

UNCLASSIFIED

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

Office of Audits

Review of the Information Security Program at the Department of State

Report Number AUD/IT-10-10, November 2009

~~IMPORTANT NOTICE~~

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

UNCLASSIFIED

UNCLASSIFIED



**United States Department of State
and the Broadcasting Board of Governors**

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability and positive change in the Department of State and the Broadcasting Board of Governors.

This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

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

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

Harold W. Geisel
Deputy Inspector General

UNCLASSIFIED

TABLE OF CONTENTS

Section	Page
EXECUTIVE SUMMARY	1
BACKGROUND.	5
RESULTS OF 2009 FISMA REVIEW.	7
Critical, Volatile, and Inherited Controls Were Not Adequately Identified or Tested	7
Connectivity Between Contractor Systems and Department Systems Was Not Adequately Identified, Tested, and Monitored	9
Contingency Plan Toolkits Should be Improved	12
Management of Configuration Management Controls Process Was Not Adequate	15
Security Weaknesses in iPost Were Not Captured in the Department POA&M Database	17
Information Security Weaknesses Were Not Adequately Managed	19
IT Audit-Related Security Weaknesses Were Not Adequately Managed	21
Security Awareness Training Requirements Were Not Enforced	24
All Employees With Significant Security Responsibilities Did Not Attend Required Role-Based Training	26
Inventory Records Were Materially Correct	27
Incident Management Program Was Adequately Managed	29
Privacy Program Is in Compliance With Federal Requirements and OMB Guidance	30
LIST OF RECOMMENDATIONS	33
ABBREVIATIONS	37
APPENDICES	
A. Scope and Methodology.	39
B. Follow-up of Recommendations From the FY 2008 FISMA Report	41
C. Bureau of Information Resource Management Response	45

EXECUTIVE SUMMARY

In response to the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3545 et seq.), the review team performed an independent evaluation of the information security program at the Department of State (Department). The review team reviewed the Department's progress in addressing FISMA information management and information security program requirements per FISMA and other statutory requirements, including Office of Management and Budget (OMB) guidance. The review team assessed performance in various areas, including certification and accreditation (C&A), plan of action and milestones (POA&M), security awareness and training, configuration management, inventory, incident reporting, and privacy requirements. Since FY 2008, the Department has taken steps to improve management controls to include the following:

- Updated Inventory Toolkits to provide guidance for inventory identification, analysis, and recording. Significant improvements have been made to ensure that inventory is materially correct.
- Effectively managed a decentralized Incident Management Program and reported incidents timely to the United States Computer Emergency Readiness Team (US-CERT).
- Updated the Privacy Impact Assessment template to make it compliant with OMB guidance.

However, further improvements are needed.

- Although the Annual Control Assessment Toolkit was modified in the third quarter of FY 2009 to include a definition of critical and volatile controls and training was provided to systems owners, the Department should work with systems owners to identify critical and volatile controls that should be tested for each application and system; expand the quality control program to include analysis of how well certification testing addresses critical, volatile, and inherited controls; and ensure all controls are tested over a 3-year C&A cycle.
- Although the C&A Toolkits were modified in FY 2009 to instruct systems owners on how to identify external and inter-connections agreements, the Department should supplement the current information provided in the C&A Main Toolkit and Inventory Toolkit to include additional guidance for

annual testing of critical and volatile controls and be more proactive in reviewing Systems Security Plans and test results to ensure compliance with the methodology in the C&A Toolkits.

- Although the Contingency Plan (CP) Toolkits were created in FY 2009, the Department should update them to include requirements that systems owners should review and revise CP following CP failed test results, create POA&M for failed CP control tests, and include verification by the Office of Information Assurance that systems owners are complying with CP Toolkits and methodology.

In addition, the Department should take the following actions:

- Create an Information Security Architecture that outlines information security responsibility for the Department's decentralized information security environment.
- Record and report systemic security weaknesses identified through the iPost/site Scoring process as POA&M actions to ensure that these weaknesses are tracked, prioritized, and remediated.
- Develop a method that ensures that each systems owner provides timely and complete updates to the POA&M database. Validate the information in the Department POA&M database, and review the Corrective Action Plan report before it is submitted to OMB.
- Create a Standard Operating Procedure for managing information technology-related security weaknesses that are identified during Chief Financial Officers Act and Office of Inspector General audits and for Government Accountability Office and OMB Circular A-123, *Management's Responsibility for Internal Control*, reviews.
- Implement methods to globally enforce the security awareness policies, and enhance existing methods to identify users who should take the Cyber Security Awareness Training Course.
- Improve methods to identify individuals with significant security responsibilities, ensure that they take the required training every 3 years, record the training records in the Office of Personnel Management-approved centralized system, and provide management with tools to monitor compliance with the training requirement.

The Toolkits provided guidance and ensured standard processes were used to perform C&A of FISMA-related systems. However, effective monitoring was not performed to ensure that systems owners were complying with established guidance

and methodology. Without active monitoring to ensure compliance, controls not tested for systems or networks may not be working effectively and could expose the Department to loss of confidentiality, integrity, or availability.

Management Comments

In its consolidated response (Appendix C), the Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security and the Bureau of Administration, concurred with the report's nine recommendations. Based on the consolidated response, OIG considers all of the recommendations resolved, pending further action.

UNCLASSIFIED

UNCLASSIFIED

BACKGROUND

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347, title III) recognized the importance of information security to the economic and national security interests of the United States. It 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, contractor, or other 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, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) 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 security controls, FISMA requires agency program officials, Chief Information Officers (CIO), Senior Agency Officials for Privacy, and Inspectors General to conduct annual reviews of the agency's information security program and report the results to OMB.

Annually, OMB provides guidance with reporting categories and questions for meeting the current year's reporting requirements. OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

Objective

In accordance with FISMA, the Office of Inspector General (OIG) initiated an annual review of the Department of State information security program and practices as they relate to FISMA.

UNCLASSIFIED

The objective of the review was to evaluate the progress the Department had made in implementing an effective information security program and related practices since the last OIG annual FISMA review in FY 2008, *Review of the Information Security Program at the Department of State* (AUD/IT-08-36, Oct. 2008).

UNCLASSIFIED

RESULTS OF 2009 FISMA REVIEW

CRITICAL, VOLATILE, AND INHERITED CONTROLS WERE NOT ADEQUATELY IDENTIFIED OR TESTED

In response to an FY 2008 FISMA report recommendation, the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), improved its Annual Control Assessment Toolkit and provided two training workshops in May 2009 for systems owners. The Toolkit provided definitions of what constitute critical and volatile controls as follows:

- Critical Control — Any control is considered critical if the failure of this single control is expected to result in a non-trivial breach of confidentiality, integrity, or availability (denial of service) of information in the system or subsystem.
- Volatile Control — Any control that shows a historical pattern of unreliability. That shall be interpreted to mean any control for the system that has been verified to be working, has subsequently failed, and has not yet been verified to be working again in three subsequent tests over at least 2 years.

The review team found that six (25 percent) of the 23 in-scope high- to moderate-impact systems reviewed documented critical or volatile controls in their test programs but that there was no rationale for selecting and testing these controls. Some systems designated a control as critical, while others showed it either as volatile or as neither. Significant control testing gaps were found for systems that were certified and accredited in the FY 2008 report. Test gaps for these systems were virtually identical to testing gaps for annual testing. For many of the testing gaps identified, test documentation cited the controls as “inherited,” either at the bureau level or from OpenNet. However, the review team found that these controls were not tested at the bureau level and had not been tested by OpenNet. The review team also found that OpenNet did not test or effectively test for the control risks at the bureau or system level. Additionally, the review team reviewed iPost controls as part of the Configuration Management (CM) review and found that while the controls did provide continuous monitoring, they did not compensate for the lack of annual testing for access and other volatile controls at the system level.

Section 2.9.2, “Selection of Security Controls for Monitoring,” of NIST Special Publication (SP) 800-37, revision 1, *Guide for the Security Certification and Accreditation of Federal Information Systems*, states:

The criteria for selecting which security controls to monitor and for determining the frequency of such monitoring should be established by the information system owner or common control provider in collaboration with the authorizing official or designated representative, chief information officer, senior agency information security officer, and risk executive (function). The criteria should reflect the organization’s priorities and importance of the information system (or in the case of common controls, the information systems inheriting the controls) to organizational operations and assets, individuals, other organizations and the Nation in accordance with Federal Information Processing Standards (FIPS) Publication 199, or the Committee on National Security Systems (CNSS) Instruction 1199. Organizations should use risk assessments, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process.

Priority for control monitoring should be given to the security controls that have the greatest volatility (i.e., the greatest potential for change) after implementation and the controls that have been identified in the organization’s plan of action and milestones for the information system.

IRM/IA’s new policy for critical and volatile controls was implemented only in the third quarter of FY 2009. As a result, earlier testing was not compliant with Department policy. IRM/IA’s quality control review did not independently verify that all critical and/or volatile controls were tested annually. IRM/IA relied on information system testers to perform the verification. The review team found that OpenNet’s boundary definition was going through significant changes, which may have contributed to gaps in Enterprise Control testing.

Controls not tested for the systems or network may not be working effectively and could expose Department data to loss of confidentiality, integrity, or availability.

Recommendation 1: The Chief Information Security Officer and the Bureau of Information Resource Management (IRM) should:

- Work with systems owners to identify critical and volatile controls to test and use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009, P1 priority controls as a starting point.
- Establish procedures to verify that volatile controls are correctly determined and tested.
- Expand the IRM quality control program to include analysis of how well certification testing addresses critical, volatile, and inherited controls and to also determine whether all controls are tested over a 3-year certification and accreditation cycle.
- Review inherited control selection procedures and update policy in the Toolkit to ensure that misunderstandings about critical but inherited control testing responsibility are resolved.
- Provide formal guidance on which NIST SP 800-53, revision 3, controls may be inherited from OpenNet and the conditions under which such inheritance will be approved.

Management Response and OIG Reply

IRM concurred with the recommendation, stating that it will update the C&A toolkit to clarify how inherited controls may be selected, update the exit criteria checklist to ensure that inherited controls are selected in a manner consistent with policy, and ask NIST to map controls to the vulnerabilities listed on the National Vulnerability Database. Based on the response, OIG considers the recommendation resolved, pending further action.

CONNECTIVITY BETWEEN CONTRACTOR SYSTEMS AND DEPARTMENT SYSTEMS WAS NOT ADEQUATELY IDENTIFIED, TESTED, AND MONITORED

In response to two FY 2008 FISMA report recommendations, the Department modified the certification and accreditation (C&A) toolkits to instruct systems owners to (a) identify external inter-connections and include copies of required Interconnection Security Agreement (ISA) and Memorandum of Understanding/Agreement (MOU/MOA) documents in the System Security Plan (SSP) and (b) test and verify,

UNCLASSIFIED

at least annually, that interconnection agreements are listed and current in the SSP. The C&A toolkits were modified by IRM/IA to include specific instructions for the following:

- Requesting that systems owners update and add to the SSP any information on ISA, MOU, and MOA interconnections.
- Modifying the inventory data call so that it includes:
 - Reviewing the completeness and content of systems connections identified in SSPs,
 - Accurately assessing the risk that those connections pose to other Department systems, and
 - Verifying (at least annually) that all active connections to/from existing major information systems are completely listed in the SSPs.

The review team found that 13 (57 percent) of 23 in-scope unclassified systems listed MOU/MOA information in their SSPs, as required, as compared with nine (50 percent) of 18 in-scope unclassified systems assessed during the 2008 FISMA review, as shown in Table 1.

Table 1. MOUs in SSPs

Pass/Fail History Table				
CA-3 Information System Connections				
MOUs/Contracts				
	Fiscal Year 2008		Fiscal Year 2009	
	Number	Percent	Number	Percent
Pass	9	50%	13	57%
Fail	9	50%	10	43%
Total	18	100%	23	100%

In FY 2009, the review team found that 11 (48 percent) of the 23 in-scope systems verified and tested CA-3 control requirements compared with seven (39 percent) of 18 in-scope systems tested during the FISMA 2008 review, as shown in Table 2.

Table 2. Verified and Tested C-3 Control

Pass/Fail History Table				
CA-3 Information System Connections				
Control Requirements Verified & Tested				
	Fiscal Year 2008		Fiscal Year 2009	
	Number	Percent	Number	Percent
Pass	7	39%	11	48%
Fail	11	61%	12	52%
Total	18	100%	23	100%

Section CA-3, “Information System Connections,” of NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information System*, July 2008, states the following:

- (i) The organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);
- (ii) The organization authorizes all connections from the external information system through the use of system connection agreements; and
- (iii) The organization monitors and controls the system interconnections on an ongoing basis.

IRM/IA was not monitoring the SSPs to ensure that they were completed correctly and that the CA-3 control was tested. Additionally, the toolkit was not updated timely and communicated to the appropriate systems owners prior to their completing their annual testing.

Systems connections, both internal and external, provide the electronic path for access and interfaces to both operating and application systems. Lack of formal identification, documentation, and testing of these connections might make these systems susceptible to security weaknesses that may impact their integrity and availability.

Recommendation 2: The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should:

- Supplement the current information provided in the Certification and Accreditation (C&A) Main Toolkit and Inventory Toolkit with additional guidance to include at least the following supplemental directives:
 - Federal Information Security Management Act control CA-3 as a requirement in the annual testing list of “critical” or “volatile” controls for all moderate- and high-impact systems.
 - Guidance on how to test and verify that the control is operating effectively.
- Be more proactive in reviewing System Security Plans and test results to ensure compliance with the methodology in the C&A Toolkits.

Management Response and OIG Reply

IRM concurred with the recommendation but stated that it did not believe it should identify a set of critical and volatile controls (C&VC) at the Department level that should be considered C&VC for all systems in the enterprise, and it proposed new criteria. The proposed new criteria would require that the C&A toolkits be modified to provide proper definition of C&VCs and that verification be performed to ensure that C&VCs are identified and tested. Based on the response, OIG considers the recommendation resolved, pending further action.

CONTINGENCY PLAN TOOLKITS SHOULD BE IMPROVED

IRM/IA made improvements to its CP toolkits in response to two FY 2008 FISMA report recommendations. In the third quarter of FY 2009, IRM/IA created the Contingency Plan Test Toolkit, which provided systems owners with clear direction on CP test requirements, including documenting test results. The Toolkit outlined an improved process and provided guidance systems owners needed to conduct CP tests appropriately. However, the review team found that some systems owners did not use the updated Toolkit and that the instructions on the Toolkit did not clearly communicate the requirements. Specifically, the review team found that CPs were not updated after contingency control failures following annual contingency planning test, when significant changes occurred, and when annual tests were performed. Exceptions noted for the 23 in-scope systems reviewed are as follows:

UNCLASSIFIED

1. The Consular Data Information Transfer System (CDITS) had three CP controls that failed in the System Accreditation Report (SAR). The controls that failed should have been identified previously as having failed in FY 2008 testing. These failures were not noted in the CP. The CP was dated August 17, 2009, and the report was dated August 17, 2009.

2. The Global International Narcotics and Law Enforcement (GINL) system had 11 failed CP controls during the SAR dated July 31, 2008. The SSP was dated December 31, 2007, and included failed CP controls. In the comments section, the plan was to be approved by January 2008. The last CP was dated December 31, 2007, and had not been updated to reflect these failed controls. The last CP Test was dated May 22, 2008, and was a “walk-through,” even though the SSP and System Categorization Form (SCF) stated that GINL was a high-risk system. High-risk systems required a “functional” test in addition to a “walkthrough.”

3. The OpenNet Electronic State Configuration Resource (e-SCORE) system was identified in the SSP and SCF as a high risk system and had only a checklist and walkthrough test performed on May 28, 2009. The last Contingency Plan was dated March 21, 2007.

4. The Integrated Document Management & Analysis System (IDMAS) had a CP dated May 2, 2007 (contact names were updated January 30, 2008). However, in the IDMAS Self Assessment dated May 10, 2007, CP-4, CP-5, and CP-7 were documented as “would fail.” IDMAS had two failed CP security controls in the SSP dated January 29, 2008. The Authority to Operate (ATO) dated May 30, 2008, had open CP findings, even though they were identified in the POA&M in May 2008.

5. The Public Key Infrastructure and BLADE (PKI/Blade) system had an Annual Assessment dated July 10, 2009, with no CP findings. In the POA&M report, PKI/Blade had open CP findings. The CP Test was a failover test, dated February 3, 2009, with POA&M findings. The CP was dated November 16, 2008. There was also a Significant Change to the system on May 22, 2009. A Significant Change to the system requires a new CP and test, according to NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires agencies to establish and periodically test the capability to continue providing services within a system based upon the needs and priorities of the system functionality. NIST SP 800-53, revision 2, further requires that agencies test and up-

UNCLASSIFIED

date their systems' CPs at least annually. The Foreign Affairs Manual (FAM) provides guidance on CP, in addition to the guidance provided by the IRM/IA toolkits.

The C&A CP Toolkit did not indicate that CPs were to be updated and reviewed by IA following failures in CP testing or failed testing of CP controls during the systems' annual or C&A tests. Additionally, the toolkit may have been updated too late for most of the systems owners to use during the FY 2009 testing to comply with OMB guidance and NIST requirements.

Without adequate testing of contingency plans, the Department cannot ensure that systems will operate properly or in a timely manner during an emergency or disruption of service. Loss of the Department's IT systems could limit management's ability to perform its missions, including its critical functions in service to the public.

Recommendation 3: The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should take the following actions:

- Update the Contingency Plan (CP) Toolkit to include the requirement that systems owners should review and revise the CP after any CP failed test results.
- Update the CP exit criteria checklist to include verification by the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), that the systems owners:
 - Conduct CP testing in accordance with the system's National Institute of Standards and Technology Special Publication 800-60, revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, availability impact level as indicated on the Security Categorization Form (SCF).
 - Create a Plan of Action and Milestones for each failed CP test/control.
 - Update the CP to address each failed CP test/control (or provide clear documentation explaining why no such update is necessary).
- Update the exit checklists for the six documents listed to include verification by IRM/IA that each document is consistent with the SCF, and modify the SCF checklist to include verification by IA that these documents are updated if the impact level is revised upward. The documents are as follows:
 - The System Security Plan
 - The Contingency Plan
 - The Security Control Assessment Plan (SCAP)
 - The Certification Report
 - The Authority To Operate
 - Future Annual or Certification and Accreditation Tests

Management Response and OIG Reply

IRM concurred with the recommendation, stating that it plans to update the CP Toolkit to include requirements that system owners should review and revise the CP after any failed CP test results and also modify the CP exit criteria checklist to verify that the systems owners are conducting CP tests in accordance with NIST guidance. Based on the response, OIG considers the recommendation resolved, pending further action.

MANAGEMENT OF CONFIGURATION MANAGEMENT CONTROLS PROCESS WAS NOT ADEQUATE

The review team found that implementation and monitoring of configuration management (CM) controls, including the scanning process, were decentralized and shared among bureaus, Information Systems Security Officers (ISSO) , and IRM/IA. Over half of the 23 in-scope systems reviewed showed CM exceptions, based on reviews of SSPs, annual testing results, and routine scanning results as reported in iPost and then used for risk scoring. iPost routinely made scanning results available to systems owners, and the risk scoring reports and associated quarterly notifications to responsible system owners raised the visibility of CM weaknesses and provided roadmaps for correction. The resulting 90 percent reduction in overall risk during the past year was a graphic demonstration of iPost's potential.

The review team found, however, that these centralized controls were not fully integrated with decentralized bureau and system level controls and did not address significant risks as follows:

- Only 90 percent of Windows servers were compliant with Systems Management Server (SMS) reporting requirements, leading to unreliable patch and virus management reporting. Time penalties in risk scoring have had only a limited effect (for example, Automated Biometric Identification System (ABIS) and IT Asset Baseline (ITAB) 877) in inducing local managers to improve performance. Recurring patch management performance issues by some sites as reported in iPost suggested that a stronger approach be considered.
- CM testing was inconsistent. Annual testing by system owners failed to include CM-6 (Configuration Settings), which is a critical and volatile control. The problem was exacerbated by the failure of routine scanning to include database configuration. In three instances where CM-6 controls were tested

as part of recertification (ABIS #877, CDITS #964, and Travel Document Issuance System Inquiry (TDIS) ITAB #89), the system failed CM-6 tests and related critical control tests (Access Controls, Systems Acquisition, and System and Information Integrity: AC-3, AC-6, AC-7, IA-5, SA-6, SA-7, and SI-2). However, other related controls (Audit and Accountability and Identification and Authentication (AU-2 and IA-4)) were successfully tested.

- The scanning tools failed to query Oracle configuration, the Department's most common database system for configuration control weaknesses that could have significant impact on application access controls.
- Scanning results for routers, firewalls, and Demilitarized Zone (DMZ) servers were not available in iPost; therefore, they were not used in risk scoring. Also, outbound e-mail content filtering was not implemented.
- The results from Intrusion Detection Systems (IDS) scanning were not reported in iPost or utilized in risk scoring.
- Risk scores were available for individual Windows hosts and aggregated to the site level based on Active Directory units. The scores were not aggregated by application systems, which would have been useful for business process owners and bureau management.

FISMA¹ requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Standard security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. These controls allow agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information. Agencies are to cite the frequency by which they implemented system configuration requirements and must document and provide NIST with any deviation from common security configurations.

Responsibility for the implementation of CM controls for the systems, operating systems, databases and network, including the scanning process, was decentralized, and the majority of the automated scanning results were not centralized and included in iPost for reporting and risk scoring.

If reporting and risk scores in iPost are not accurately identifying the action risk to systems because the scores were limited to the Windows environment and did not include critical scan results, such as the application databases and the network (firewall, routers, and switches), Department data may be exposed to loss of integrity and confidentiality because configuration standards may not be implemented.

¹ Pub. L. No. 107-347 § 3544(b)(2)(D)(iii).

Recommendation 4: The Chief Information Security Officer, Bureau of Information Resource Management, the Systems Integrity Director of Diplomatic Security, and the Deputy Chief Information Officer for Business Planning and Customer Service should:

- Address the extent to which centralization versus decentralization of control testing, remediation, and management should be readjusted to produce better configuration management (CM).
- Analyze and document the extent to which centralized automation of CM is an efficient and more cost-effective method than the current decentralized method.
- Develop an Information Security Architecture that considers how to request, review, document, and approve CM exceptions that may be necessary to allow the business of the Department of State to be conducted and provide criteria for the decision process.

Management Response and OIG Reply

IRM concurred with the recommendation to create an Information Security Architecture for the Information System Department. Based on the response, OIG considers the recommendation resolved, pending further action.

SECURITY WEAKNESSES IN iPOST WERE NOT CAPTURED IN THE DEPARTMENT POA&M DATABASE

IRM/IA managed a centralized POA&M Department database where security weaknesses from all the various bureaus were identified quarterly, monitored, and used to generate the quarterly reports for OMB reporting. However, systemic security weaknesses identified through the iPost/Site Scoring process were not entered into the Department's POA&M database when they were not resolved immediately. Systemic weaknesses require a broader process/policy/budget change and not just technical mitigation of a particular weakness with existing resources. They may also include weaknesses that might require project management and/or coordinated action among multiple departments or bureaus to resolve.

OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, August 23, 2004, states that the POA&M process was designed to resolve IT security control weaknesses with prioritization to ensure that vulnerabilities are addressed in a timely and cost-effective manner. Memorandum

M-04-25 includes a spreadsheet that should be used as a model to identify and develop specific weaknesses, points of contact, resources required, scheduled completion dates, milestones with attendant completion dates, changes in milestones, and statuses.

FISMA requires that agencies develop POA&Ms to capture weaknesses identified during the C&A process, Office of Inspector General (OIG) or Chief Financial Officers (CFO) Act audits, and internal control reviews. These weaknesses need to be corrected and/or mitigated.

The POA&M process facilitates the remediation of security weaknesses and provides a means of planning and monitoring corrective actions, categorizing risk, defining roles and responsibilities for security weakness resolution, assisting in identifying the resource requirements necessary to mitigate the weaknesses, tracking and prioritizing resources, and informing decision makers. Also, NIST² recommends that the POA&M be updated, stating, “The updates should occur at appropriate intervals to capture significant changes to the information system, but not so frequently as to generate unnecessary paperwork.”

The iPost/Site Scoring process has been in production approximately a year, and the review team found that the process is evolving and has a lot of potential. However, IA has not yet developed a process to report systems systemic weaknesses that are not remediated within a predefined time period into the centralized POA&M database.

The centralized POA&M did not include iPost systemic security weaknesses. Security weaknesses that remain unresolved for an extended period of time may increase vulnerabilities and exposures that could be exploited by intruders, and they may impact the integrity, availability, and confidentiality of the Department’s systems and the network infrastructure.

Recommendation 5: The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to accomplish the following:

- Record systemic security weaknesses identified through the iPost/Site Scoring process as Plan of Action and Milestones (POA&M) actions to ensure the weaknesses are tracked, prioritized, and remediated.
- Report POA&M actions on a quarterly basis for sites that have low scores, requiring them to raise those scores.
- Report POA&M actions for risk covered by iPost scoring “exceptions.”

² NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Management Response and OIG Reply

IRM indicated concurrence with the recommendation to record systemic security weaknesses identified in iPost in the Department POA&M database, but it expressed “reservations” about the statement that all technical weaknesses must be closed and that iPost scoring is not part of the POA&M process. Based on the response, OIG considers this recommendation resolved, pending further action.

INFORMATION SECURITY WEAKNESSES WERE NOT ADEQUATELY MANAGED

IRM/IA and the respective bureaus need to improve management of security weaknesses. The review team found that policies, procedures, and tools are in place to track, maintain, update, validate, and prioritize security weaknesses at each of the respective bureaus. Also, quarterly updates from the respective bureaus’ databases were consolidated in the Department database that was managed by IA. However, the review team found that active monitoring, validation, and implementation of remediation steps to correct the security weaknesses were not performed by the respective bureaus or by IA, as was reported in the FY 2008 FISMA report.

POA&Ms were not updated when there was a change in status. The review team found that the FY 2009 third quarter Corrective Action Plan (CAP) that was sent to OMB showed that the Bureau of Consular Affairs (CA) had 28 POA&M actions with “120 days overdue” dates, which was over 50 percent of the POA&M action items listed on the CAP report. Discussions with management and a review of the CA POA&M database revealed that many of these items had been corrected, but the POA&M status was not updated before these items were reported to CAP and issued to OMB.

FISMA requires that agencies develop POA&Ms to capture weaknesses identified during the C&A process, OIG or CFO Act audits, and internal control reviews. These weaknesses need to be corrected and/or mitigated. The POA&M process facilitates the remediation of security weaknesses and provides a means for planning and monitoring corrective actions, categorizing risk, defining roles and responsibilities for security weakness resolution, assisting in identifying the resource requirements necessary to mitigate the weaknesses, tracking and prioritizing resources, and informing decision makers. Also, NIST³ recommends that the POA&M be updated, stating, “The updates should occur at appropriate intervals to capture significant changes to the information system, but not so frequently as to generate unnecessary paperwork.”

³ NIST SP 800-37.

According to the FAM:⁴

Quarterly, systems owners must review and update their plan-of-action-and-milestones (POA&M) tool:

- (1) POA&M reports must list residual risks and remediation efforts associated with the information systems under their control (see 5 FAM 814 for definition of system owner);
- (2) Failure to submit quarterly POA&M updates may result in loss of funding and could lead to loss of accreditation and termination of the program.

According to IA management, there had been several personnel changes in the functional area that managed the POA&M process. As a result, there had been a lack of oversight to ensure that bureaus were in compliance with POA&M policies and guidelines.

Security weaknesses that remain unresolved for an extended period of time may increase vulnerabilities and exposures that could be exploited by intruders and may impact the integrity, availability, and confidentiality of systems and the network infrastructure. Without a POA&M process that validates that security weaknesses were remediated timely, management could not ensure that its systems were adequately secured and protected.

Recommendation 6: The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to implement the following:

- Coordinate with systems owners to develop a method that ensures that each systems owner provides timely and complete updates to the Plan of Action and Milestones (POA&M) databases and to relevant officials, including the Bureau of Information Resource Management, Office of Information Assurance (IA), on a regular basis (Recommendation 4 in the FY 2008 FISMA report).
- Ensure that IA management implements a process to validate information in the Department of State POA&M database and performs a quality review on the Corrective Action Plan report before it is submitted to the Office of Management and Budget.

⁴ 5 FAM 1063.5c, "Reporting."

Management Response and OIG Reply

IRM concurred with the recommendation, stating that it will perform a quality assurance review before submitting the CAP to OMB and will provide “formal quarterly grade letters” to bureaus on the quality of their POA&M process implementation. Based on the response, OIG considers the recommendation resolved, pending further action.

IT AUDIT-RELATED SECURITY WEAKNESSES WERE NOT ADEQUATELY MANAGED

The review team noted there were no Standard Operating Procedures (SOP) for managing IT-related security weaknesses identified during CFO and OIG audits and GAO and OMB Circular A-123, *Management's Responsibility for Internal Controls*, reviews:

- OIG provided an extract of its Compliance Analysis and Tracking System (CATS) database to IRM/IA using codes that were provided by IRM/IA. The CATS database did not include an attribute to indicate whether an OIG recommendation was IT related. Because of the lack of this identifier, IRM/IA had to manually review the extract provided by OIG and then import the recommendations deemed to be related to IT into IRM/IA's Department-level (POA&M) database. There was no evidence that a root cause analysis was performed and that these recommendations were actionable with milestones and scheduled completion dates.
- Audits conducted by external auditors were not included in the CATS database. According to the OIG, IT recommendations from the A-123 reviews were provided directly to IRM, and IRM was responsible for distributing the recommendations to the responsible bureaus and importing them into the Department POA&M database. No formal documented procedures existed to process these recommendations, and there was no evidence that a root cause analysis was performed and that these recommendations were actionable with milestones and scheduled completion dates.
- IT audit recommendations resulting from CFO audits of IT general and application controls for financial accounting application systems were sent directly to IRM/IA and imported into the Department's POA&M database. There was no evidence that a root cause analysis was performed and that these recommendations were actionable with milestones and scheduled completion dates.

UNCLASSIFIED

The review team found that no formal process and no centralized process for identifying and managing IT-related audit findings existed. Overlaps were not identified and jointly managed, and recommendations that impacted both IT and business processes were not analyzed for root cause and addressed in a collaborative way by both IRM/IA and the respective bureaus. In most instances, the review team found that recommendations or Notices of Potential Recommendations (NFR) were not analyzed for root cause and actionable with milestones before they were imported into the POA&M Department database.

FISMA requires that agencies develop POA&Ms to capture weaknesses identified during the C&A process, OIG and CFO Act audits, and internal control reviews. These weaknesses need to be corrected and/or mitigated. The POA&M process facilitates the remediation of security weaknesses and provides a means for planning and monitoring corrective actions, categorizing risk, defining roles and responsibilities for security weakness resolution, assisting in identifying the resource requirements necessary to mitigate the weaknesses, tracking and prioritizing resources, and informing decision makers. Also, NIST recommends that the POA&M be updated, stating, "The updates should occur at appropriate intervals to capture significant changes to the information system, but not so frequently as to generate unnecessary paperwork."

The FAM⁵ defines responsibilities of the Assistant Secretary for Resource Management and Chief Financial Officer that include the following:

- (7) Provides advice and technical assistance in developing necessary guides for performing risk assessments and management control reviews and designing management control systems;
- (8) Approves subsequent plans for risk assessments and reviews of management control systems;
- (9) Establishes and maintains a program of quality assurance over management control evaluations, reviews, and follow-up corrective actions;
- (10) Recommends Management Control Steering Committee action on proposed management control designs;
- (11) Ensures that appropriate follow-up action is taken on management control deficiencies and financial losses by providing necessary guidance in designing needed additional controls;
- (12) Maintains a continuing liaison with and awareness of the activities of other Department elements having responsibilities for activities that contribute to the goals and objectives of the management control program; and

⁵ 2 FAM 022.3, "The Assistant Secretary for Resource Management and Chief Financial Officer."

UNCLASSIFIED

(13) Reviews Government Accountability Office, Inspector General, contractor, or management reports that apply in whole or in part to management controls; reviews the analyses that Information Resource Management (IRM) performs, which focuses on automated systems (general and application controls); and ensures that risk assessments, management control reviews, and determinations of deficiencies consider these sources of information.

The OIG database did not have an attribute that uniquely tagged each IT recommendation to facilitate the process for IRM/IA to extract only IT-related recommendations in the Department POA&M database. Each OIG functional area submitted its IT-related audit findings or recommendations to IRM/IA, and no formal SOP existed to identify root causes and turn these weaknesses into POA&M actionable items.

Some IT-related recommendations may not be tracked in the OIG database and imported into the POA&M database. Additionally, there may be duplicate efforts or lack of efforts to jointly manage and implement controls to remediate IT-related findings from OIG, GAO, and CFO audits and A-123 reviews. Without an effective process that ensured that these security weaknesses were tracked and remediated timely, management did not have assurance that its systems were adequately secured and protected. This may impact the integrity, availability, and confidentiality of systems and the environment.

Recommendation 7: The Chief Financial Officer, Bureau of Information Resource Management, and systems owners should work together to develop, publish, and implement detailed Standard Operating Procedures (SOP) for addressing information technology (IT) audit-related weaknesses and findings. These SOPs should define the following:

- Clear objectives and criteria on what should be actionable and tracked in the Office of Information Assurance Plan of Action and Milestones (POA&M) Department of State database and how duplicated findings or findings that include business processes and multiple bureaus should be addressed in a collaborative effort among various parties.
- Responsibilities for each functional area in reviewing the findings or recommendations or notices of potential findings and turning them into actionable items to include root cause analyses, proposed actionable solutions, responsible parties for implementing the solutions, and milestones/tasks, including reasonable, scheduled completion dates, before they are imported into the POA&M Department database.

Management Response and OIG Reply

IRM concurred with the recommendation to work with CFO and Circular A-123 auditors to create SOPs for addressing information technology audit-related weaknesses, as recommended. Based on the response, OIG considers the recommendation resolved, pending further action.

SECURITY AWARENESS TRAINING REQUIREMENTS WERE NOT ENFORCED

The Department has developed and implemented information security policies and procedures, including several information security awareness programs, to comply with NIST requirements and OMB guidance. The policy requires that all users take the web-based Cyber Security Awareness Course within 10 days of being granted log-in access to OpenNet (Department of State Network). The review team found that all users with access to OpenNet did not take the PS800 Cyber Security Awareness Course within 10 days of access to OpenNet or annually by their course anniversary date. Users were reminded of this requirement, most recently in 08 All Diplomatic and Consular Posts telegram (ALDAC) 087187 and Department Notice 2008_08_060. The review team found that enforcement of this requirement was not uniform from site to site. The Department used Active Directory (AD) to identify all OpenNet users who were required to take the course. OIG reported to OMB in FY 2008 that 55,000 (81 percent to 95 percent) employees and contractors had taken the Cyber Security Awareness Course. IRM reported that as of September 1, 2009, the State Department had 70,000 OpenNet users, and the Bureau of Diplomatic Security reported that 67,800 users (97 percent) had taken the Cyber Security Awareness course.

FISMA requires that agencies have sufficiently trained personnel to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines. FISMA also states that the required agency-wide information security program “shall include security awareness training to inform personnel, including contractors, of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks.” NIST SP 800-53, revision 2, recommends that basic security awareness training be provided to all new information systems users (employees and contractors) before granting them log-in privileges to the system. It also states that employees should be provided with security awareness training annually to remind them of their responsibilities to protect information assets.

Enforcement of the PS800 Cyber Security Awareness course completion requirement was a decentralized function at the ISSO level. The Department’s policy to

revoke a user's access to the network if the course was not taken within 10 days of access to OpenNet or annually by the employee's course anniversary date was not mandatorily enforced by all ISSOs. The existing link between AD and the PS800 Cyber Security Database did not ensure that all users added to AD were also in the database. The ISSOs were responsible for notifying employees within their functional area of responsibility of the requirement to complete the course.

Security awareness training educates employees about the methods the agency has implemented to protect information assets, the controls implemented, and the risks to the organization if those controls are compromised. Employees who are not properly trained about computer security may cause, contribute to, or become victims of vulnerabilities or security breaches, such as e-mail exploits, account or password sharing, inadequate safeguarding of passwords or computer resources, Internet misuse, corporate espionage, and social engineering.

Recommendation 8: The Director of the Foreign Service Institute and the Director of the Office of Computer Security, Bureau of Diplomatic Security, should:

- Implement methods to globally enforce the security awareness policies to suspend a user's access if the Cyber Security Awareness Course is not taken within 10 days of access to the Department of State Network or annually by the employee's anniversary date.
- Enhance already existing connectivity between Active Directory (AD) and the Course so that each time a user is created in AD, the user's identification is also registered in the Cyber Security database per Diplomatic and Consular Posts telegram ALDAC 087187 and Department Notice 2008_08_060.
- Provide additional monitoring tools for the Information Systems Security Officers to ensure user compliance with established policies.

Management Response and OIG Reply

IRM concurred with the recommendation, stating that it will implement methods globally to enforce the security awareness policy, integrate information in the Active Directory with information in the Cyber Security Awareness database, and provide ISSOs with monitoring tools to ensure compliance with Information Security Awareness policies. Based on the response and the actions already taken, OIG considers the recommendation resolved, pending further action.

ALL EMPLOYEES WITH SIGNIFICANT SECURITY RESPONSIBILITIES DID NOT ATTEND REQUIRED ROLE-BASED TRAINING

The Department developed and implemented a “role-based information assurance training program” to meet the federal requirements under FISMA and OPM guidance. The FY 2007 Information Assurance Training Plan identified and provided specific training courses for the following identified roles: Executives, Senior Level Managers, Program Managers and IT Security Managers, Auditors, Technical Security Personnel, and Other IT Security Roles.

All training records were stored in an OPM-approved centralized system, the “Student Training Management System” (STMS). This system tracked all registrations and course completions for only courses identified in the Information Assurance Plan. However, it did not track courses that are Department paid that employees take yearly to meet continuing professional education requirements. Management did not receive a report periodically showing which training courses employees with significant security responsibilities had attended. Of the sampled selections of 15 U.S.-based ISSOs with significant security responsibilities, five (33.33 percent) had not attended any training courses in the past 3 years, two of whom were branch chiefs. All 14 sampled international ISSOs had attended at least one role-based training course in the past 3 years per the plan’s requirement. This year, the CIO reported to OMB that only 24 percent (1,008 of 4,135) of the employees and contractors with significant security responsibilities had attended role-based training in FY 2008.

OMB guidelines and NIST SP 800-16, *Information Technology Training Requirements: Role- and Performance-Based Model*, April 1998, require that agencies identify employees with significant security responsibilities and provide specialized training. FISMA mandates that agencies implement IA training to enhance awareness of all personnel and to ensure the protection of the agency’s information assets. Among the CISO responsibilities is the need to ensure sufficient IA training for all Department systems users. This includes general awareness training, as well as specific role-based training, for those with significant information security responsibilities. The IA training plan defined guidelines for Department information system security awareness and training. In addition, the plan provided guidance on identifying employees with significant information security responsibilities and the recommended training associated with these responsibilities.

The review team found that controls did not exist to identify and monitor annually training for employees with significant security responsibilities. Department managers were not provided periodic reports from the STMS that showed requirements and compliance with training requirements.

Employees with significant security responsibilities were tasked with implementing, enforcing, and monitoring compliance with the Department's security policies and guidelines. Without ensuring that annual training needs are met, these personnel may be unaware of their security responsibilities or be improperly prepared to effectively perform those duties.

This increases the risk of a computer security incident that could result in loss, destruction, or misuse of sensitive data and resources.

Recommendation 9: The Bureau of Diplomatic Security Assistant Director of Training, the Bureau of Information Resource Management Chief Information Security Officer, and bureau systems owners should work together to:

- Improve methods to identify individuals with significant security responsibilities;
- Notify these individuals, including employees, supervisors, managers, and executives, of their role-based training requirement;
- Monitor compliance with the training requirements;
- Provide management with reports that show compliance with the training requirement; and
- Modify the Student Training Management System to capture other training programs, such as those paid for by the Department, to meet Continuing Professional Education requirements (for example, CISSP designation).

Management Response and OIG Reply

IRM concurred with the recommendation, stating it will consider methods to identify who has significant security responsibilities and develop methods to communicate and monitor compliance with training requirements. Based on the response, OIG considers the recommendation resolved, pending further action.

INVENTORY RECORDS WERE MATERIALLY CORRECT

In response to four FY 2008 FISMA report recommendations relating to inventory systems management and oversight of contractor systems, IRM/IA modified its

procedures for collecting, analyzing, and managing inventory systems. The review team found that IRM/IA had implemented several controls procedures that were reviewed and verified during the team's analysis of 3rd and 4th quarter inventory records. Specifically, the following controls were implemented:

- The inventory toolkits were updated to provide guidance on inventory identification, analysis, and recording. The FY 2009 inventory data call provided increased focus on defining and identifying “contractor systems” and “system connections” that were missing in FY 2008.
- The FY 2009 inventory data call was initiated in early November 2008.
- Routine quarterly inventory data calls were made, and they reminded bureau and post systems owners to report new systems and significant changes to systems to ensure the accuracy of their FISMA-reportable inventory.

FISMA requires the Department to keep an inventory of information systems. OMB Circulars A-123, A-127 (*Financial Management Systems*), and A-130 (*Management of Federal Information Resources*) require agencies to develop and maintain an information systems inventory, document the types of information systems required to be reported, and detail how and how often those reports must be submitted to OMB. FIPS Publication 199 requires that agencies categorize their information systems as low-, moderate-, or high-impact. Systems with privacy-related information automatically raise the systems to the level of “Major Information Systems,” thereby needing to be reported in the information system inventory.

In FY 2009, the inventory process included quarterly (as opposed to annually in FY 2008) data calls to identify, qualify, and quantify all information systems in use at each bureau and overseas post. The process was intended to identify the universe of information systems and IT assets such as networks (general support systems), applications, and websites. IRM/IA used the results of the data call to populate two primary databases: the IT Asset Baseline (ITAB) and the FISMA Inventory Database. ITAB stored the universe of the Department's IT assets inventory and was used to track and report the IT assets managed by the Department. The FISMA Inventory Database stored information on identified major information systems that are FISMA reportable. IRM/IA analyzed the data in the ITAB database with the asset owner in order to identify the major information systems that should be reported in the inventory as those evaluated for FISMA compliance.

The inventory information included in the Department's 3rd quarter inventory records was the basis for selection of the systems that were used to perform tests based on OMB guidelines. Selected for in-scope testing were 23 high- and moderate-

impact systems, consisting of 18 from the prior year's in-scope sample and five additional systems, which the review team assumed contained PII data. The 18 systems from the prior year were included in the sample because the review team believed that an analysis of these systems would provide a method for judging what improvements had been made in the C&A process and also to verify implementation of the FY 2008 recommendations. The review team found the inventory to be materially correct with no management recommendations.

INCIDENT MANAGEMENT PROGRAM WAS ADEQUATELY MANAGED

The review team found that even though incident response management was decentralized, well-defined procedures existed and the process was well coordinated and operated effectively in the past 2 years. The computer incident response team (CIRT), within DS, was the center of the Department's incident response program. CIRT's efforts to safeguard the Department's networks involved collaboration and information sharing with other program officials within DS, including the Cyber Threat Analysis Division (CTAD) and the Virus Incident Response Team (VIRT). In addition, CIRT officials coordinated with IRM's Firewall Team and Enterprise Network Management Operations Center, systems managers, ISSOs, regional computer security officers, and the privacy team. CIRT worked cohesively with these entities to identify threats; monitor networks; identify, analyze, and report anomalies; implement corrective action; and identify trends to improve the security posture for the Department.

FISMA requires agencies to establish procedures for detecting, reporting, and responding to security incidents. NIST SP 800-61, revision 1, *Computer Security Incident Handling Guide*, March 2008, provides guidance to agencies on establishing an effective incident response program. The guidance focuses on four phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. OMB Circular A-130, Appendix III, requires agencies to develop SSPs. SSPs are an overview of the security requirements of the system and describe the controls in place or planned to meet those requirements. The SSPs also delineate the responsibilities for and the expected behavior of all individuals who access the system. The SSP is organized into three general classes of security controls: management, operational, and technical. Incident reporting is part of the operational security controls.

To verify that security incidents were reported timely to the US-CERT,⁶ as required by Department policy, the review team obtained and reviewed DS CIRT

⁶ US-CERT is the operational arm of the National Cyber Security Division at the Department of Homeland Security.

monthly and daily reports for the months of October 2008 and January and April 2009. The review team found that in October, 14 PII tickets were identified and reported to US-CERT, as required; in January, five Information Security tickets were identified and reported to US-CERT, as required; and in April, five PII tickets and one unauthorized access ticket were reported to US-CERT. A few minor exceptions were identified in April, but the review team was able to resolve the issues with supporting e-mail documentation from CIRT.

PRIVACY PROGRAM IS IN COMPLIANCE WITH FEDERAL REQUIREMENTS AND OMB GUIDANCE

At the Department of State, the Assistant Secretary for Administration is the Senior Agency Official for Privacy and is responsible for implementing privacy programs. The Privacy Division managed and operated a privacy program in compliance with OMB policies and guidance and developed and documented adequate, compliant policies for safeguarding privacy-related information. Privacy training is provided to employees but is not mandatory.

Privacy guidance and provisions for all Federal agencies are described in section 208 of the E-Government Act of 2002⁷ and OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003. Per the E-Government Act of 2002, agencies are required to conduct privacy impact assessments (PIA) for electronic information systems and collection and make the assessments publicly available. Further, the agency must post privacy policies on agency Web sites and translate privacy policies into a standardized machine-readable format. OMB Memorandum M-03-22 provides additional guidance to the agencies and directs agencies to conduct reviews of how information about individuals is handled within their respective agency when they use electronic means to collect new information or when agencies develop or buy new systems to handle collections of PII.

The Privacy Division created a new PIA template with a guide to assist systems owners in developing required PIAs and tools for identifying and mitigating privacy risks. The review team obtained and reviewed the new PIA template and found that it addressed all applicable privacy OMB-required content. For each of the 23 in-scope systems, the review team determined whether a PIA should have

⁷ Pub. L. No. 107-347, 44 U.S.C., ch. 36.

been completed, the new PIA template was used, and the template was completed correctly in accordance with the guidelines. The review team found that five of the in-scope systems did not contain PII and did not require a PIA; eight systems used the new template and were completed correctly; and of the eight that did not use the new template, three of these eight did not state clearly what PII data was collected. According to the Privacy Officer, a program was implemented in response to the FISMA FY 2008 review to update the PIA template in FY 2009 and to use a 3-year approach to migrate all existing PIAs to the updated template as the systems are recertified. Based on advice from the review team, the Privacy Officer agreed to accelerate implementation of the new PIA template.

UNCLASSIFIED

UNCLASSIFIED

LIST OF RECOMMENDATIONS

Recommendation 1: The Chief Information Security Officer and the Bureau of Information Resource Management (IRM) should:

- Work with systems owners to identify critical and volatile controls to test and use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009, P1 priority controls as a starting point.
- Establish procedures to verify that volatile controls are correctly determined and tested.
- Expand the IRM quality control program to include analysis of how well certification testing addresses critical, volatile, and inherited controls and to also determine whether all controls are tested over a 3-year certification and accreditation cycle.
- Review inherited control selection procedures and update policy in the Toolkit to ensure that misunderstandings about critical but inherited control testing responsibility are resolved.
- Provide formal guidance on which NIST SP 800-53, revision 3, controls may be inherited from OpenNet and the conditions under which such inheritance will be approved.

Recommendation 2 : The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should:

- Supplement the current information provided in the Certification and Accreditation (C&A) Main Toolkit and Inventory Toolkit with additional guidance to include at least the following supplemental directives:
 - Federal Information Security Management Act control CA-3 as a requirement in the annual testing list of “critical” or “volatile” controls for all moderate- and high-impact systems.
 - Guidance on how to test and verify that the control is operating effectively.

- Be more proactive in reviewing System Security Plans and test results to ensure compliance with the methodology in the C&A Toolkits.

Recommendation 3 : The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should take the following actions:

- Update the Contingency Plan (CP) Toolkit to include the requirement that systems owners should review and revise the CP after any CP failed test results.
- Update the CP exit criteria checklist to include verification by the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), that the systems owners:
 - Conduct CP testing in accordance with the system's National Institute of Standards and Technology Special Publication 800-60, revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, availability impact level as indicated on the Security Categorization Form (SCF).
 - Create a Plan of Action and Milestones for each failed CP test/control.
 - Update the CP to address each failed CP test/control (or provide clear documentation explaining why no such update is necessary).
- Update the exit checklists for the six documents listed to include verification by IRM/IA that each document is consistent with the SCF, and modify the SCF checklist to include verification by IA that these documents are updated if the impact level is revised upward. The documents are as follows:
 - The System Security Plan
 - The Contingency Plan
 - The Security Control Assessment Plan (SCAP)
 - The Certification Report
 - The Authority To Operate
 - Future Annual or Certification and Accreditation Tests

Recommendation 4: The Chief Information Security Officer, Bureau of Information Resource Management, the Systems Integrity Director of Diplomatic Security, and the Deputy Chief Information Officer for Business Planning and Customer Service should:

- Address the extent to which centralization versus decentralization of control testing, remediation, and management should be readjusted to produce better configuration management (CM).

- Analyze and document the extent to which centralized automation of CM is an efficient and more cost-effective method than the current decentralized method.
- Develop an Information Security Architecture that considers how to request, review, document, and approve CM exceptions that may be necessary to allow the business of the Department of State to be conducted and provide criteria for the decision process.

Recommendation 5: The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to accomplish the following:

- Record systemic security weaknesses identified through the iPost/Site Scoring process as Plan of Action and Milestones (POA&M) actions to ensure the weaknesses are tracked, prioritized, and remediated;
- Report POA&M actions on a quarterly basis for sites that have low scores, requiring them to raise those scores.
- Report POA&M actions for risk covered by iPost scoring “exceptions.”

Recommendation 6: The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to implement the following:

- Coordinate with systems owners to develop a method that ensures that each systems owner provides timely and complete updates to the Plan of Action and Milestones (POA&M) databases and to relevant officials, including the Bureau of Information Resource Management, Office of Information Assurance (IA), on a regular basis (Recommendation 4 in the FY 2008 FISMA report).
- Ensure that IA management implements a process to validate information in the Department of State POA&M database and performs a quality review on the Corrective Action Plan report before it is submitted to the Office of Management and Budget.

Recommendation 7: The Chief Financial Officer, Bureau of Information Resource Management and systems owners should work together to develop, publish, and implement detailed standard operating procedures (SOP) for addressing information technology (IT) audit-related weaknesses and findings. These SOPs should define the following:

- Clear objectives and criteria on what should be actionable and tracked in the Office of Information Assurance Plan of Action and Milestones (POA&M)

Department of State database and how duplicated findings or findings that include business processes and multiple bureaus should be addressed in a collaborative effort among various parties.

- Responsibilities for each functional area in reviewing the findings or recommendations or notices of potential findings and turning them into actionable items to include root cause analyses, proposed actionable solutions, responsible parties for implementing the solutions, and milestones/tasks, including reasonable, scheduled completion dates, before they are imported into the POA&M Department database.

Recommendation 8: The Director of the Foreign Service Institute and the Director of the Office of Computer Security, Bureau of Diplomatic Security should:

- Implement methods to globally enforce the security awareness policies to suspend a user's access if the Cyber Security Awareness Course is not taken within 10 days of access to the Department of State Network or annually by the employee's anniversary date.
- Enhance already existing connectivity between Active Directory (AD) and the Course so that each time a user is created in AD, the user's identification is also registered in the Cyber Security database per Diplomatic and Consular Posts telegram ALDAC 087187 and Department Notice 2008_08_060.
- Provide additional monitoring tools for the Information Systems Security Officers to ensure user compliance with established policies.

Recommendation 9: The Bureau of Diplomatic Security Assistant Director of Training, the Bureau of Information Resource Management Chief Information Security Officer, and bureau systems owners should work together to:

- Improve methods to identify individuals with significant security responsibilities;
- Notify these individuals, including employees, supervisors, managers, and executives, of their role-based training requirement;
- Monitor compliance with the training requirements;
- Provide management with reports that show compliance with the training requirement; and
- Modify the Student Training Management System to capture other training programs, such as those paid for by the Department, to meet Continuing Professional Education requirements (for example, CISSP designation).

ABBREVIATIONS

AD	Active Directory
ATO	Authority to Operate
C&A	certification and accreditation
CA	Bureau of Consular Affairs
CAP	Corrective Action Plan
cdits	Consular Data Information Transfer System
CFO	Chief Financial Officers
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIRT	Computer Incident Response Team
CM	Configuration Management
CNSS	Committee on National Security Systems
CP	Contingency Plan
CPE	Continuing Professional Education
Department	Department of State
DS	Diplomatic Security
FAM	Foreign Affairs Manual
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IA	Office of Information Assurance
IDS	Intrusion Detection Systems
IG	Inspector General
IRM	Information Resource Management
IRM/IA	Office of Information Assurance, IRM
ISA	Interconnection Security Agreement

UNCLASSIFIED

ISSO	Information System Security Officers
IT	information technology
NIST	National Institute of Standards and Technology
MOU/MOA	Memorandum of Understanding/Agreement
OIG	Office of Inspector General
OMB	Office of Management and Budget
OpenNet	Department of State internal network (intranet)
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	plan of action and milestones
PTA	Privacy Threshold Analysis
RM	Bureau of Resource Management
SAR	System Accreditation Report
SCAP	Security Control Assessment Plan
SCF	System Categorization Form
SMS	Systems Management Server
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team

UNCLASSIFIED

APPENDIX A

SCOPE AND METHODOLOGY

The scope of the review was limited to the Inspector General's reporting categories (as listed) and questions included in Office of Management and Budget (OMB) Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, August 20, 2009. The reporting categories included the following:

- Inventory
- Certification and Accreditation (C&A), Security Controls Testing, and Contingency Plan Testing
- Evaluation of Agency Oversight of Contractor Systems and Quality of Agency Inventory
- Evaluation of the Agency's Plan of Action and Milestones (POA&M) Process
- Inspector General (IG) Assessment of the C&A Process
- IG Assessment of the Agency's Privacy Program and Privacy Impact Assessment (PIA) Process
- Configuration Management
- Incident Reporting
- Security Awareness Training
- Peer-to-Peer File Sharing

The review team conducted this review in accordance with OMB guidance and Federal Information Security Management Act of 2002 (FISMA) recommendations, which required that the team plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the review objectives. To accomplish this, the review team did the following:

- Reviewed prior FISMA reports and their supporting work papers.
- Interviewed Department of State Information System management to gain an understanding of the policies, procedures, and controls used to implement FISMA and OMB guidelines.

- Reviewed policies and procedures posted on the Department's intranet, OpenNet.
- Documented its understanding of the environment.
- Obtained third quarter inventory records. Made a judgmental selection of 23 systems for the in-scope FY 2009 testing. The sample of 23 consisted of 18 systems from the previous year (FY 2008) and five new systems from the current year that may have interfaces with other systems and contain personally identifiable information.
- Obtained and analyzed supporting evidence from management to determine whether the policies, procedures, and controls implemented operated effectively during the fiscal year.
- Obtained and analyzed evidence to determine whether management had implemented corrective actions to close prior years' audit findings and recommendations.

During the review, the review team documented and communicated to management issues identified through Notices of Potential Finding and Recommendations. These notices were communicated to the Department management, who concurred with all of them.

APPENDIX B

FOLLOW-UP OF RECOMMENDATIONS FROM THE FY 2008 FISMA REPORT

The review team reviewed actions implemented by management to mitigate the control gaps identified in the FY 2008 FISMA report. The current status of each of those recommendations is as follows:

Recommendation 1: The Chief Information Officer should reschedule annual inventory data call activities to allow sufficient time to complete the analysis of pending items prior to the annual FISMA review.

2009 Status – Closed. Inventory analysis started in November 2008, with quarterly updates performed in 2009.

Recommendation 2: The Chief Information Officer should ensure that system owners are provided with improved guidance for properly identifying contractor-owned or -operated systems and how to report them for systems inventory purposes.

2009 Status – Closed. Improved guidance was provided in inventory ToolKits, and follow-up was performed by the Bureau of Information Resource Management, Office of Information Assurance.

Recommendation 3: The Chief Information Officer should ensure that national security systems are properly classified and accounted for by the Bureaus of Information Resources Management and Diplomatic Security in their respective Federal Information Security Management Act inventories.

2009 Status – Closed. Only one national security system was found in the wrong inventory system during an analysis of the inventory systems. This was not an exception.

Recommendation 4: The Chief Information Officer should coordinate with systems owners to develop a method to ensure that each systems owner provides

timely and complete updates to plans of action and milestones databases and relevant officials, including the Bureau of Information Resource Management, Office of Information Assurance, on a regular basis.

2009 Status – This is a repeat recommendation from the FY 2008 report. It has become Recommendation 6 in the FY 2009 report.

Recommendation 5: The Chief Information Officer should develop and test system connection agreement control (NIST SP 800-53 control CA-3) between Department system owners and external connection system owners to serve as a compensating control for systems security plan testing.

2009 Status – Partially implemented. This recommendation was combined with Recommendation 10, which was also partially implemented, and has become Recommendation 2 in the FY 2009 report.

Recommendation 6: The Chief Information Officer should review the security control testing program to ensure that all critical controls are identified and tested at least annually for high and moderate risk systems.

2009 Status – Partially implemented. This recommendation has become Recommendation 1 in the FY 2009 report.

Recommendation 7: The Chief Information Officer should update its policy on contingency planning to require that contingency plan test results be incorporated into an updated system contingency plan.

2009 Status – Partially implemented. This recommendation was combined with Recommendation 8, which was also partially implemented, and has become Recommendation 3 in the FY 2009 report.

Recommendation 8: The Chief Information Officer should provide guidance to system owners to ensure that contingency plan test results are adequately documented and incorporated, as needed, into the plans of action and milestone process.

2009 Status – Partially implemented. This recommendation was combined with Recommendation 7, which was also partially implemented, and has become Recommendation 3 in the FY 2009 report.

Recommendation 9: The Chief Information Officer should develop and document a process for management and oversight of contractor-owned and/or -operated information systems. This documented process should include, at a minimum, the process for identifying and describing the interconnectivity between contractor systems and the Department.

2009 Status – Closed. Improved guidance was provided in inventory Toolkits and follow-up was performed by the Bureau of Information Resource Management, Office of Information Assurance.

Recommendation 10: The Chief Information Officer should develop and maintain Interconnection Security Agreements and Memoranda of Understanding/Agreements in System Security Accreditation files.

2009 Status – Partially implemented. This recommendation was combined with Recommendation 5, which was also partially implemented, and has become Recommendation 2 in the FY 2009 report.

Recommendation 11: The Chief Information Officer should establish a process to monitor and validate security awareness training provided to those individuals without access to Department networks.

2009 Status – Open.

UNCLASSIFIED

UNCLASSIFIED

APPENDIX C

BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE



United States Department of State

Washington, D.C. 20520

November 18, 2009

MEMORANDUM

TO: OIG – Mr. Harold W. Geisel (Acting)

FROM: CIO – Janice Fedak, Acting

SUBJECT: Draft Report on Review of the *Information Security Program at the Department of State* (AUD/IT-XX-XX)

Thank you for the opportunity to provide comments on the draft FISMA Report for 2009.

IRM's responses to the recommendations in the draft FISMA 2009 report are attached.

IRM/IA acknowledges that the OIG did not close recommendation 11 from the FY 2008 FISMA Report this year. IRM will continue to work with the OIG to obtain resolution.

IRM's response to the draft FISMA 2009 report has been coordinated with Bureau of Diplomatic Security and Bureau of Administration. Please consider this a consolidated response.

List of Recommendations

Recommendation 1

The Chief Information Security Officer, Bureau of Information Resource Management (IRM) should:

- Work with systems owners to identify critical and volatile controls to test and use National Institute of Standards (NIST) Special Publication (SP) 800-53, revision 3, *Recommended Security Controls for Federal Information Systems*, August, 2009, P1 priority controls as a starting point.
- Establish procedures to verify that volatile controls are correctly determined and tested.
- Expand the IRM quality control program to include analysis of how well certification testing addresses critical, volatile, and inherited controls and to also determine whether all controls are tested over a 3-year certification and accreditation cycle.
- Review inherited control selection procedures and update policy in the Toolkit to ensure that misunderstandings about critical but inherited control testing responsibility are resolved.
- Provide formal guidance on which NIST SP 800-53, revision 3, controls may be inherited from OpenNet and the conditions under which such inheritance will be approved.

IRM Response:

IRM notes that the reservations and observations about critical and volatile controls stated in the response to recommendation 8, also apply here.

IRM proposes the following criteria to close these recommendations:

- Recommendation elements 1-3 shall be considered completed when recommendation 8 is closed.
- IRM will update policy in the C&A toolkit to clarify how inherited controls may be selected, and to better document more clearly where responsibility for the inherited control lies. In addition we will clarify that even if some part of the control is inherited, there may be an additional need for local controls, and encourage system owners to consider this.
- IRM will modify its exit criteria checklists to verify that:
 - Inherited controls have been selected in a manner consistent with policy.
 - No system specific part of the control has been overlooked.
 - The combination of inherited control and any system specific part of the control is adequate to meet 800-53 (or other security requirement) if properly implemented.
 - The system owner knows who is responsible for each inherited control and can verify whether the inherited control is working.
- IRM will ask NIST to map 800-53 controls to the vulnerabilities listed in the National Vulnerability Database (NVD). If NIST is unable to do this, IRM will attempt a mapping

and document the results. IRM notes that if each federal agency does such a mapping independently, the odds that the conclusions of each agency will be even broadly similar is low. The lack of a mapping is a significant national problem that would best be addressed by NIST or OMB.

- IRM will map non-NVD controls included in site scoring to 800-53 and document the results.

Recommendation 2

The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should:

- Supplement the current information provided in the Certification and Accreditation (C&A) Main Toolkit and Inventory Toolkit with additional guidance to include at least the following supplemental directives:
 - Federal Information Security Management Act control CA-3 as a requirement in the annual testing list of “critical” or “volatile” controls for all moderate- and high-impact systems.
 - Guidance on how to test and verify that the control is operating effectively.
- Be more proactive in reviewing System Security Plans and test results to ensure compliance with the methodology in the C&A Toolkits.

IRM Response:

In numerous conversations, the OIG suggests that it believes that IRM should identify a set of critical and volatile controls (C&VC) at the Department level that would be considered C&VC for all systems in the enterprise. Because IRM has not done this, the OIG has identified C&VCs which it believes meet these criteria, and evaluated the Department against these controls.

IRM is not convinced that it can meaningfully identify C&VCs without considering the specifics of each system. But it is willing to reconsider this question over the next few months.

IRM thanks the OIG for suggesting what they consider to be C&VCs. We note however, that last year when IRM asked NIST senior staff whether they agreed with the OIG’s proposed definitions from last year, they did not. We also note that NIST was unable to provide any practical guidance to better define these terms. In the absence of such guidance, IRM has provided operational definitions of C&VCs, within the discretion provided (required) by NIST. We note that every Federal agency is using a different definition from the others. This makes implementing the intent (not to mention the letter) of the NIST guidance practically impossible.

IRM proposes the following criteria to close this recommendation:

- IRM will review the candidate C&VCs proposed by the OIG, and consider whether they should be adopted by the Department.

- Special consideration shall be given to control CA-3, which is of special concern to the OIG.
- The decision and rationale for selecting C&VCs at the Department level shall be documented in a memorandum for the file.
- The toolkits involved with testing C&VCs will be modified to state more emphatically and explicitly that they must be tested in accordance with 800-53A. IRM believes that 800-53A provides more than adequate guidance in this area.
- IRM will add criteria in its exit criteria checklists to verify that:
 - C&VCs have been correctly identified for each system in the SSP.
 - The C&VCs selected are consistent with the Department's definitions.
 - The C&VCs are included in each annual test.
- The definition of volatile controls shall be clarified because the OIG found the following definition to be ambiguous:

The current definition: "Any control that shows a historical pattern of unreliability. This shall be interpreted to mean any control for a system that has been verified to be working, subsequently failed, and has not yet been verified to be working again in three consecutive subsequent tests over at least 2 years."

The definition should be changed to: "Any control that shows a historical pattern of unreliability. This shall be interpreted to mean that if a control fails a test (after it is initially verified to be working) then it shall be considered volatile for at least two years. To be removed from the volatile list it must pass at least three consecutive tests successfully, and there must be at least 24 months between the first and last of these passed tests."

Recommendation 3

The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should:

- Update the Contingency Plan (CP) Toolkit to include the requirement that systems owners should review and revise the CP after any CP failed test results.
- Update the CP exit criteria checklist to include verification by the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), that the systems owners:
 - Conduct CP testing in accordance with the system's National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, availability impact level as indicated on the Security Categorization Form (SCF).
 - Create a Plan of Action and Milestone for each failed CP test/control.
 - Update the CP to address each failed CP test/control (or provide clear documentation explaining why no such update is necessary).

- Update the exit checklists for the six documents listed to include verification by IRM/IA that each document is consistent with the SCF, and modify the SCF checklist to include verification by IA that these documents are updated if the impact level is revised upward. The documents are as follows:
 - The System Security Plan
 - The Contingency Plan
 - The Security Control Assessment Plan (SCAP)
 - The Certification Report
 - The Authority To Operate
 - Future Annual or Certification and Accreditation Tests

IRM Response:

IRM proposes the following criteria to close this recommendation:

- Update the Contingency Plan Toolkit to include the requirement that systems owners review and revise the Contingency Plan following any Contingency Plan failed test results.
- The contingency plan exit criteria checklist will be modified to verify that:
 - Contingency Plan testing is conducted in accordance with the system's NIST SP 800-60 availability impact level as indicated on the Security Categorization Form (SCF).
 - A POA&M action was created for each failed contingency plan tests/control.
 - The contingency plan was updated to address each failed contingency plan tests/control (or that clear documentation is provided explaining why no such update is necessary).
- The exit checklists for each of the following documents will be modified to verify that each document is consistent with the System Categorization Form. The SCF checklist will be modified to verify that these documents are updated if the impact level is revised upward.
 - The System Security Plan
 - The Contingency Plan
 - Security Control Assessment Plan (SCAP)
 - Certification Report
 - Authority To Operate
 - Future Annual Tests

Recommendation 4

The Chief Information Security Officer, Bureau of Information Resource Management, and the Senior Coordinator for Security Infrastructure Directorate should:

- Address the extent to which centralization versus decentralization of control testing, remediation, and management should be readjusted to produce better configuration management (CM).
- Analyze and document the extent to which centralized automation of CM is an efficient and more cost-effective method than the current decentralized method.
- Develop an Information Security Architecture that considers how to request, review, document, and approve CM exceptions that may be necessary to allow the business of the Department of State to be conducted and provide criteria for the decision process.

IRM Response:

IRM notes that

- The findings, while true, do not always imply that the Department is either non-compliant or deficient.
- The OIG assumes that the Department has no ability to accept risk for selected detailed exceptions, an assumption we reject.
- We are not convinced that the cause and effect are connected.

Further, we note that the level of insight into configuration management allowed by iPost and Site Scoring has allowed the Department to significantly reduce these problems over the last year. This has been a major success which seems more significant than the weaknesses found.

Further, we note that auditors assertions that critical and/or volatile controls were not tested is based on the auditor's judgment of what is critical and/or volatile, while by NIST standards, that is the Department's decision to make, consistent with criteria defined by the Department.

Nevertheless, IRM concurs with the recommendation, and proposes the following criteria to close the recommendation:

- IRM/BPC/EAP will address the extent to which decentralization vs. centralization of control testing, remediation, and management should be readjusted to produce better configuration management.
- As part of this analysis, IRM/BPC/EAP in coordination with IRM/IA and DS/SI/CS, shall document the extent to which centralized automation of configuration management is a more effective and cost efficient method than the current de-centralized manual processes.
- As a corollary, the architecture shall consider how to request, review, document and approve configuration management exceptions that may be necessary to allow the business of the Department to be conducted, and provide criteria for the decision process.

Recommendation 5

The Chief Information Security Officer, Bureau of Information Resource Management, will work with systems owners to accomplish the following:

- Record systemic security weaknesses identified through the iPost/Site Scoring process as Plan of Action and Milestones (POA&M) actions to ensure the weaknesses are tracked, prioritized and remediated.
- Report POA&M actions on a quarterly basis for sites that have low scores, requiring them to raise those scores.
- Report POA&M actions for risk covered by iPost scoring “exceptions.”

IRM Response:

IRM has two reservations about recommendation 5. Note: IRM has the same reservations concerning recommendation 1.

Reservation 1: The OIG’s recommendation seems to contend that all technical weaknesses must be closed.

The OIG recommendation is admirable, but is counter to the existing guidance governing Department and Agencies. As an example, when OMB implemented the FDCC standard, it allowed Departments and Agencies to partially adopt the standard, in effect allowing Departments to manage some risk. In practice, Department of State network systems have adopted the same policy. As long as overall risk is at an acceptable level, the Department of State policy is that the site owner may accept certain risks as necessary for business operations.

While one cannot waive 800-53 controls, Departments and Agencies do have the option to implement standards that accept residual risk from other controls which (though desirable) may not have been met. No POA&M is needed if the Department decides to accept risks

Reservation 2: The OIG recommendation seems to contend that the iPost scoring system is not part of the POA&M process.

IRM refutes this contention based upon the fact iPost is an integral extension of the POA&M process, and is much stronger than similar processes implemented at any other identified Federal agency.

Notwithstanding these reservations, discussions with the OIG suggest that there are actions the Department can and should take to address these broad concerns, without 100% agreement with the NFR. IRM proposes the following management decision. IRM will:

- Record systemic security weakness identified through the iPost/Site Scoring process as POA&M actions to ensure closure of the systemic weakness. Systemic weaknesses are those which require a broader process/policy/budget change, and not just technical mitigation of a particular weakness with existing resources. Systemic weaknesses also include those which might require project management and/or coordinated action among multiple offices to resolve.
- Record POA&M actions on a quarterly basis for sites that have low scores, requiring them to raise those scores. This action will be in addition to the process of sending failure letters to site managers, which is already proving to be effective.
- Record POA&M actions for risk covered by iPost scoring “exceptions”.
- Not record POA&M actions for individual technical weaknesses.

- Not assume that all risks must be mitigated, as long as overall risk is kept at a level which the Department chooses to accept.

Recommendation 6

The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to implement the following:

- Coordinate with systems owners to develop a method that ensures that each systems owner provides timely and complete updates to the Plan of Action and Milestones (POA&M) databases and to relevant officials, including the Bureau of Information Resource Management, Office of Information Assurance (IA), on a regular basis (Recommendation 4 in the FY 2008 FISMA report).
- Ensure that IA management implements a process to validate information in the Department POA&M database and performs a quality review on the Correction Action Plan report before it is submitted to the Office of Management and Budget.

IRM Response:

IRM suggests that this recommendation will be closed when IRM meets the criteria proposed earlier for closing Recommendation 4 from the FY 2008 FISMA review.

IRM/IA is still continuing to work on the response for Recommendation 4 from the FY 2008 FISMA review. Beginning in the 3rd quarter of 2010, formal quarterly grade letters will be sent to Bureaus on the quality of Bureau POA&M process implementation. IA will also perform a quality assurance review prior to submitting the CAP to OMB.

Recommendation 7

The Chief Information Officer, Bureau of Information Resource Management and systems owners should work together to develop, publish, and implement detailed Standard Operating Procedures (SOP) for addressing information technology (IT)-audit related weaknesses and findings. These SOPs should define the following:

- Clear objectives and criteria on what should be actionable and tracked in the Office of Information Assurance's (IA) Plan of Action and Milestones (POA&M Department database and how duplicated findings or findings that include business processes and multiple bureaus should be addressed in a collaborative effort among various parties. Responsibilities for each functional area in reviewing the findings or recommendations or notices of potential findings and turning them into actionable items to include root cause analyses, proposed actionable solutions, responsible parties for implementing the solutions, and milestones/tasks, including reasonable, scheduled completion dates, before they are imported into the POA&M Department database.

The review team also recommends that OIG modify its Compliance Analysis and Tracking System database to include a field that flags IT recommendations that should be imported into the Department's POA&M database.

IRM Response:

IRM notes that no evidence is presented to document the finding that the OIG Compliance Analysis and Tracking Systems (CATS) database has recommendations related to IT that should clearly be in the POA&M database, but are not.

IRM concurs with the findings and will work toward resolution to the extent of its ability to do so. It should be noted that not all of the auditors mentioned in the recommendation work for the Department.

IRM recommends the following criteria to close the parts of this recommendation that are the responsibility of the Department:

- IRM will work with the OIG, CFO Auditors, and A-123 auditors on an SOP, as recommended. Either an SOP will result, or the IRM will document why it has not been possible to develop a joint SOP.
- If the OIG is able to add a field to CATS which flags recommendations that need to be tracked in the POA&M system, we will gladly use it to decide which items to track.
 - We recommend that the SOP to be developed jointly would include clear and objective criteria to decide what should be tracked.
- For each security-related IT audit recommendation to be tracked in the POA&M system, IRM/IA will include the following in the POA&M system (if documented in the audit report and/or management comments):
 - A root cause analysis (which will be included in the POA&M Finding text box),
 - Proposed actionable solution (required now),
 - Responsible parties (required now),
 - Tasks and scheduled completion dates (required now).
- IRM acknowledges that not all current POA&M actions are defined as "actionable" (with clearly defined exit criteria), but we are working to improve this.

Recommendation 8

The Director of the Office of Computer Security, Bureau of Diplomatic Security in coordination with the Director of the Foreign Service Institute should:

- Implement methods to globally enforce the security awareness policies to suspend a user's access if the Cyber Security Awareness Course is not taken with 10 days of access to the Department of State Network or annually by the employee's anniversary date.

- Enhance already existing connectivity between Active Directory (AD) and the Course so that each time a user is created in AD, the user's identification is also registered in the Cyber Security database per Diplomatic and Consular Posts telegram ALDAC 087187 and Department Notice 2008_08_060. Provide additional monitoring tools for the Information Systems Security Officers to ensure user compliance with established policies.

IRM Response:

IRM proposes the following criteria to close this recommendation:

- Active Directory will be standardized to identify which user accounts correspond to primary user accounts per ALDAC 087187 and Department Notice 1008_08_060. The ALDAC and Department Notice have been issued and is attached.
- This data from active directory will be matched to and integrated with awareness training completion data from FSI, in iPost.
- An iPost report/screen will show when additional awareness training is needed for each primary user account.
- Primary user accounts without adequate security awareness training shall be assigned a significant risk score that increases over time.

Recommendation 9

The Bureau of Diplomatic Security, Assistant Director of Training, the Bureau of Information Resource Management, Chief Information Security Officer, and the bureau system owners should:

- Improve methods to identify individuals with significant security responsibilities;
- Notify these individuals including employees, supervisors, managers, and executives of their role-based training requirement;
- Monitor compliance with the training requirements;
- Provide management with reports that show compliance with the training requirement; and
- Modify the Student Management Training System to capture other training programs, such as those paid for by the Department, to meet Continuing Professional Education requirements (for example, CISSP designation).

IRM Response:

The Department proposes the following criteria to close this recommendation:

- The Department will consider (and adopt, as appropriate) improved methods to identify who has significant security responsibilities.
- DS and IA will develop methods to notify individuals (including employees, supervisors/managers, and Executives) with significant security responsibilities of needed training.
- DS and IA will develop methods to incentivize bureaus to ensure that their staff who need role-based training obtain it on a timely basis.

- These methods will be documented in the Department of State IA Training Plan.
- The methods will be implemented.

Department Notice: Annual Cyber Security Awareness Online Course

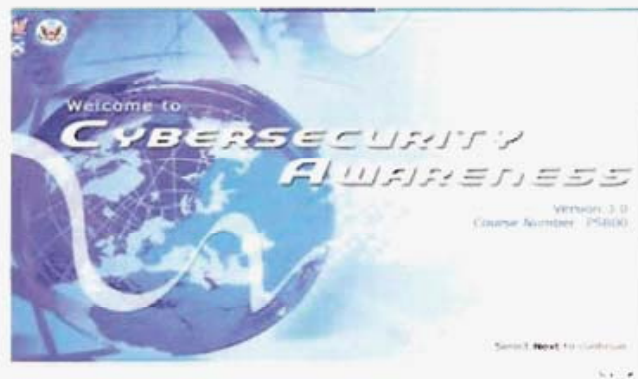
Page 1 of 1

United States Department of State

Department Announcement

Office of Origin: DS/EX
Announcement Number: 2008_08_060
Date of Announcement: August 14, 2008

Annual Cyber Security Awareness Online Course



All Department of State computer users are required to complete and pass the annual online Cyber Security Awareness course (PS800) before the one-year anniversary of their last cyber awareness test. Any user that fails to meet this requirement may have their OpenNet Plus access revoked, pending completion of the course and exam.

To register and take the course and exam online, please click on the link below and follow the instructions:

<http://fsi.state.gov/fsi/sait/default.asp?Cat=Awareness%20Training>.

If you have questions about the course, please contact: awareness@state.gov.

If you have technical problems with the course, please contact: fsicshelpdesk@state.gov.

Please visit the Office of Computer Security's website for updated information on computer security policies, procedures, and news at: <http://cs.ds.state.gov>.

[◀ Return to previous page](#)

Telegram

Page 1 of 2

UNCLASSIFIED STATE 00087187

VZCZCXRO9966

RR RUEHAG RUEHAO RUEHAP RUEHAT RUEHBC RUEHBI RUEHBL RUEHBZ RUEHCD
RUEHCHI RUEHCI RUEHCN RUEHDA RUEHDE RUEHDF RUEHDT RUEHDO RUEHED RUEHEL
RUEHFK RUEHFL RUEHGA RUEHGD RUEHGH RUEHGI RUEHGR RUEHHA RUEHHM RUEHHO
RUEHHT RUEHIHL RUEHIK RUEHJO RUEHJS RUEHKN RUEHKR RUEHKS RUEHKUK
RUEHKW RUEHLA RUEHLH RUEHLN RUEHLZ RUEHMA RUEHMC RUEHMJ RUEHMR RUEHMRE
RUEHMT RUEHNAG RUEHNG RUEHNH RUEHNL RUEHNP RUEHNZ RUEHPA RUEHPB RUEHPD
RUEHPOD RUEHPT RUEHPW RUEHQO RUEHRD RUEHRG RUEHRN RUEHROV RUEHRS
RUEHTM RUEHTRO RUEHVC RUEHVK RUEHYG

DE RUEHC #7187 2262254

ZNR UUUUU ZZH

R 132249Z AUG 08

FM SECSTATE WASHDC

TO ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE

RUEHTRO/AMEMBASSY TRIPOLI 2236

BT

UNCLAS STATE 087187

FOR ALL USERS, ISSOS, IMOS, RCSOS

E.O. 12958: N/A

TAGS: ASEC, AADP, AMGT

SUBJECT: Annual Cyber Security Awareness Online Course -
PS800

1. All Department of State computer users are reminded that they must complete and pass the annual online Cyber Security Awareness course, PS800, before the one-year anniversary of their last cyber awareness test. Any user that fails to meet this requirement may have their OpenNet Plus access revoked pending completion of the course and exam.

2. To register and take the course and exam online, please access the following link and follow the instructions:

<http://fsi.state.gov/fsi/sait/default.asp?Cat=Awareness%20Training>

3. If you have questions about the course, please contact: awareness@state.gov. If you are having technical problems with the course, please contact: fsicshelpdesk@state.gov. Also, please visit the Office of Computer Security's website for updated information on computer security policies, procedures, and news at <http://cs.ds.state.gov/>.

4. Minimize considered.

RICE

BT

#7187

NNNN

UNCLASSIFIED

Telegram

Page 2 of 2

UNCLASSIFIED STATE 00087187

UNCLASSIFIED

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

Call the Office of Inspector General
HOTLINE
202-647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our Web site at:
<http://oig.state.gov>

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