNet security weaknesses identified from contingency plan test results, recommendations from external auditors, and annual tests and audits of security controls are not tracked in the enterprise POA&M database, as required by OMB<sup>15</sup> and the Committee on National Security Systems (CNSS).<sup>16</sup> The Department did not properly follow OMB and CNSS mandated guidance for the ClassNet GSS to address all weaknesses identified by program reviews and evaluations. Not addressing security weakness for national security systems is a vulnerability that threatens Department assets and the nation.

In addition, we found that the Department had not implemented corrective actions to address the POA&M control weaknesses within the OpenNet GSS identified in OIG’s FY 2010 FISMA report. Specifically, the Department’s POA&M process and program had the following control deficiencies:

- It did not consistently record essential resources to remediate and resolve security weaknesses. According to OMB,<sup>17</sup> POA&Ms should include the estimated funding resources required to resolve the weakness as well as the anticipated source of funding.
- It did not accurately and timely update remediation schedules to reflect actual system owners and others’ performance to resolve or mitigate control weaknesses. NIST SP

---

<sup>15</sup> OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.

<sup>16</sup> CNSS Policy No. 22, “Information Assurance Risk Management Policy for National Security Systems.” (Feb. 2009)

<sup>17</sup> OMB Memorandum M-04-25.

**UNCLASSIFIED**

800-37<sup>18</sup> states that the organization is required to update the plans of action and milestones on an ongoing basis.

The deficiencies within the POA&M process occurred because the Department had not developed criteria to prioritize the importance of security weaknesses from both an enterprise and bureau basis. Currently, the Department permits each bureau to prioritize risks within its respective environment and to budget accordingly without consideration of the risk and exposure to the Department as a whole. If the Department does not appropriately prioritize corrective actions on an enterprise basis, the most important actions (highest security risks) may not receive the required resources for remediation, thereby exposing the Department's sensitive data, systems, and hardware to unauthorized access and activities.

Currently, IRM/IA issues a quarterly POA&M Grading Memorandum process; however, this memorandum is distributed to the bureaus' or offices' ISSOs and not to senior management. Without the proper review and maintenance of POA&Ms, IT management may not be aware of the status of remediation. Furthermore, the inadequacy of the POA&M process adversely effects the capital planning process.

**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.

**Management Response:** The Department stated that it “concludes that the problems identified are not material (or are now being addressed) for the following reasons:

- The Department has a compliant process for tracking POA&M items on ClassNet.
- The Department has started distributing quarterly grades (effective Q1-FY2012) to executive officers, as recommended.
- Quarterly updates to POA&M data are not warranted, unless there has been a change of status. The grading covered under the prior bullet addresses this issue.”

The Department also stated that the iPost system “performs many of the functions of a POA&M system at a level of timeliness and detail that the traditional POA&M approach cannot achieve. Given the MIT Lincoln Labs findings on the trade-off between

---

<sup>18</sup> NIST SP 800-37.

## UNCLASSIFIED

completeness and timeliness discussed previously, the Department concludes that deficiencies in the traditional POA&M system are not a material risk to the security of the Department, given iPost as a compensating control.

**OIG Analysis:** OIG considers this recommendation unresolved. The Department did not provide evidence during the evaluation that the POA&M process was all inclusive. The Department POA&M process on ClassNet does not include identified security vulnerabilities during security testing, OIG audits, or other assessments. Therefore, this process fails to track Department actions to remediate identified weaknesses. Additionally weaknesses that are identified in the scanning results are not added to the POA&M tracking. Although the Department stated that it had started distributing the quarterly memorandums, it did not take this action within the time period of the FISMA evaluation. The Department stated that iPost has replaced the traditional POA&M process. The independent public accountant determined, based on the issues noted with iPost (detailed in section G), that the system is not mature enough to compensate for the POA&M process. This recommendation can be resolved when the Department can document that the POA&M process includes the required elements for tracking, that the POA&M process accounts for weaknesses identified by all sources (scans, assessments, and OIG findings), and corrective actions are taken in the accordance with NIST and OMB requirements.

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

The Department needs to improve account management processes in Active Directory (AD) for OpenNet and ClassNet. In FY 2010, 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 approximately 128,000 OpenNet AD users' accounts, we identified the following deficiencies:

- Approximately 400 guest, test, and temporary accounts were in the AD accounts. The FAM<sup>19</sup> states, "The data center manager and the system manager may not maintain permanent user IDs and passwords on AISs for visitors, vendor service personnel, training, demonstrations, or other purposes."
- Approximately 9,000 accounts have not been used (never logged on). The FAM<sup>20</sup> requires user privileges to be reviewed annually to verify that privileges are still appropriate.
- Approximately 400 accounts with passwords set not to expire. The FAM<sup>21</sup> requires passwords to be changed at least every 60 days.

---

<sup>19</sup> 12 FAM 622.1-3(b), "Password Controls."

<sup>20</sup> 12 FAM 622.1-3(i).

<sup>21</sup> 12 FAM 622.1-3(j).

## UNCLASSIFIED

- Approximately 300 Install Accounts were within AD accounts. The FAM<sup>22</sup> requires the removal of non-permanent (that is, visitor and training) user accounts and passwords.

From a population of approximately 36,000 ClassNet AD accounts, we identified the following discrepancies:

- Approximately 200 guest, test, and temporary accounts were in the AD accounts. The FAM<sup>23</sup> states, “The data center manager and the system manager may not maintain permanent user IDs and passwords on AISs for visitors, vendor service personnel, training, demonstrations, or other purposes.”
- Approximately 4,000 accounts have not been used (never logged on). The FAM<sup>24</sup> requires user privileges to be reviewed annually to verify that privileges are still appropriate.
- Approximately 900 accounts with passwords set not to expire. The FAM<sup>25</sup> requires passwords to be changed at least every 60 days.
- Approximately 200 Install Accounts were within AD accounts. The FAM<sup>26</sup> requires the removal of non-permanent (that is, visitor and training) user accounts and passwords.

Each bureau and post is responsible for user account management, such as adding new users and removing or modifying existing users’ accounts. Additionally, the Department had not developed and implemented processes and procedures to ensure that bureaus and posts performed an annual review and recertification of users’ privileges. Inadequate account and identity management controls increase the risk that temporary and active accounts may be accessed and used by Department and contractor personnel to perform unauthorized activities, such as modifying or improperly releasing sensitive Department information or accessing and modifying operating system software.

**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.

---

<sup>22</sup> 12 FAM 629.2-2(c), “Administrative Security – Password Controls.”

<sup>23</sup> 12 FAM 632.1-4(d), “Password Controls.”

<sup>24</sup> 12 FAM 622.1-3(i).

<sup>25</sup> 12 FAM 622.1-3(j).

<sup>26</sup> 12 FAM 629.2-2(c), “Administrative Security – Password Controls.”

## UNCLASSIFIED

**Management Response:** The Department stated that it “agrees there is a potential risk” with user accounts and that it will, begin “scoring stale accounts in iPost.” The Department further stated that it will, in December 2011, “conduct a more complete assessment of this problem and determine what prioritized mitigation actions are justified by the current level of risk.”

The Department also stated that based on “a preliminary investigation of the accounts identified as deficient by the OIG using a random sample of accounts in each of the remaining categories,” it found that OIG “had overestimated the level of deficiency by a large percentage.”

**OIG Analysis:** OIG considers this recommendation resolved, pending further action. OIG has determined that accounts such as group mailboxes accounts and service accounts that have not been used and are active are vulnerable to insider exploitation. The Department should also consider the weaknesses identified in the user accounts analyses when performing its own analyses. Because the Department has agreed to conduct a more complete assessment of this problem, this recommendation can be closed when OIG reviews and accepts documentation showing that the Department is properly maintaining the Active Directory.

### **F. The User Provisioning Process for Creating, Modifying, and Disabling Users’ Accounts Requires Significant Improvement**

The Department’s user provisioning process for creating, modifying, and disabling users’ accounts is not in compliance with the FAM. The FAM<sup>27</sup> requires ISSOs to maintain all password/receipt acknowledgement forms to comply with NIST SP 800-53.<sup>28</sup> The FAM<sup>29</sup> also states the data center manager and the system manager, in conjunction with the ISSO, must revoke user access privileges for employees and contractors who are transferred or terminated. We found control deficiencies within the Department’s user provisioning process as follows:

- Two of 25 ClassNet Domain Administrators accounts did not have corresponding individual user accounts, which results in no individual accountability of actions for Domain Administrators.
- Of 894 separated FTE accounts, 294 accounts were not terminated or deactivated in a timely manner. In addition, of the 294 accounts that were terminated, 104 had a remote access security token.
- All 25 new user accounts created within the past fiscal year did not have documentation (Password/Receipt Form) available for audit.
- All seven network administrator accounts created within the past fiscal year did not have documentation available for audit.

---

<sup>27</sup> 12 FAM 622.5, “Log and Record Keeping.”

<sup>28</sup> NIST SP 800-53, rev. 3, Aug. 2009, *Recommended Security Controls for Federal Information Systems and Organizations*.

<sup>29</sup> 12 FAM 621.3-3, “System Access.”

## UNCLASSIFIED

- One of 25 OpenNet domain administrators/administrators accounts was used as a group account.

The user provisioning weaknesses occurred because the ISSOs are not performing their user account responsibilities of creating, disabling, and reviewing user access in an effective manner. The Department had not established the controls necessary to ensure the bureau and post ISSOs perform their duties effectively by disabling accounts.

These control weaknesses increase the potential that unauthorized activities can occur without timely detection, which adversely affects confidentiality, integrity, and availability of the data on OpenNet and ClassNet. In addition, an ineffective user provisioning program and ineffective procedures and practices increases the Department's risk of unauthorized users having access to the network to enable the performance of unauthorized activities such as modifying Department sensitive data, improperly releasing sensitive data, or intentionally destroying sensitive data.

**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).

**Management Response:** The Department stated that the deactivation of accounts recommendation is related to a financial audit. The Department further stated that it "will investigate the other findings within six months to determine their scope and materiality to the security of the Department" and that based on the results of this review, it "will determine a risk-based and cost-effective solution to any issues identified," which "may range from accepting the risk, to further corrective action."

**OIG Analysis:** OIG considers this recommendation resolved, pending further action. This recommendation can be closed when the Department provides documentation showing proper maintenance related to creating, modifying, and deleting accounts and its comparison of the terminated user listings provided by bureau and post personnel officers and the 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, and in a manner consistent with Department of State policy. Additionally the Department's statement that the "deactivation of accounts . . . is related to" the financial systems audit presents the appearance that IRM does not fully understand that the security weakness is an enterprise-wide vulnerability and is not isolated to the financial systems. The financial systems of the Department are only a segment of the entire enterprise. Since IRM has done an analysis on the account management on the financial systems, the Department needs to consider taking further action for the remainder of the enterprise.

## **G. Continuous Monitoring Program Needs To Be Improved**

The Department had partially implemented a continuous monitoring program at the organization level and the system level in accordance with OMB<sup>30</sup> and NIST SP 800-37.<sup>31</sup> However, the Department had not taken action to resolve the continuous monitoring control deficiencies identified in the FY 2010 FISMA report *Review of the Information Security Program at the Department of State*. We evaluated the Department's implementation of these continuous monitoring components and found deficiencies. (The deficiencies are detailed in Appendix H.) Therefore, the continuous monitoring program is only partially implemented.

At the organizational level, the ISSC had not developed a formal continuous monitoring strategy that addresses framing risk, assessing risk, responding to risk, and monitoring risk in accordance with NIST SP 800-39. Department officials stated that the Department is implementing continuous monitoring strategy at a cost-effective, risk-based level of detail and will submit the strategy to the ISSC for approval.

At the system level, the Department uses the iPost system as its principal system for implementing continuous monitoring organization-wide. For example, the Department performs vulnerability assessment scanning every 36 hours. However, this system has not been fully implemented. The following conditions were reported in the FY FISMA 2010 report on the Department's information security program:

- The scanning tools do not assess Oracle, the Department's most common database system, and UNIX security configurations for configuration control weaknesses, which could adversely impact application access controls.
- Scanning results for routers, firewalls, and Demilitarized Zone servers were not available in iPost; therefore, these results were not used in risk scoring.

We found that the Department had not documented an enterprise-wide continuous monitoring program strategy within its System Security Plans (SSP) to assist system owners in evaluating various control deficiencies. The evaluation identified 11 of 30 systems in which the system security plan lacked a continuous monitoring strategy for the system. The strategy was not updated because the System Security Officer (SSO) did not update the SSPs in accordance with NIST SP 800-53, Revision 3 and NIST SP 800-37. Specifically, NIST SP 800-37 requires

---

<sup>30</sup> OMB M-11-33 states, "Agencies should develop an enterprise-wide strategy for monitoring security controls on an ongoing basis. A robust and effective continuous monitoring program will ensure important procedures included in an agency's security authorization package (e.g., as described in system security plans, security assessment reports, and POA&Ms) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis. This will help make the security authorization process more dynamic and responsive to today's federal missions and rapidly changing conditions. NIST SPs 800-37, Revision 1; NIST SP 800-53, Revision 3; and NIST SP 800-53A Revision 1, provide guidance on continuous monitoring programs."

<sup>31</sup> The security documentation needed for continuous monitoring, which includes security impact analyses, security control assessments reports, plans of action and milestones, and authorization documentation, is described in NIST 800-37, rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (Feb. 2010), app. G, "Continuous Monitoring—Managing and Tracking the Security State of Information Systems."

**UNCLASSIFIED**

that an organization-defined continuous monitoring strategy be implemented. NIST SP 800-53, Revision 3<sup>32</sup> requires that the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process, security impact analysis, ongoing security control assessment, and a method to report the security state of the system to appropriate organizational officials. During the course of our evaluation, we inquired about the implementation of iPost on ClassNet and were informed that iPost was not currently implemented. Therefore, we did not perform an assessment of any hosts or networks residing on ClassNet. Furthermore, we discovered that iPost was in production on ClassNet as of August 2011, which exceeded our testing timeframe.

Additionally, the Government Accountability Office (GAO), in July 2011, issued a continuous monitoring report on the Department's iPost system.<sup>33</sup> GAO stated the following concerning iPost:

While State has reported success with implementing iPost to provide ongoing monitoring of certain controls over Windows hosts on OpenNet and reporting the status of these controls across the enterprise to appropriate officials, the department faces an ongoing challenge in continuing this success because it does not have a documented continuous monitoring strategy in place.

In addition to those weaknesses identified in the FY 2010 FISMA report on the Department's information security program and the specified weaknesses presented in the GAO report, the FY 2011 evaluation identified weaknesses with the Department's existing continuous monitoring approach to include the following:

- The Department did not identify all Windows operating systems or Department assets on OpenNet.
- The Department did not take into consideration those security controls that cannot be tested with automation (that is, physical and environmental controls, effectiveness of the IT security training, and the newest family of controls that deal with IT program management).

Not having a robust continuous monitoring program prevents an organization from fully understanding the security state of the information system over time. It also limits an organization's ability to effectively monitor its environment with changing threats, vulnerabilities, and technologies, thereby effecting missions/business functions. Without a fully implemented continuous monitoring program, management cannot conduct ongoing authorizations of information systems.

**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*.

---

<sup>32</sup> NIST SP 800-53, CA-7, "Continuous Monitoring."

<sup>33</sup> *Information Security: State Has Taken Steps To Implement a Continuous Monitoring Application, but Key Challenges Remain* (GAO-11-149, July 8, 2011).

## UNCLASSIFIED

**Management Comments:** The Department stated that it “agrees some increased level of documentation,” as was recommended, “would be valuable.”

**OIG Analysis:** OIG considers this recommendation resolved. The recommendation can be closed when OIG reviews and accepts documentation showing that the ISSC has developed, documented, and implemented an enterprise-wide continuous monitoring strategy.

**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 are to be monitored.

**Management Response:** The Department stated that it is “already engaged in” efforts pertaining to the scanning software, that it will “pursue [these efforts] with an appropriate level of priority,” that it “will expand the coverage of the risk scoring program,” and that it “will continue to expand coverage of risk in iPost.” As far as documenting a strategy in its security plans, the Department stated that “the continuous monitoring strategy is an enterprise level strategy” and therefore “does not need to be addressed in detail in every system security plan.”

Regarding implementation of a continuous monitoring strategy at the enterprise-wide level, the Department stated that this implementation “will require continuous improvement and thus never be completed” and that its “current continuous monitoring implementation is being copied as a model by other government agencies and the private sector.”

**OIG Analysis:** OIG considers this recommendation unresolved. Although OIG is aware that the Department has received nation-wide recognition for its continuous monitoring program, the Department must document a continuous monitoring strategy in every security plan, as required by NIST.

Furthermore, in its response to the Government Accountability Office’s July 2011 report on information security,<sup>34</sup> the Department responded as follows: “State officials

---

<sup>34</sup> *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain* (GAO 11-49, July 2011).

## UNCLASSIFIED

indicated that the focus on Windows hosts for risk scoring was due, in part, because of the desire to demonstrate success of the risk scoring program before considering other types of network devices.”

Also, the Department needs to provide OIG documentation showing a documented enterprise-wide level continuous monitoring strategy, scanning results of non-Windows systems, operating procedures to include non-Windows scan results in iPost, and continuous monitoring plans at the system level.

### **H. The Continuity of Operations Program Needs to Be Improved**

The Department’s Continuity of Operations Program is not operating effectively and has not been documented in accordance with NIST SP 800-34 and FCD-2.<sup>35</sup> 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.

We found that the Continuity of Operations Plan (COOP) Communication Plan (CCP) for emergency communications and the network had not been updated with significant changes since 2008. The COOP CCP had not been updated in accordance with NIST SP 800-34<sup>36</sup> because IRM focuses on the Bureau Emergency Action Plan (BEAP)<sup>37</sup> instead of the CCP, which contributes to the continuation of communications and the network for the entire Department. For example, the following significant changes occurred but were not updated:

- The mirrored data redundancy within OpenNet between the Enterprise Service Operations Center (ESOC) East, the Harry S. Truman Building, and the Beltsville Information Management Center.
- The deployment of the SMART Core Messaging Application- Unclassified and the SMART Core Messaging Application- Classified, which both provide the ability to electronically release (send) and receive formal Departmental messages, interest profiling, message archiving, dissemination rules, and Role-Based Access Controls.
- The retirement of the mainframes at the Department of State.

---

<sup>35</sup> Federal Continuity Directive 2 (FCD-2) (February 2008), “Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process,” provides guidance and direction to Federal Executive Branch departments and agencies in the process for identifying their mission essential functions (MEFs), potential primary mission essential functions (PMEFs), and national essential functions (NEFs), and the Business Process Analysis (BPA) and Business Impact Analysis (BIA) that support and identify the relationships between these essential functions. It also provides guidance on the processes for conducting a BPA and BIA for each of the potential PMEFs that assist in identifying essential function relationships and interdependencies, time sensitivities, threat and vulnerability analyses, and mitigation strategies that affect and support the PMEFs. Also, see FDC-1, Federal Executive Branch National Continuity Program and Requirements, from which FCD-2 is derived.

<sup>36</sup> NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (last updated Nov. 11, 2010).

<sup>37</sup> 6 FAM 422.3(a), “Bureau Emergency Action Plan (BEAP),” defines a BEAP as a “bureau-specific plan used to describe actions taken to ensure the safety of Department employees and to ensure bureau readiness to continue MEFs across a wide range of domestic emergencies that impact the Department.”

## UNCLASSIFIED

- The development of the new data center ESOC West.

In addition, we identified the following deficiencies:

- IRM had not documented an entity-wide Business Impact Analysis (BIA) to ensure the coordination of the recovery prioritizations of critical mission/business processes and services in the event of a disruption within the ESOC. The BIA had not been documented because IRM does not think that the entity-wide BIA applies to its contingency planning process. However, NIST SP 800-34, Revision 1,<sup>38</sup> states that the BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes.
- The entity-wide process-based BIA, which supports COOP functions developed by the Office of Emergency Management (OEM) to support Federal Continuity Directive 2 (FCD-2), does not agree with the OpenNet Contingency Plan. For example, OEM officials stated that the infrastructure should not be interrupted in the event of a disaster, and IRM officials stated that the infrastructure Maximum Tolerable Downtime is 24 hours. The inconsistency between the two documents occurred because the Department does not require OEM and IRM to coordinate with the continuity of operations planning. According to NIST SP 800-34, Revision 1, information systems that support COOP functions will be identified in the process-based BIA.

An out-of-date COOP CCP increases the risk that the Department may not be able to recover in a timely manner or may experience difficulty in recovering from a disaster. Additionally, the IRM CCP supports the Department COOP; therefore, the COOP relies upon the CCP to be current. Without a BIA, there is an increased risk that the Department will not recover mission-critical functions based on established recovery priorities. Additionally, the lack of communication between OEM and IRM may cause incongruent requirements and the expectations in the availability of the infrastructure in the event of a disaster.

**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 Foreign Affairs Manual that contains guidance and direction for development and implementation of Continuity of Operations Communication Plan.

---

<sup>38</sup> NIST SP 800-34, rev. 1.

## UNCLASSIFIED

**Management Response:** The Department indicated that it would take the actions recommended except for performing an entity-wide BIA and developing a strategy to prioritize recovery of the critical assets.

**OIG Analysis:** OIG considers this recommendation unresolved. This recommendation can be resolved when the Department agrees to perform an entity-wide BIA and develop a strategy to prioritize the recovery of the critical assets. The Department also needs to provide OIG documentation showing that the Department is updating the Continuity of Operations Communication Plan annually or when changes occur and provide evidence that the FAM has been updated to include guidance on the development and implementation of the Communication Plan.

**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*.

**Management Response:** The Department stated that it “considers the documents already aligned” but that it would develop criteria to determine when the BIA and the Department GSS downtime is “adequately coordinated” and “verify that these criteria are met.”

**OIG Analysis:** OIG considers this recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department has updated the *Foreign Affairs Manual* and the Continuity of Operations Communication Plan and that it has aligned the BIA of the Primary Essential Functions with the Maximum Tolerable Downtime of the network.

### **I. Information System Contingency Plans Needs To Be Improved**

The Department needs to improve the information system contingency planning program. An effective contingency planning program is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability.

We found that information system contingency plans (ISCP) had not been documented in accordance with NIST SPs 800-34, Revision 1, and 800-53, Revision 3, and with the FAM.<sup>39</sup> In our sample of 25 systems, we found the following deficiencies:

- Three systems—OpenNet, WebPass, and TDS Contingency Plans (CP)—had not documented an alternate recovery site. According to NIST SPs 800-34, Revision 1, and 53, Revision 3, agencies are required to identify an alternate storage site that is geographically separated from the primary storage site so that the alternate site is not susceptible to the same hazards.

---

<sup>39</sup> 5 FAM 1064.2, “Contingency Planning and Continuity of Operations.”

## UNCLASSIFIED

- One system—State Messaging and Archive Retrieval Toolset (SMART) - Classified system—did not have a CP. The FAM<sup>40</sup> states that system owners and non-Department entities are required to develop and maintain contingency plans for the major applications and general support systems under their control that process, store, or transmit Federal information.
- Two systems—eCountryClearance (eCC) and Secure Integrated Logistics Management System (S-ILMS)—CPs were not sufficiently detailed to enable the proper recovery and damage assessment. NIST SP 800-34, Revision 1,<sup>41</sup> requires the agency to address specific actions the organization should take following a system disruption or an emergency. Plans should be formatted to provide quick and clear directions in the event that personnel unfamiliar with the plan or the systems are called upon to perform recovery operations.
- Fifteen systems did not document the annual backup test, as required by NIST<sup>42</sup> for moderate- and high-impact systems, to verify media reliability and information integrity. (Systems that did not have annual backup testing are described in Appendix F).
- Three systems—OpenNet, WebPass, and TDS—had not documented backup procedures.

The control deficiencies occurred within the contingency planning program because the Department relies extensively on the system owners and bureaus to execute the Department's policies, establish and implement internal procedures, and ensure compliance with NIST SP 800-34, Revision 1.

Additionally, the Department had not developed reporting requirements for obtaining assurance of performance from the system owners and bureaus. By inadequately documenting the contingency plan, there is an increased risk that the Department will not be able to recover its mission-critical systems timely in the event of a significant disruption. Also, the Department increases the risks that it will not be able to meet its mission requirements and continue normal business activities.

**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:

---

<sup>40</sup> 5 FAM 1064.2(a)(1).

<sup>41</sup> NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010) (last updated Nov. 11, 2010).

<sup>42</sup> NIST SP 800-53, rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Aug 2009).

## UNCLASSIFIED

- 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.

**Management Response:** The Department stated it “will document compliance and/or non-compliance to the OIG findings and take the necessary corrective action.”

**OIG Analysis:** OIG considers this recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department has documented and is maintaining and updating the contingency plan program documentation.

**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.

**Management Response:** The Department stated it “will document compliance and/or non-compliance to the OIG findings and take the necessary corrective action.”

**OIG Analysis:** OIG considers this recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department has updated the FAM policy regarding backup and updates to the contingency plans, has updated the Contingency Plan Test Review checklist, and has remediated deficiencies found within the individual information system contingency plans.

## **J. Oversight of Contractor Systems and Extensions Needs Improvement**

The Department had not implemented an effective program for the oversight of contractor systems and contractor extensions (remote network connections to Department systems). Although the Department established initial contract agreements and conducted initial risk assessments for contractor extensions, we noted several deficiencies. For example, COCO systems did not have security-related documentation. The FAM<sup>43</sup> and NIST SP 800-47<sup>44</sup> require that the Department document the interconnection agreements between the network and the contractor with language similar to that contained in a memorandum of understanding (MOU) and an interconnection security agreement (ISA). The agreement must be submitted to IRM/IA.

Specifically, for COCO systems, IRM/IA did not provide documentation for the following:

- For all five COCO systems, a contractor agreement and system security documentation were lacking for the State Assistance Management System (SAMS); the Consular Visa System (CVS); the Antiterrorism Assistance (ATA) Student Database; the Foreign Service Office Tester (FSOT) system, and the Gateway to State (GTS). The Department relies on a decentralized security program whereby system owners/bureaus are responsible for overseeing COCO systems that provide services to a bureau.
- Of five COCO systems, ATOs were not made available for review for four systems (SAMS, CVS, ATA database, and FSOT). According to OMB,<sup>45</sup> the Department must assess security controls in accordance with NIST guidelines for contractor systems that collect, process, maintain, and house Government information.

The list of OpenNet extensions does not contain a complete inventory of workstations at other Government agencies. For example, OpenNet terminals (workstations) were observed by an OIG audit team at International Boundary and Water Commission (IBWC) and Broadcasting Board of Governors (BBG) offices. These connections are not on the list of OpenNet extensions. The Department tracks only OpenNet extensions at contractor sites and vendors and does not include other third parties, such as Government agencies.

We also found that the Department did not have an effective mechanism in place to identify the total number of contractors' personnel who had access to and privileges within the Department's network, applications, databases, and data. OMB Memorandum M-11-33 states: "Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems."

---

<sup>43</sup> 5 FAM 1065.3-1, "Requests for Interagency and Non-Department Connectivity."

<sup>44</sup> NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, Aug 2002.

<sup>45</sup> OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

## UNCLASSIFIED

The Department's contractor oversight process is decentralized whereby the Department assigns responsibility to the bureaus and posts and the system owner to provide better contractor oversight. For instance, to obtain information on the total number of Department contractor personnel, personnel from each Department bureau and office would have to be contacted. The Department had not established procedures to identify the number of contractors. DS and HR officials stated that they are collaborating to develop a Contractor Personnel Support System. According to DS officials, once the system is fully implemented and integrated with other systems, it will provide contractor oversight information for the Department.

Without adequate contractor oversight, the Department has minimal assurance that COCO systems, contractor extensions, and contractor personnel are compliant with FISMA, OMB requirements, and NIST standards. Additionally, without oversight, there is an increased risk that Department data collected, processed, and maintained can be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

**Recommendation 16.** We recommend that the Chief Information Officer, as required by 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 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.

**Management Response:** The Department indicated that it will align its contractor oversight program with Federal standards and guidelines. However, the Department stated that it “does not agree that [the] assignments [to implement a program whereby COCOs are overseen by IRM/IA] need to be changed.”

**OIG Analysis:** OIG considers the recommendation unresolved. Because contractor systems pose an even greater security risk because of the lack of Department presence, a COCO system security program overseen by IRM/IA is needed, and the Department needs to this action. Regarding the contractor oversight program, the Department needs to provide OIG documentation showing that it has aligned its contractor oversight program with Federal standards and guidelines.

**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

## UNCLASSIFIED

Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

**Management's Response:** The Department stated that it "will verify" that all Department computers at other Federal agencies "are clearly documented" and that it had not found any "defects with regard to the process for contractor sites."

**OIG Analysis:** OIG considers this recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department has developed and is implementing new and enhanced security requirements to coordinate security activities for tracking all extensions to include contractor sites.

**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 Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

**Management Comments:** The Department stated that it does not agree with the recommendation because "knowing the exact total number of contractors (a continuously changing number)" does not impact the security of the Department and OMB Memorandum M-11-33 does not require this.

**OIG Analysis:** OIG considers this recommendation unresolved. OMB Memorandum M-11-33 requires that agencies provide security training and awareness to all employees, including contractors, and further requires agencies to develop policies for information security oversight of contractors and other users who have privileged access to Federal data. This recommendation can be resolved when the Department agrees to take action to identify its total number of contractors.

### **K. Capital Planning Requires Improvement**

We found that information security was not fully integrated into the Department's Capital Planning and Investment Control (CPIC) process. As a result, management may be unaware of the Department's complete IT security portfolio. CPIC is the decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and IT security in support of agency missions and business needs. OMB Memorandum 11-33 mandates the Department integrate and fund IT security over the lifecycle of each system. The memorandum also states that security requirements for a steady state system, which is an existing system, that generates maintenance and operation costs at current capability and performance level must be met before new funds are spent on new systems or an existing system is modernized.

## UNCLASSIFIED

For four<sup>46</sup> of 10 appropriated IT security investments reviewed, the Department did not provide documentation showing obligations and expenditures. Approximately \$164 million was appropriated for the IT security investments; however, because of the lack of documentation for the project expenditures, there is an increased risk associated with the potential inability to achieve overall security program objectives within defined cost, schedule, and technical constraints. The CIO did not comply with provisions of the Clinger-Cohen Act of 1996, which require assumption of responsibility and accountability for IT investments. Inadequate monitoring shows a lack of accountability once funds are approved.

We identified the following control weaknesses related to the CPIC process:

- The Department did not provide OMB with required information related to IT security investments that have a significant dependency for the IT Infrastructure major investment. In a sample of 10 non-major investments that made up the IT Infrastructure major investment, we found none of the 10 investments were identified by the unique project identifier (UPI) in OMB Circular A-11<sup>47</sup> Exhibit 300,<sup>48</sup> even though OMB requires an agency to report IT security initiatives and investments not directly tied to a major investment on a separate line identified as “non-major.” By not including IT security investments that have a significant dependency on the IT infrastructure major investment in the exhibit 300, OMB does not have an accurate amount spent on IT security.
- IT security costs from the Department’s Plans of Actions and Milestones (POA&Ms) are not captured in the capital planning process. Specifically, the Department’s implementation of the POA&M process did not reflect the unique project identifiers (UPI)<sup>49</sup> for each corrective action plan as required by OMB.<sup>50</sup> According to OMB, security costs identified in POA&Ms are required to be captured within each investment’s Exhibit 300 and summarized to Exhibit 53.<sup>51</sup>

IRM had not developed procedures to reflect guidelines contained in the FY 2010 OMB Circular A-11, which states that non-major investments that are directly tied to major investments can be collapsed into a major investment. The Department was not aware of the OMB<sup>52</sup> requirement that each POA&M must have a unique project

---

<sup>46</sup> The four systems are Department Bandwidth Management, Foreign Affairs Network, IT Infrastructure–IRM, and Enterprise Network Management.

<sup>47</sup> OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*.

<sup>48</sup> Exhibit 300, *Capital Asset Plan and Business Case Summary*, is the document OMB uses to assess investments and ultimately make funding decisions. The exhibit also provides OMB with a robust assessment of the investment and is the vehicle for IT investments to justify lifecycle and annual funding requests to OMB.

<sup>49</sup> UPIs consist of the identifier depicting agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported (Exhibit 300), type of investment, agency four-digit identifier, and two-digit investment category code.

<sup>50</sup> OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*.

<sup>51</sup> Exhibit 53, *Agency IT Investment Portfolio*, provides an overview of the agency’s entire IT portfolio by listing every IT investment, lifecycle, and budget-year cost information.

<sup>52</sup> OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*.

**UNCLASSIFIED**

identifier. Without providing proper justification for funds, the Department's accountability of the IT Infrastructure investment is not fully supported. The lack of integration between the POA&M process and the capital planning process negatively affects the fund prioritization among the IT investments. Ultimately, inadequate oversight increases the risk of unapproved investments being funded.

**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.

**Management Response:** The Department stated that it "agree[d]" with this recommendation "but not the authorities cited." However, it stated that it will track and include a summary report for all obligations and expenditures for all IT projects that have a material level of funding or significant security risk and that it will "[i]nclude UPIs in the Department's POA&M for each system."

**OIG Analysis:** OIG considers this recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the Department is tracking all obligations and expenditures for all IT projects and including UPIs in its POA&M for each system.

## **OIG Additional Analyses of Management Comments**

In its response to the draft report, the Department provided additional comments and information that were not recommendation specific. These comments and OIG's responses are as presented.

### **Continuous Monitoring**

The Department stated that it disagreed with OIG that continuous monitoring, as currently conducted, produced lower risk than a traditional C&A program, and on the relative importance of completeness and compliance vs. timeliness and risk-based prioritization. Having carefully considered these factors, the Department is convinced its continuous monitoring program, which is 300 times more timely than traditional three-year reauthorizations, produces significantly lower security risk on its networks.”

OIG continues to support the concept of continuous monitoring. However, as implemented within the Department, compounded with the lack of documentation that exists, those deficiencies represent a serious internal control weaknesses. While the Department has repeatedly questioned the accuracy of the examples provided by OIG to support the weaknesses identified in this report, the Department has not refuted these weaknesses.

### **Risk-Based Versus Compliance-Based Assessment**

Regarding the Department's comments on risk-based versus compliance-based assessment of the information security program, OIG maintains that the lack of security controls (internal controls) in the supporting general support systems constitutes a substantial risk to information and information systems. The Department's inability to produce a continuous monitoring and risk management strategy reinforces OIG's position regarding a defined approach to addressing risk and taking corrective actions. Because IRM cannot provide a repeatable process used to identify and correct weaknesses that can be continued by others, OIG is unable to assess the effectiveness of the existing “risk-based” process. Currently, the process is under the sole control of limited personnel within IRM and is not fully vested with others responsible for involvement in the risk based decision making for the Department. Furthermore, because the continuous monitoring and risk management strategies are not documented, the ability to continue making decisions that are based on management having an accurate representation of the vulnerabilities in the Department's information security program is questionable. These factors alone contribute to the risk to the Department but if some catastrophic event occurs to the few IRM employees who are currently managing the continuous monitoring and risk management strategies the ability to continue would be hampered because there is no documentation to explain how the process is supposed to be working.

### **Completeness and Timeliness**

Regarding the statements concerning completeness and timeliness, OIG agrees that the past 3-year cycle of FISMA did not present a current state of the security controls in an

**UNCLASSIFIED**

information system. However, the continuous monitoring approach does not provide a complete state of information system security controls. The current implementation tests a limited number of the security controls repeatedly, but it does not provide a methodology to test all of the security controls over the life of the security authorization, as required by NIST. Although the current process does provide a timely response to a small subset of the security controls, it lacks a strategy to explain how other controls are tested and allows the majority of security controls to be untested. Since many of these controls require a manual assessment to determine the degree of effectiveness over the course of the security authorization, the inability of the Department to document the continuous monitoring strategy and a lack of plan of action and milestones to enact corrective actions place the Department's vital information and information systems at significant risk.

## **List of Current Year Recommendations**

**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.

**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.

**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.

**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.

**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.

**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

## UNCLASSIFIED

Awareness course within the required timeframe as required by the Information Assurance Training Plan.

**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.

**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.

**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).

**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*.

**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.

## UNCLASSIFIED

- 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 are to be monitored.

**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.

**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*.

**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.

**Recommendation 15.** As required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-34, Revision 1, *Contingency Planning Guide for*

## UNCLASSIFIED

*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.

**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.

**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*.

**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

**UNCLASSIFIED**

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*.

**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.

## **Appendix A. Objectives, Scope, and Methodology**

In order to fulfill its responsibilities related to the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) contracted with Williams, Adley & Company, 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 2011.

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 evaluation 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 and OIG believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

We performed fieldwork from April through July 31, 2011. Our fieldwork was completed before OMB Memorandum M-11-33,<sup>1</sup> *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011, was issued. This memorandum provided instructions for FY 2011 reporting requirements. We reviewed the memorandum and evaluated its impact on our results but determined that no changes were required to be made.

---

<sup>1</sup> OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

**UNCLASSIFIED**  
**DRAFT**

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, M-10-15, and M-11-33.<sup>2</sup>
- Department policies and procedures such as 5 FAM and 12 FAM.<sup>3</sup>
- Federal laws, regulations, and standards such as FISMA, OMB Circular A-130, Appendix III,<sup>4</sup> and OMB Circular No. A-11.<sup>5</sup>
- NIST Special Publications (SP), Federal Information Processing Standards (FIPS), other applicable NIST publications, and industry best practices.

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

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

The evaluation covered the period of October 1, 2010, to September 30, 2011. 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 FIPS 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 evaluation approach addressed the reporting instructions from OMB Memorandum M-11-33.

---

<sup>2</sup> 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 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; and M-11-33, respectively.

<sup>3</sup> 5 FAM, "Information Management" and 12 FAM, "Diplomatic Security".

<sup>4</sup> OMB Circular A-130 Revised Appendix III, "Security of Federal Automated Information Resources."

<sup>5</sup> OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*.

**UNCLASSIFIED**  
**DRAFT**

- 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 30 systems for our sample. (See Appendix I.).
- 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 *Review of Department of State Information Security Program* (AUD/IT-11-07, Nov. 2010).

## **Appendix B. Followup of Recommendations From the FY 2010 FISMA Report**

The evaluation team reviewed actions implemented by management to mitigate the findings identified in the FY 2010 FISMA report. The current status of each of the recommendations is as follows:

**Recommendation 1.** We recommend that the Chief Information Officer verify the Federal Information Security Management Act systems inventory list to the Information Technology Asset Baseline to ensure that all information technology systems are accurately accounted for.

*2011 Status: Closed. We reviewed the population of the FY 2010 fourth quarter FISMA inventory list and the population of the FY 2011 third quarter FISMA inventory list. We verified all changes between the two populations within ITAB. The list was accurate and complete.*

**Recommendation 2.** We recommend that the Chief Information Security Officer ensure that systems operated by a contractor, including systems rated low cost and low impact, the security authorization process, including completion of a risk assessment and implementation of necessary security controls, and that security authorization packages are completed on a timely basis.

*2011 Status: This recommendation is partially closed. The systems rated low cost and low impact that are operated by contractors are websites hosted on foreign Internet Service Providers (ISPs). The Department cannot enforce FISMA/NIST requirements for websites hosted on foreign ISPs, as FISMA and NIST are US law/standards. The evaluation found that security authorization packages were not completed accurately and on a timely basis. It has become Recommendation 3 (Finding A) in the FY 2011 report.*

**Recommendation 3.** We recommend that the Chief Information Officer develop a process to periodically update the resources recorded in the plans of action and milestones (POA&M) and that it update, in the POA&Ms, those completion dates for corrective actions that have expired.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 7 (Finding D) in the FY 2011 report*

**Recommendation 4.** We recommend that the Chief Information Officer, the Foreign Service Institute, and the Bureau of Diplomatic Security implement methods to enforce the security awareness policy to suspend a user's access if the user has not taken the Cyber Security Awareness course within the required timeframe.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 6 (Finding C) in the FY 2011 report.*

**UNCLASSIFIED**

**Recommendation 5.** We recommend that the Chief Information Officer, the Foreign Service Institute, and the Bureau of Diplomatic Security complete the Department of State's corrective action plan (which involves Active Directory, security awareness completion data, and iPost) to enforce the security awareness policy to suspend a user's access if the Cyber Security Awareness course is not taken within the required timeframe.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 6 (Finding C) in the FY 2011 report.*

**Recommendation 6.** We recommend that the Chief Information Officer and the Bureau of Diplomatic Security define and identify personnel who have significant security responsibilities and ensure that they receive the appropriate training. Also, the Student Training Management System should be modified to capture other training systems, such as those paid for by the Department of State, to meet continuing professional education requirements.

*2011 Status: Closed. In the evaluation we were able to identify the titles of personnel who have significant security responsibilities in the IA Training Plan.*

**Recommendation 7.** We recommend that the Chief Information Officer complete the end-to-end configuration management initiative, including implementation of the standard operating environment.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 4 (Finding B) in the FY 2011 report.*

**Recommendation 8.** We recommend that the Chief Information Officer:

Install an NIST approved encryption algorithm that controls access to support controls access to OpenNet Everywhere (ONE), reconfigure the ONE session timeout setting to 20 minutes, retain remote access authorization forms to show supervisory approval, and document the necessary risk assessment to determine the electronic authentication level for ONE.

*2011 Status: Closed. The evaluation assessed Global OpenNet (GO), the replacement for ONE, and found the security controls were implemented in accordance with OMB and NIST. Based on the electronic process from the implementation of GO, we have determined that the electronic authorization forms requires supervisory and executive director approval before the remote access user receives a FOB key.*

**Recommendation 9.** We recommend that the Chief Information Officer enhance the Active Directory account management automated tools to flag accounts that have not been used within the past 60 days and ensure that all accounts are configured with passwords that expire every 60 days.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 8 (Finding E) in the FY 2011 report.*

**Recommendation 10.** We recommend that the Chief Information Officer ensure that

**UNCLASSIFIED**

program managers and office managers annually review access privileges of users under their supervision so that the number of guest, test, and temporary accounts and accounts that have not been used is reduced.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 8 (Finding E) in the FY 2011 report.*

**Recommendation 11.** We recommend that the Bureau of Diplomatic Security implement proper staff awareness through training and have shift supervisors, as part of the shift change procedures, ensure that personally identifiable information data incidents are reported to the U.S. Computer Emergency Response Team within the required 1-hour timeframe.

*2011 Status: Closed. The evaluation found that Diplomatic Security ensures that personally identifiable information data incidents are reported to US CERT within the required 1-hour timeframe.*

**Recommendation 12.** We recommend that the Chief Information Officer include, under its continuous monitoring program scanning results for databases, firewalls, routers, and switches and include the results in the Risk Scoring Program dashboard.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 11 (Finding G) in the FY 2011 report.*

**Recommendation 13.** We recommend that the Chief Information Officer identify the secondary site for the State Messaging and Archive Retrieval Toolset (SMART) system and complete development of the SMART's system contingency plan.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 14 (Finding I) in the FY 2011 report.*

**Recommendation 14.** We recommend that the Bureau of Administration review all relevant information technology and professional services contracts to ensure that they contain the required Department of State Acquisition Regulations information security clauses.

*2011 Status: Closed.*

**Recommendation 15.** 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.

*2011 Status: This is open and a repeat recommendation from the FY 2010 report. It has become Recommendation 18 (Finding J) in the FY 2011 report.*

## **Appendix C. Systems With Invalid Authority To Operate**

As part of the security authorization testing, we requested the most recent authorities to operate (ATOs) for the sample of 30 systems. The ATO is the final security authorization decision from the designated authorizing official to the information system. Per National Institute of Standards and Technology Special Publication 800-37,<sup>1</sup> the authorization decision document contains the following information: authorization decision, terms and conditions for the authorization, and authorization termination date.

**Table 1. Systems With Invalid Authority To Operate**

<b>Bureau Name</b>	<b>Name</b>	<b>Package No.</b>	<b>Type</b>	<b>FIPS Categorization</b>
EUR	EXTRANET	1140	UNCL	L
IO	USEVI	2412	UNCL	L
IRM	TEDS	593	CL	H
IRM	WINAD	633	UNCL	M
IRM	TDS	719	CL	H
IRM	WebPASS	744	UNCL	M
IRM	SMART-C	2744	CL	H
L	IDMAS	647	UNCL	H
IRM	OpenNet	633	UNCL	M
IRM	ClassNet	631	CL	H

**Legend**

<b>Bureaus</b>	<b>System Classification and Categorization</b>
EUR-Bureau of European Affairs	CL- Classified Network
IO-Bureau of International Organization Affairs	UNCL- Unclassified Network
IRM- Bureau of Information Resource Management	H- High Impact
L- Office of the Legal Advisor	M- Moderate Impact

<sup>1</sup> NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Feb 2010

**UNCLASSIFIED**

**Appendix D. Systems With Outdated Security Baseline Controls**

In the evaluation, we assessed a sample of 30 systems (see Appendix I) to determine whether the systems were in compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Information Systems* (August 2009) (last updated May 1, 2010). NIST SP 800-53 Revision 3 provides guidelines for selecting and specifying security controls (management, operational, and technical) for information systems supporting the executive agencies of the Federal Government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Table 1 lists the systems for which security controls have not been updated to comply with NIST SP 800-53 Revision 3.<sup>1</sup>

**Table 1. Systems With Outdated Security Baseline Controls**

Sample #	Bureau Name	Name	Package No.	Type	FIPS Categorization	Compliance (Y/N)
1	A	ILMS	830	UNCL	M	N
2	CA	IVAMS	97	UNCL	M	N
3	CA	FEP	344	UNCL	M	N
4	CA	PLOTS	346	UNCL	M	N
5	CA	CLASS	558	UNCL	H	N
6	CA	MIS	724	UNCL	M	N
7	CA	OPSS	898	UNCL	M	N
8	CA	PLMS	4547	UNCL	M	N
9	DS	CMS	424	UNCL	M	N
10	DS	SIMAS	798	UNCL	M	N
11	DS	IDMS	1000	UNCL	M	N
12	EUR	EXTRANE T	1140	UNCL	L	N

<sup>1</sup> OMB Memorandum M-11-33 FY 2011 FAQs states that agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB.

**UNCLASSIFIED**

<b>13</b>	HR	GTS	843	UNCL	M	N
<b>14</b>	IIP	CMS (IIP)	600	UNCL	L	N
<b>15</b>	IO	USEVI	2412	UNCL	L	N
<b>16</b>	IRM	WINAD	633	UNCL	M	N
<b>17</b>	IRM	OPENNET (Transport)	634	UNCL	M	N
<b>18</b>	IRM	TDS	719	CL	H	N
<b>19</b>	IRM	WebPASS	744	UNCL	M	N
<b>20</b>	IRM	SMART - SBU	2743	UNCL	M	N
<b>21</b>	IRM	EDW	2747	UNCL	M	N
<b>22</b>	L	IDMAS	647	UNCL	H	N
<b>23</b>	M/PRI	eCC	966	UNCL	M	N
<b>24</b>	MED	eMED	299	UNCL	M	N

**Legend**

Bureaus	
A – Bureau of Administration	IO-Bureau of International Organization Affairs
CA – Bureau of Consular Affairs	IRM- Bureau of Information Resource Management
DS – Bureau of Diplomatic Security	L- Office of the Legal Advisor
EUR - Bureau of European Affairs	M/PRI – Office of Management Policy, Rightsizing and Innovation
HR – Bureau of Human Resources	MED – Office of Medical Services
IIP – Office of International Information Programs	
System Classification and Categorization	
Classification	Categorization
CL- Classified Network	H- High Impact
UNCL- Unclassified Network	M- Moderate Impact
	L – Low Impact

## **Appendix E. Vulnerability Assessment**

As part of the evaluation, we requested that the Bureau of Diplomatic Security, Security Infrastructure Directorate, Office of Computer Security (DS/SI/CS), execute vulnerability scans on a sample of 16 systems during the period August 1 to September 1, 2011. A total of 472 hosts<sup>1</sup> from the 16 systems were active and tested. DS/SI/CS is responsible for performing vulnerability scans on the Department's systems as part of its security assessment duties. As part of the Department's continuous monitoring program, DS stores the vulnerability scans in a database for iPost. iPost subsequently retrieves the vulnerability scan results and analyzes the results for the risk scoring program. For the systems tested, we reviewed the vulnerability scan configurations, analyzed the results, and summarized the results. The weaknesses we identified are summarized as follows:

- A. Systems, operating systems, and applications with critical system and security patches which had not been applied.
- B. Systems that did not meet the standards set forth in the System Configuration Policy and Procedures.
- C. Systems that allowed access to system resources via anonymous logins and passwords, default credentials, and unsecured access points.

The risk ratings are defined as follows:

- High Risk - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (for example, an administrator or a, root accounts) to the machine over a remote connection. Examples are: IIS Remote Data Services, remote procedure call automount daemon (RPC Automountd).
- Medium Risk - The vulnerability discovered on the system can lead directly to an attacker gaining non-privileged access (for example, standard user) to the machine over a remote connection. Examples are: Coldfusion viewexample.cfm and, Open and accessible NetBIOS ports.
- Low Risk - The vulnerability discovered on the system provides enticement data to the attacker that may be used to launch a more informed attack against the target environment. In addition, the vulnerability may indirectly lead to an attacker's gaining some form of access to the machine over a remote connection.

---

<sup>1</sup> A host is computer that is connected to a Transmission Control Protocol/Internet Protocol (TCP/IP) network, including the Internet. Each host had a unique IP address.

**UNCLASSIFIED**

A. Vulnerabilities and Unpatched Systems

For the 16 systems tested, the total number of high, medium, and low risk vulnerabilities identified during vulnerability analyses are shown in Table 1.

**Table 1. Host Vulnerabilities By Risk Rating**

No.	System Name	Active Hosts (Number of IP Addresses)	Number of High Risk Vulnerabilities	Number of Medium Risk Vulnerabilities	Number of Low Risk Vulnerabilities
1	FEP	6/6	214	269	45
2	IAVMS	11/13	237	265	58
3	OPSS	4/9	87	143	28
4	PLOTS	2/2	25	58	9
5	FSA	9/13	175	203	56
6	EDW	9/9	153	269	56
7	WebPASS	2/11	27	40	14
8	EMED	7/9	228	300	48
9	CLASS	12/12	71	315	75
10	ILMS	163/512	3,193	2,818	702
11	MIS	4/4	93	125	28
12	PLMS	10/10	313	454	75
13	IPMS	182/258	2,274	4,870	1,265
14	OPENNET	10/10	175	390	103
15	WINAD	10/10	9	36	9
16	Smart-SBU	31/59	1,246	1,099	229
<b>TOTAL</b>		<b>472/947</b>	<b>8,520</b>	<b>11,654</b>	<b>2,800</b>

**UNCLASSIFIED**

For the 16 systems tested, the total number of patches that were not installed on the hosts, by system, are shown in Table 2.

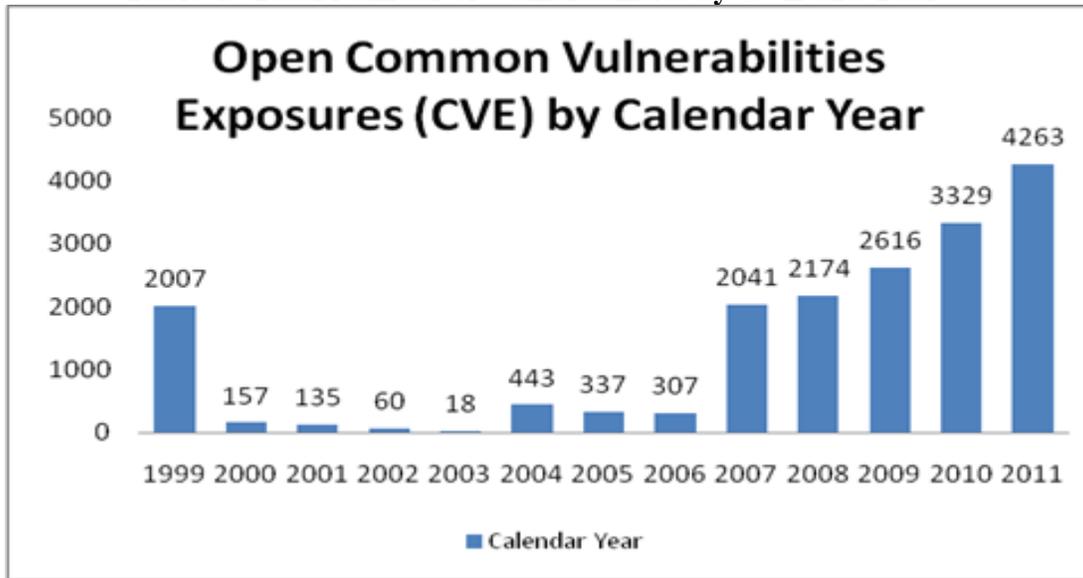


For the 16 systems tested, we performed an analysis of the Common Vulnerabilities and Exposures (CVEs) and risk ratings. CVE is a dictionary of publicly known information security vulnerabilities and exposures. The number of weaknesses identified are shown in Table 3, and the number of vulnerabilities are shown in Table 4.

**Table 3. Number of Vulnerabilities Identified by CVE and Risk Rating**

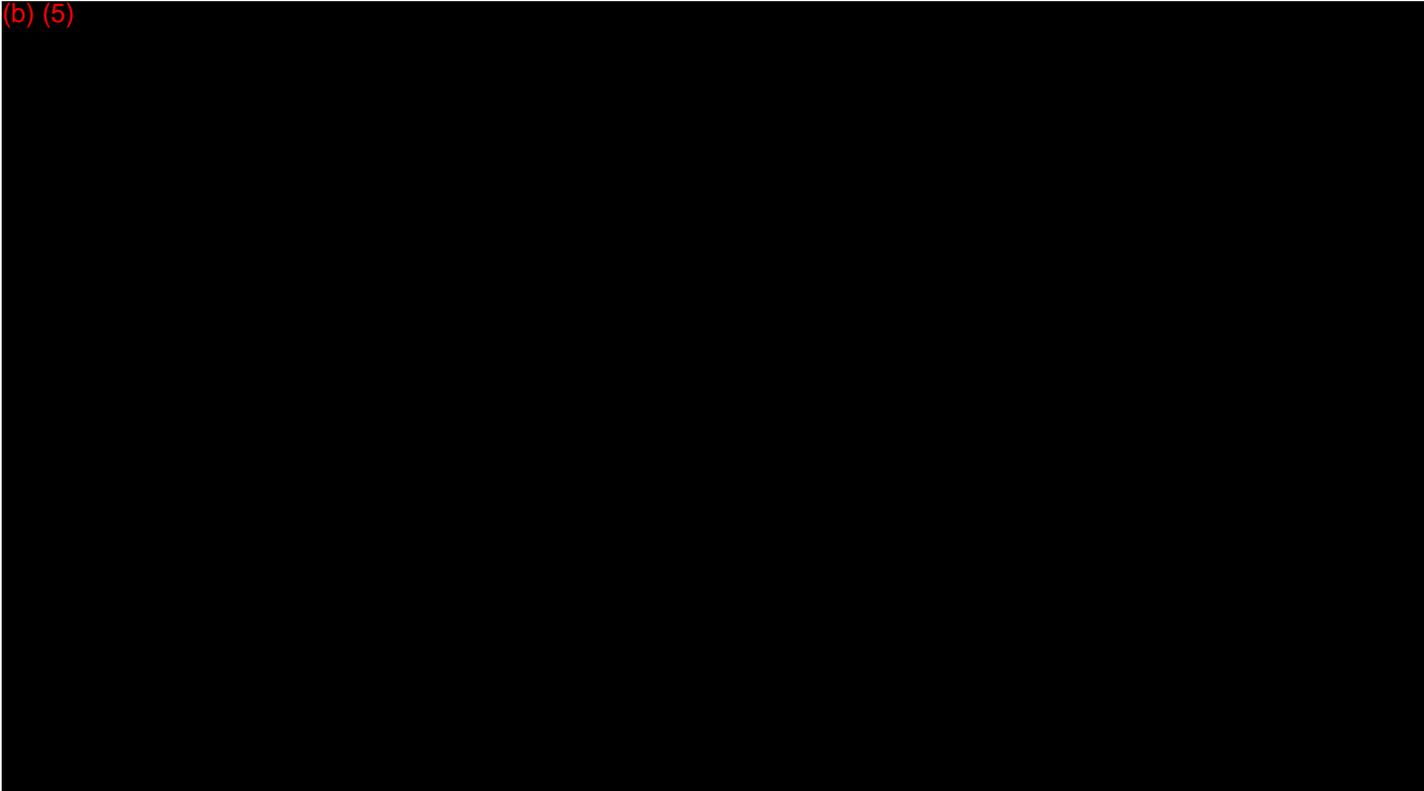
CVE ID No.	Risk Rating	Number of Vulnerabilities Identified
CVE-2008	High	613
CVE-2008	Medium	1,559
CVE-2009	High	1,109
CVE-2009	Medium	1,466
CVE-2010	High	1,529
CVE-2010	Medium	1,797
CVE-2011	High	3,002
CVE-2011	Medium	1,261

Table 4. Total Number of Vulnerabilities by CVE and Year



B. Security Configuration Compliance

We also compared a sample of mandatory DS configuration settings with what is being checked and identified the weaknesses shown in Table 5.



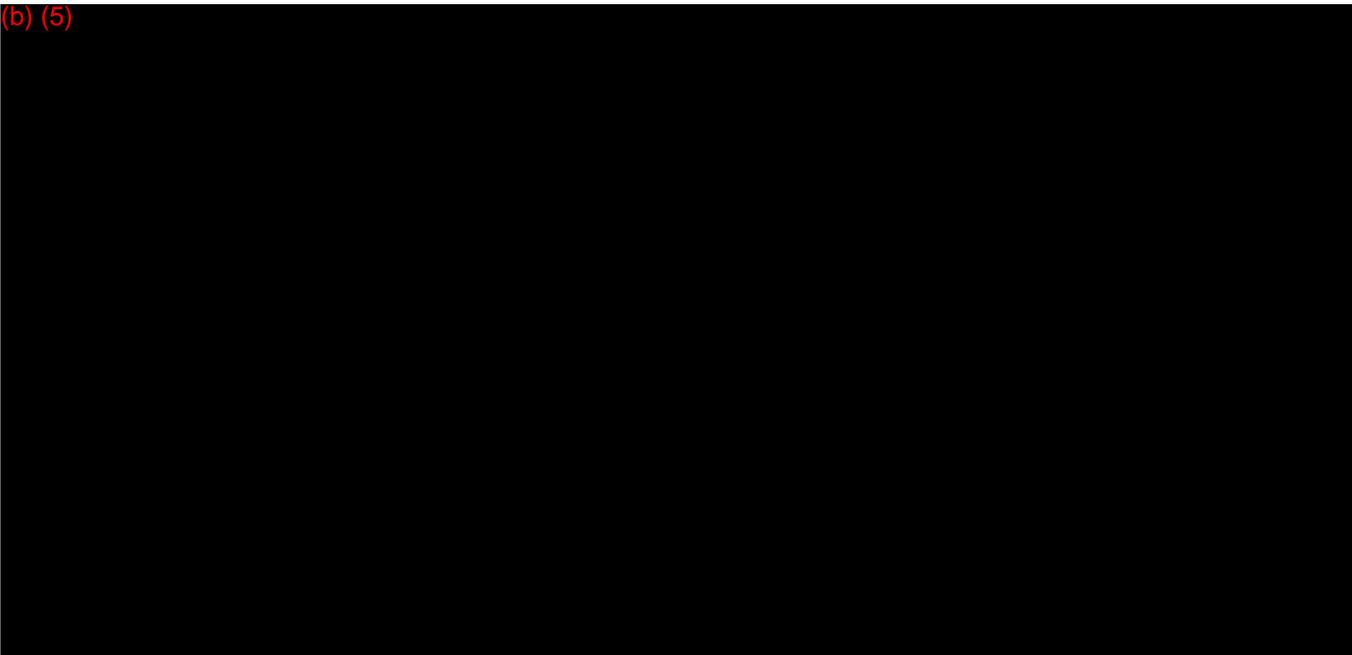
**UNCLASSIFIED**

SMART-SBU	Windows File Permissions for file:	For file: %systemdrive%\AUTOEXEC.BAT The following accounts should have the specified permissions: Account Sid = S-1-5-32-544; name = Administrators; permissions = XRQNWATBUDEPO(full) Account Sid = S-1-5-18; name = System; permissions = XRQNWATBUDEPO(full) Account Sid = S-1-5-32-545; name = Users; permissions = XRQNE(read and execute) No other accounts should have any rights.
MSSMTPDFBE01	%systemdrive%\AUTOEXEC.BAT	

C. Anonymous Logins and Passwords

Although the logical access weaknesses identified in Table 6 are not categorized as high risk, the default passwords were not in accordance with FAM policies.

(b) (5)



**UNCLASSIFIED**

**Appendix F. Systems Without Annual Backup Plan Testing**

As part of the contingency plan testing, we requested annual backup test results for the sample of 25 systems. According to Department of State officials, each system owner is responsible for testing the backup media to verify media reliability and information integrity.

The systems for which system owners did not provide documentation of annual backup tests are shown in Table 1.

**Table 1. Systems Without Annual Backup Plan Testing**

Sample #	Bureau	Name	Package No.	Type	FIPS Categorization	Annual Backup Testing
1	A	ILMS	830	UNCL	M	N
2	A	S-ILMS	2716	CL	H	N
3	CA	IVAMS	97	UNCL	M	N
4	CA	FEP	344	UNCL	M	N
5	CA	PLOTS	346	UNCL	M	N
6	CA	PLMS	4547	UNCL	M	N
7	CA	MIS	724	UNCL	M	N
8	DS	CMS	424	UNCL	M	N
9	HR	GTS	843	UNCL	M	N
10	IRM	TDS	719	CL	H	N
11	IRM	WebPASS	744	UNCL	M	N
12	IRM	SMART - SBU	2743	UNCL	M	N
13	IRM	SMART-C	2744	CL	H	N
14	L	IDMAS	647	UNCL	H	N
15	MED	eMED	299	UNCL	M	N

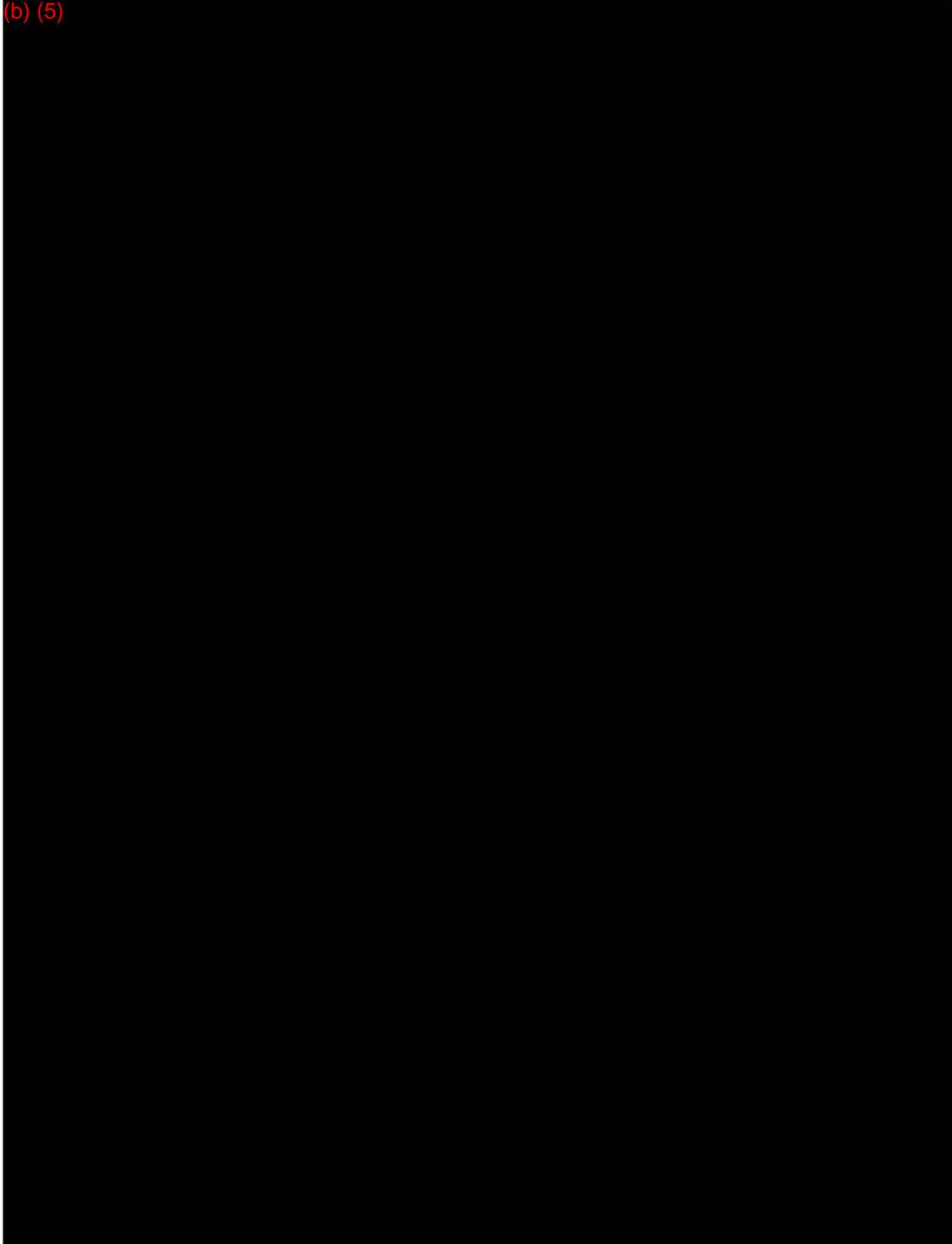
**Legend**

Bureaus	
A – Bureau of Administration	IRM- Bureau of Information Resource Management
CA – Bureau of Consular Affairs	L- Office of the Legal Advisor
DS – Bureau of Diplomatic Security	MED – Office of Medical Services
HR – Bureau of Human Resources	
System Classification and Categorization	
Classification	Categorization
CL- Classified Network	H- High Impact
UNCL- Unclassified Network	M- Moderate Impact

## Appendix G. Servers Without Critical Patches

The 17 servers that did not have critical patches installed are shown in Table 1.

(b) (5)



## Appendix H. Summary of Department of State Continuous Monitoring Controls Compliance With Federal Guidance

Deficiencies noted in the Department of State’s continuous monitoring controls in accordance with Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011, and National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1*, dated February 2010, are shown in Table 1.

**Table 1. Analysis of Continuous Monitoring Compliance With Federal Guidance**

<b>Regulation Source</b>	<b>Continuous Monitoring Components</b>	<b>Implemented</b>	<b>Comment</b>
<b>OMB Memorandum 11-33</b>	Continuous monitoring programs and strategies should address: (i) the effectiveness of deployed security controls;	Partially Implemented	Control deficiencies were noted in the following sections: <ul style="list-style-type: none"> <li>• Risk Management (<b>Finding A</b>)</li> <li>• Configuration Management (<b>Finding B</b>)</li> <li>• Plans of Actions and Milestones (<b>Finding D</b>)</li> </ul>
<b>OMB Memorandum 11-33</b>	(ii) changes to information systems and the environments in which those systems operate; and.	Partially Implemented	Several control deficiencies were noted in configuration management. ( <b>Finding B</b> )
<b>OMB Memorandum 11-33</b>	(iii) compliance to federal legislation, directives, policies, standards, and guidance with regard to information security and risk management. Agencies will be required to report the security state of their information systems and results of their ongoing authorizations through CyberScope in accordance with the data feeds defined by DHS.	Partially Implemented	Based upon the control deficiencies identified in this report, the Department is not in compliance with FISMA regulations.

**UNCLASSIFIED**

<p><b>NIST SP 800-37</b></p>	<p>Configuration management and control processes for organizational information systems</p>	<p>Partially Implemented</p>	<p>Several control deficiencies were noted in configuration management. <b>(Finding B)</b></p>
<p><b>NIST SP 800-37</b></p>	<p>To assess the Security Impact Changes</p>	<p>Implemented</p>	<p>No findings noted.</p>
	<p>To assess the subset of management, technical, and operational controls</p>	<p>Partially Implemented</p>	<p>Three systems [Content Management System (CMS), WebPASS, and SMART-C] did not have an annual assessment of security controls performed as part of its continuous monitoring of annual controls. <b>(Finding A)</b></p>
	<p>Security status reporting to appropriate organizational officials</p>	<p>Partially Implemented</p>	<p>The Department’s Plans of Action and Milestones (POA&amp;M) process is not fully and effectively implemented and the program is not compliant with FISMA and OMB requirements.</p> <p>The Department has not implemented a POA&amp;M process to address and resolve security weaknesses identified on ClassNet GSS.</p> <p>In addition, the evaluation found the Department has not implemented effective corrective actions to address the POA&amp;M control weaknesses within the OpenNet GSS identified in the FY 2010 report <i>Review of the Information Security Program at the Department of State</i>. <b>(Finding D)</b></p>
	<p>Active involvement by authorizing officials in the ongoing management of information system-related security risks.</p>	<p>Partially Implemented</p>	<p>For authority to operate (ATO), which provides proof that an authorizing official approved a system to operate, the evaluation found that nine of 30 systems tested did not have a full security assessment and authorization performed. <b>(Finding A)</b></p>

**UNCLASSIFIED**

**Appendix I. Sample Selection of Information Systems Listed in Information Technology Asset Baseline Used for FY 2011 Evaluation**

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

<b>Name</b>	<b>Acronym</b>	<b>Bureau</b>	<b>Classification</b>	<b>Categorization</b>
Integrated Logistics Management System	ILMS	Bureau of Administration	Unclassified	Moderate
Secure-Integrated Logistics Management System	S-ILMS	Bureau of Administration	Classified	High
Immigrant Visa Allocation Management System	IVAMS	Bureau of Consular Affairs	Unclassified	Moderate
Front End Processor	FEP	Bureau of Consular Affairs	Unclassified	Moderate
Passport Lookout Tracking System	PLOTS	Bureau of Consular Affairs	Unclassified	Moderate
Consular Lookout & Support System	CLASS	Bureau of Consular Affairs	Unclassified	High
Management Information System	MIS	Bureau of Consular Affairs	Unclassified	Moderate
Online Passport Status Service	OPSS	Bureau of Consular Affairs	Unclassified	Moderate
Passport Lockbox Manifest Search	PLMS	Bureau of Consular Affairs	Unclassified	Moderate
Case Management System	CMS	Bureau of Diplomatic Security	Unclassified	Moderate
Security Incident Management and Analysis	SIMAS	Bureau of Diplomatic Security	Unclassified	Moderate
Identity Management System	IDMS	Bureau of Diplomatic Security	Unclassified	Moderate
FSA Eurasia Database	FSA	Bureau of Educational and Cultural Affairs	Unclassified	Moderate
extranet.usembassy.it	EXTRANET	Bureau of European and Eurasian Affairs	Unclassified	Low
Gateway to State	GTS	Bureau of Human Resources	Unclassified	Moderate
Integrated Personnel Management System	IPMS	Bureau of Human Resources	Unclassified	Moderate
Content Management System	CMS (IIP)	Bureau of International Information Programs	Unclassified	Low
United States Embassy Vienna Internet website	USEVI	Bureau of International Organizations	Unclassified	Low
COMSEC Accounting Reporting and Distribution	CARDS	Bureau of Information Resource Management	Classified	Moderate

**UNCLASSIFIED**

System				
Telegram Distribution System	TEDS	Bureau of Information Resource Management	Classified	High
Windows Active Directory	WINAD	Bureau of Information Resource Management	Unclassified	Moderate
OpenNet Plus Transport GSS	OPENNET	Bureau of Information Resource Management	Unclassified	Moderate
Telegram Delivery System	TDS	Bureau of Information Resource Management	Classified	High
Web Post Administrative Software Suite Explorer	WebPASS	Bureau of Information Resource Management	Unclassified	Moderate
SMART Core Messaging-Unclassified	SMART - SBU	Bureau of Information Resource Management	Unclassified	Moderate
SMART Core Messaging-Classified	SMART-C	Bureau of Information Resource Management	Classified	High
Enterprise Data Warehouse	EDW	Bureau of Information Resource Management	Unclassified	Moderate
Integrated Document Management & Analysis System	IDMAS	Office of the Legal Advisor	Unclassified	High
eCountryClearance	eCC	Office of Management Policy, Rightsizing and Innovation	Unclassified	Moderate
Electronic Medical Records System	eMED	Office of Medical Services	Unclassified	Moderate

**UNCLASSIFIED**

**Appendix J. Department of State Response**



United States Department of State

*Chief Information Officer*

*Information Resource Management*

*Washington, D.C. 20520-6311*

November 2, 2011

**UNCLASSIFIED**  
**MEMORANDUM**

TO:           OIG – Mr. Harold W. Geisel

FROM:       IRM – Susan H. Swart 

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

REF:        OIG Memo Dated Oct. 26, 2011 Subject: Draft Report on Evaluation  
of Department of State Information Security Program

Thank you for the opportunity to provide comments on the draft “Report on Evaluation of Department of State Information Security Program Report for 2011” (OIG FISMA report). Our response to the annual OIG FISMA report is attached and was coordinated with the Bureau of Diplomatic Security, Bureau of Administration, Bureau of Human Resources, and the Foreign Service Institute. Please consider this a consolidated reply to your request.

**UNCLASSIFIED**

## Department Response to Draft Report on Evaluation of Department of State Information Security Program

Before addressing individual recommendations, the Department would like to provide a few overview sections to address several themes that run thru this year's OIG FISMA report.

### **1) Use of Continuous monitoring to replace traditional Certification and Authorization:**

The FISMA FY2011 reporting instructions (OMB memorandum 11-33) explicitly offer the Executive Departments and Agencies the authority to substitute an appropriate risk-based continuous monitoring program in lieu of the formerly required reauthorizations that had previously been required every three years. In relevant part, the instructions state:

**Is a security reauthorization still required every three years or when an information system has undergone significant change as stated in OMB Circular A-130?** No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. . . Continuous monitoring programs thus fulfill the three-year security reauthorization requirement, so a separate re-authorization process is not necessary.<sup>1</sup>

The Department chose to implement OMB's guidance and instructions and base ongoing reauthorization of the Department's networks (not applications) on continuous monitoring. The OIG does not concur with the Department's acceptance of this risk, and the FISMA reporting instructions provide instructions for addressing such disagreements. In relevant part, the instructions state:

**Who is responsible for deciding the acceptable level of risk (e.g., the CIO, program officials and system owners, or the IG)? What if they [The CIO and the OIG] disagree?** The agency head ultimately is responsible for deciding the acceptable level of risk for their agency.<sup>2</sup>

**2) Compliance vs. Risk-Based Analysis:** Under the FISMA FY2011 reporting instructions, both the Department and the OIG are required to take a risk-based approach. Applying this principle, compliance of guidelines should only be performed when the risk of non-compliance is assessed. Moreover, simple compliance may not be enough to address risk.

The report faults the Department's risk scoring program because it does not currently include routers and switches. However, the Department did scan its routers and switches to assess vulnerabilities<sup>3</sup> and found a risk score of 7,476 points associated with routers and switches compared to a score of 160,000,000 across all devices originally scanned in 2008. The vulnerabilities posed by routers and switches represent less than 0.005% of total vulnerabilities.

---

<sup>1</sup> OMB M-11-33, FAQ 28.

<sup>2</sup> OMB M-11-33, FAQ 15.

<sup>3</sup> CVEs

If the height of the Washington Monument<sup>4</sup> represented all the risk scored by State's Vulnerability Scanner in iPost as of the summer of 2008, the amount represented by the vulnerabilities on routers and switches today is less than 0.34 inches. While that 0.34 inches is a risk, it is minuscule compared to the metaphorically equivalent of 555 feet of original risk.

Applying the risk-based principles, the Department fully intends to perform a risk-based analysis and prioritize the OIG findings and address the corresponding recommendations accordingly. The Department, again applying the risk-based approach, is obligated to address higher risk issues before addressing OIG findings and recommendations.

**3) Completeness vs. Timeliness:** The traditional FISMA three-year reauthorization process focuses on "completeness" of testing and remediation, largely ignoring timeliness. Likewise, this report focuses on the completeness of the Department's continuous monitoring program, implying the program is inadequate and ineffective if it is not 100% complete.

A current Massachusetts Institute of Technology (MIT) Lincoln Labs study quantifies the tradeoff between completeness and timeliness in reducing security risk on a network. The study shows that a regimen of complete testing annually<sup>5</sup> is only as effective at reducing risk as testing 17% of controls every 2 months.<sup>6</sup> Because the Department's continuous monitoring program is both 3-4 times more complete and 20 times timelier than the second case above<sup>7</sup>, one can reasonably conclude it is more effective than a complete but slow process such as the traditional FISMA three-year authorization process. Timeliness is important because it is commensurate with those who attack our networks - at Internet speed. To prevent attacks, we must be faster at removing weaknesses than they are at exploiting them.

The Department has worked tirelessly to increase the timeliness of detection and remediation of the highest priority weaknesses, which is consistent with both the principles of continuous monitoring and a risk-based approach.

**4) Accuracy of Findings:** In many cases, the Department found the OIG findings significantly overstate the quantitative size of problems. As a result, the Department's management responses state we must first accurately assess the size and nature of the assumed problem, before prioritizing and selecting a management approach.

One example of inaccuracy is located in section E of the draft OIG report. In this section, the OIG documented account types requiring a business justification. However, the OIG did not provide evidence that such a justification was missing. The Department evaluated a small scientifically valid sample of the aforementioned accounts and checked them for a business

---

<sup>4</sup> According to the National Park Service, <http://www.nps.gov/wamo/index.htm>, the Washington Monument is 555 feet and 5 1/8 inches tall.

<sup>5</sup> This is more timely than complete testing of all 800-53 controls every three years, as formerly required by FISMA, and which we assume the OIG would accept as compliant.

<sup>6</sup> This example is based on several assumptions that do apply to State. However they are not addressed here to make this description suitably concise. The Department would be happy to review this study with the auditors.

<sup>7</sup> And 300 times more timely than meeting the former FISMA requirements.

justification. The vast majority had a valid business justification. As such, the OIG draft report overstates the extent of the problem by 380% on one network, and by 1,100% on another.

**5) Conclusions:** The Department disagrees with the OIG on whether continuous monitoring, as currently conducted, produces lower risk than a traditional C&A program, and on the relative importance of completeness and compliance vs. timeliness and risk-based prioritization. Having carefully considered these factors, the Department is convinced its continuous monitoring program, which is 300 times more timely than traditional three-year reauthorizations, produces significantly lower security risk<sup>8</sup> on its networks.

**6) Management Responses to Recommendations:** The remainder of this response provides specific management responses to each of the draft OIG recommendations in the context of the overall comments provided above.

**Recommendation 1: {Section A}** 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.

**Department Response to Recommendation 1:**

The Department does not agree that the lack of meetings poses any material risk to the security of the Department. Moreover, there is no requirement that this voluntarily created internal group meet with recurring frequency. The Department exercised its valid authority<sup>9</sup> to conclude there was no need to meet and believes there is no basis for OIG to substitute its own judgment. The ISSC chairpersons will survey the ISSC membership on reasons to meet, and conduct meetings accordingly.

**Recommendation 2: {Section A}** 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.

**Department Response to Recommendation 2:**

The Department agrees that some increased level of documentation in this area could be beneficial. The Department notes that under the OMB instructions guidance, it is the Department's judgment that shall decide how much documentation is needed to reduce risk.<sup>10</sup> The Department's Designated Authorizing Authority (DAA) will determine the level of documentation adequate to manage risk.

---

<sup>8</sup> Neither produce zero risk, and achieving zero risk is not foreseeable.

<sup>9</sup> OMB M-11-33

<sup>10</sup> *op. cit.*

**Recommendation 3: {Section A}** 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.

**Department Response to Recommendation 3:**

With regard to bullet 2, we note that FISMA FY2011 reporting instructions explicitly removed any such requirement. We quote:

**Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?** No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs.<sup>[1]</sup> (emphasis in original)

Based on this instruction, the Department does not agree with the recommendation in bullet 1.

With regard to bullet 3, the new NIST SP 800-53 guidance was not fully implemented<sup>[2]</sup> until June 2010, and thus compliance was not required for C&As starting before June 2011. All Department C&As commencing after June 2011 will comply with the new version of NIST 800-53/53A. The Department's C&A Toolkit has been fully updated to implement this change. Applying a risk-based approach, the Department does not judge it necessary to retroactively adjust prior C&As to meet this new standard.<sup>[3]</sup>

With regard to bullet 4, the Department performs such annual testing on all its systems, except in rare cases that are vigorously pursued.

**Recommendation 4: {Section B}** 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

---

<sup>[1]</sup> OMB M-11-33, FAQ 28.

<sup>[2]</sup> A new NIST 800-53A was needed to implement the new 800-53, and was not published until June 2010.

<sup>[3]</sup> Authority is OMB M-11-33, FAQ 15.

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.

**Department Response to Recommendation 4:**

The Department notes this recommendation is based on three findings:

- Some “critical” patches were not installed.
- iPost failed to report 100% of required configuration settings.
- Less than 100% of all vulnerabilities are mitigated.

In general, the OIG is using a criterion focused upon completeness, and overlooking timeliness. This is a “compliance-based” approach not consistent with FY2011 FISMA reporting instructions that require both the Department and OIG to assess risk and make judgments of how to best achieve security.

More specifically, the OIG asserts the Department is not checking 100% of configuration settings within the "required" three-year timeframe. Utilizing a risk-based approach, the Department is applying the analysis conducted by MIT Lincoln Labs examining the tradeoff between completeness and timeliness of testing. This study shows the following two conditions have approximately equal risk:<sup>11</sup>

100% completeness every year = 17% completeness every two months
--

Because the Department checks nearly 90% of configuration settings every three days, the Department’s risk is significantly lower than the traditional C&A requirement (100% completeness every three years). In this case, evidence shows timeliness trumps completeness in lowering risk.

The Department examined each of the three OIG findings and determined the findings do not reflect a material increase of risk for reasons documented elsewhere.<sup>12</sup> The Department will continue to assess risk in these areas, and if a material risk to the security of the Department is found, the Department will take appropriate steps.

**Recommendation 5: {Section C}** 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 in accordance with the Information Assurance Training Plan.

<sup>11</sup> Given other assumptions applicable to the Department.

<sup>12</sup> Available for auditor inspection.

**Department Response to Recommendation 5:**

The Department agrees with this recommendation because the condition of not tracking (individually) those who need role-based training creates undue risk for the Department. The Department will develop a method of tracking of who needs and who has received role-based training; comparable to what is available for awareness training (including risk scoring in iPost).

**Recommendation 6: {Section C}** 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 in accordance with the Information Assurance Training Plan.

**Department Response to Recommendation 6:**

The Department has conducted a preliminary study of compliance with annual completion of the PS-800 training course. These preliminary findings show nearly 100% of those who require training receive training within 30 days of the due date. The Department does not consider this level of non-compliance to be a material risk to the security of the Department.

This is especially true, considering there are several other sources of awareness training including the daily awareness program at login, as well as weekly and quarterly sources.

The OIG proposal to automatically suspend account access (without human intervention) has a high risk of creating serious denial-of-service issues and as such, itself poses risks to the security of the Department.

The Department will conduct a complete assessment of compliance in this area and take appropriate action if a material level of non-compliance is indicated.

**Recommendation 7: {Section D}** We recommend that the Chief Information Officer:

- Implement a Plan 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.<sup>13</sup>
- 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*.

---

<sup>13</sup> With regard to POA&Ms this source states "Require a formal Enterprise-level Plan of Actions and Milestones (POA&M) containing: (i) systemic information system and organizational security weaknesses and deficiencies; (ii) risks relating to the identified weaknesses and deficiencies requiring further mitigation; and (iii) specific actions to mitigate identified risks." The Department believes that our POA&M process for ClassNet meets these requirements in all material regards.

- 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.

**Department Response to Recommendation 7:**

The Department has examined the detailed findings supporting the summary statements in this draft document. The Department concludes that the problems identified are not material (or are now being addressed) for the following reasons:

- The Department has a compliant process for tracking POA&M items on ClassNet.
- The Department has started distributing quarterly grades (effective Q1-FY2012) to executive officers, as recommended.
- Quarterly updates to POA&M data are not warranted, unless there has been a change of status. The grading covered under the prior bullet addresses this issue.

The Department notes the iPost system performs many of the functions of a POA&M system at a level of timeliness and detail that the traditional POA&M approach cannot achieve. Given the MIT Lincoln Labs findings on the trade-off between completeness and timeliness discussed previously, the Department concludes that deficiencies in the traditional POA&M system are not a material risk to the security of the Department, given iPost as a compensating control.<sup>14</sup>

**Recommendation 8: {Section E}** 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.

**Department Response to Recommendation 8:**

The Department notes that operational considerations require some accounts to be set “not to expire” and such accounts are scored and noted in iPost. The Department considers this process appropriate.

The Department conducted a preliminary investigation of the accounts identified as deficient by the OIG using a random sample of accounts in each of the remaining categories found. The Department’s study concluded the OIG had overestimated the level of deficiency by 380% on ClassNet and by 1,100% on OpenNet. The Department cannot find a single incident in FY2011 where one of these accounts was compromised. In part, this is because of compensating controls: for example, unauthorized access via guessing of passwords is significantly mitigated by automatically locking accounts after three bad passwords are offered.

---

<sup>14</sup> Authority to make this judgment is provided by OMB M-11-33, FAQ 15.

The Department agrees there is a potential risk with these types of accounts. In December 2011, the Department will commence scoring stale accounts in iPost. The Department will also conduct a more complete assessment of this problem and determine what prioritized mitigation actions are justified by the current level of risk.

**Recommendation 9: {Section F}** 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).

**Department Response to Recommendation 9:**

The deactivation of accounts recommendation is related to Financial Audit findings under the title “Untimely Removal of Inactive or Separated Employees’ User Accounts”. The management response to the related financial audit findings address the deactivation of account issues raised above.

The Department will investigate the other findings within six months to determine their scope and materiality to the security of the Department. This review will use reliable statistical methods, ensuring results may be projected to the population of all accounts from the review. Based upon this review, the Department will determine a risk-based and cost-effective solution to any issues identified. This solution may range from accepting the risk, to further corrective action.

**Recommendation 10: {Section G}** 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*.”

**Department Response to Recommendation 10:**

The Department agrees some increased level of documentation, as called for in recommendation 2, would be valuable.

**Recommendation 11: {Section G}** 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 are to be monitored.

**Department Response to Recommendation 11:**

Regarding bullet 1, the Department notes that implementation of an effective continuous monitoring strategy will require continuous improvement and thus never be completed. The Department's current continuous monitoring implementation is being copied as a model by both other government agencies and the private sector.

Regarding bullet 2, the Department is already engaged in these efforts and will pursue them with an appropriate level of priority. Test scans of routers and switches show that if the height of the Washington Monument represented the total risk in place in the summer of 2008, the risk of "uncovered" routers and switches would be less than 0.34 inches high. The Department will continue to prioritize such risks and expand the coverage of the risk scoring program.

Regarding bullet 3, the Department will continue to expand coverage of risk in iPost in line with the priorities established under bullet 2.

Regarding bullet 4, the Department notes that the continuous monitoring strategy is an enterprise level strategy. Thus, the continuous monitoring strategy does not need to be addressed in detail in every system security plan.

**Recommendation 12: {Section H}** We recommend that the Chief Information Officer, in accordance with 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.

**Department Response to Recommendation 12:**

The Department will:

- Develop a master table of contents for the OpenNet security documentation across sub-systems so that the OIG can find the COOP plans and updates in ON subsections.
- Develop criteria to determine when COOP plans have been adequately addressed in these documents.
- Verify that significant changes to COOP plans are in compliance with the applicable criteria.

**Recommendation 13: {Section H}** 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 in accordance with NIST SP 800-34, Revision 1, “*Contingency Planning Guide for Federal Information Systems.*”

**Department Response to Recommendation 13:**

The Department considers the documents already aligned and will:

- Develop criteria to determine when the BIA and State GSS downtime are adequately coordinated.
- Verify that these criteria are met.

**Recommendation 14: {Section I}** 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.

**Department Response to Recommendation 14:**

The Department will document compliance and/or non-compliance to the OIG findings and take the necessary corrective action.

**Recommendation 15: {Section I}** 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.

**Department Response to Recommendation 15:**

The Department will document compliance and/or non-compliance to the OIG findings and take the necessary corrective action.

**Recommendation 16: {Section J}** 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.

**Department Response to Recommendation 16:**

Regarding bullet 1, the Department will document compliance and/or non-compliance to the OIG findings and take the necessary corrective action.

Regarding bullet 2, the Department does not agree that these assignments require change and thus does not agree with the recommendation.

**Recommendation 17: {Section J}** 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*.

**Department Response to Recommendation 17:**

**UNCLASSIFIED**

UNCLASSIFIED

12

The Department will verify that all Department of State computers at other Federal agencies are clearly documented. (We found no defects with regard to the process for contractor sites.)

**Recommendation 18: {Section J}** 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*.

**Department Response to Recommendation 18:**

The Department does not agree with this recommendation because a) knowing the exact total number of contractors (a continuously changing number) does not have an impact upon the security of the Department, and b) it is not required by M-11-33.

**Recommendation 19: {Section K}** 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.

**Department Response to Recommendation 19:**

The Department agrees with the recommendation, but not the authorities cited and will:

- Track and include a summary report for all obligations and expenditures for all IT projects with a) a material level of funding, or b) significant security risk.
- Include UPIs in the Department's POA&M for each system.

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

Call the Office of Inspector General  
**HOTLINE**  
**202/647-3320**  
**or 1-800-409-9926**  
to report illegal or wasteful activities.

You may also write to  
Office of Inspector General  
U.S. Department of State  
Post Office Box 9778  
Arlington, VA 22219

Please visit our Web site at [oig.state.gov](http://oig.state.gov)

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

**UNCLASSIFIED**

**UNCLASSIFIED**