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 (FISMA)

Report Number AUD/IT-08-36, October 2008

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, Section 209 of the Foreign Service Act of 1980, the Arms Control and Disarmament Amendments Act of 1987, and the Department of State and Related Agencies Appropriations Act, FY 1996. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its oversight responsibility with respect to the Department of State and the Broadcasting Board of Governors to identify and prevent fraud, waste, abuse, and mismanagement.

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 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.

Mark W. Duda
Assistant Inspector General for Audits

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In response to the annual requirements of the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG) performed an independent evaluation of the information security program at the Department of State (Department). OIG reviewed the Department's progress in addressing information management and information security program requirements per FISMA and other statutory requirements, including Office of Management and Budget (OMB) guidance. The OIG team assessed performance in various areas, including inventory, plan of action and milestones (POA&M), certification and accreditation (C&A), security planning, contingency planning, risk management, incident response, security awareness and training, configuration management, and privacy requirements.

Since last year, the Department has taken several steps to improve management controls, including conducting a comprehensive data call of all of its domestic bureaus and overseas posts in an effort to accurately identify its FISMA reportable inventory. The Department improved its POA&M process by developing databases to manage the POA&M process and posting a toolkit on its website to assist system owners with the POA&M process for those systems that require C&A. The Department's C&A process and quality also improved since OIG's review last year. The Department also has made progress in addressing its privacy responsibilities. The Department documented its agency-wide requirements for configuration management within policy established by the Bureaus of Diplomatic Security (DS) and Information Resource Management (IRM). Further, the Department implemented several new initiatives in FY 2008 to improve its incident reporting services and analyses. Finally, the Department began addressing the awareness training requirement for non-system employees—an issue previously reported by OIG.

While improvements have been made, OIG identified controls needing further enhancements. Specifically, the Chief Information Officer (CIO) should ensure that:

- annual inventory data call activities are rescheduled to allow sufficient time to complete the analysis of pending items prior to the annual FISMA review;
- system owners are provided with improved guidance for properly identifying contractor-owned or operated systems and how to report them for systems inventory purposes;
- national security systems are properly classified and accounted for by IRM and DS in their respective FISMA inventories;
- a method is developed and made available to systems owners for providing timely and complete updates to POA&M data;
- system connection agreement controls between Department system owners and external connection system owners are developed and tested to serve as a compensating control for systems security plan testing;

[1] 44 U.S.C. § 3545 et seq.

- critical controls are identified and tested annually;
- the policy on contingency planning is updated to include a requirements that test results are incorporated into an updated contingency plan;
- guidance is provided to systems owners for ensuring adequate documentation and incorporation of test results into the POA&M process;
- a process is developed and documented for identifying and describing interconnectivity between contractor systems and the Department;
- Interconnection Security Agreements and Memoranda of Agreement/Understanding are developed and maintained for contractor-owned and/or operated systems; and
- a process is established to monitor and validate security awareness training provided to those individuals without access to Department networks.

BACKGROUND

Section 3545 of FISMA directs each agency to conduct an annual independent evaluation of its information security program and practices. 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. OMB Memorandum M-08-21,[2] issued on July 14, 2008, contained guidance to assist OIGs on reporting FISMA performance metrics.

Section 3544(b) of FISMA requires that agencies develop, document, and implement an agency-wide information security program. As part of that program, section 3544(b)(6) requires that the CIO develop a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. OMB Memorandum M-04-25,[3] dated August 23, 2004, discusses the POA&M requirements for federal agencies, which include identifying tasks that need to be accomplished, resources required to accomplish the elements of the POA&M, milestones to meet the task, and scheduled milestone completion dates. The memorandum includes a spreadsheet to be used as a model to develop POA&Ms, including details such as identified weaknesses, point of contact, resources required, scheduled completion date, milestones with completion date, changes in milestones, identification of weaknesses, and status. National Institute of Standards and Technology (NIST) SP 800-53[4] lists the security controls that system owners should implement for their systems, depending on

---

[2] Office of Management and Budget Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 14, 2008.
[3] Office of Management and Budget Memorandum M-04-25, *Memorandum for Heads of Executive Department and Agencies,* August 23, 2004.
[4] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, December 2006.

applicability to the system. The annual C&A process required by NIST SP 800-37[5] identifies security control weaknesses requiring remediation.

SCOPE AND METHODOLOGY

The OIG team consisted of staff with the OIG Office of Audits and the audit services firm of Regis & Associates, PC. References to the work conducted for this evaluation by OIG refer to this team. To perform the FISMA evaluation, OIG researched federal laws, regulations, and guidance to identify relevant criteria for implementing and managing information security programs. To identify prior issues and to follow up on past recommendations, OIG also reviewed previous reports on evaluations of the Department's information security and privacy programs. OIG reviewed documents provided by Department officials regarding systems inventory, C&A, POA&Ms, standard operating procedures, process guides, and training. OIG's analysis was based on information and documentation for the period ending the third quarter of FY 2008 to allow sufficient time for analysis and verification by the team. The Department is reporting its inventory numbers based on the fourth quarter of FY 2008. OIG judgmentally selected a subset of 21 of 182 high and moderate-impact level systems. The Department's inventory comprised 357 systems. OIG selected its subset sample from the high- and moderate-impact level systems, consisting of 38 and 144 systems respectively, for a total of 182. With this subset of 21 systems, OIG performed an in-depth review of the Department's management controls over its information systems inventory, contingency plans and annual testing, C&A, POA&M, privacy, and configuration management processes.

OIG met with officials in DS, IRM, and the Bureau of Administration (A Bureau) to discuss roles and responsibilities for implementing and managing information security programs for Department networks. OIG met with DS and IRM officials regarding C&A, configuration management, the POA&M process, and security awareness training. In addition, OIG met with officials in the A Bureau regarding privacy policy and the protection of personally identifiable information (PII). The team also sent a questionnaire and contacted bureau system owners for the 21 sample systems to obtain information pertaining to their respective information systems concerning the lifecycle of systems. OIG discussed, with officials from OMB, expectations for government-wide compliance with Federal Desktop Core Configuration (FDCC) requirements.

The results of OIG's review are discussed below and in the attached reporting template. OIG's Office of Audits conducted its fieldwork for this review from June 19, 2008, to August 29, 2008. A draft of this report was provided to officials in the A, IRM, and DS bureaus for their management review and comment, and the comments were considered and incorporated into this final report as appropriate.

In its October 2, 2008, formal response, Department officials concurred with all of the recommendations made by OIG in this report (see Appendix A). Based on the

---

[5] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

corrective actions underway and planned, OIG considers all of the recommendations resolved, pending final action. Comments or questions about the report may be directed to Karen Bell, Deputy Assistant Inspector General for Audits, at bellk@state.gov or by telephone at 703-284-2604.

RESULTS

Inventory Management

The Department has put significant effort into producing a reliable and accurate inventory under the guidelines of FISMA. For FYs 2007 and 2008, the Department has conducted a comprehensive data call to all of its domestic bureaus and overseas posts in an effort to identify all information systems and related assets. The Department's methodology to determine its total number of systems reportable for FISMA includes a combination of Federal Information Processing Standards (FIPS) Publication 199 and the Department of State Guidelines on Definitions Related to Federal Information Systems.[6] The Department's system inventory reported for FISMA is based on its information as of the fourth quarter of FY 2008. OIG performed its analysis of the inventory process and reportable systems based on third quarter FY 2008 information because of report deadlines.

Improvements have been made in achieving a complete systems inventory, but more enhancements are needed to ensure that all applicable systems and assets are properly identified as or associated with reportable systems.

Improvements Made

According to Department officials, the inventory process includes an annual data call to identify, qualify, and quantify all information systems in use at each bureau and overseas post. The process is intended to identify the universe of information systems and IT assets such as networks (general support systems), applications, and websites. Using the results of the data call, IRM's Office of Information Assurance (IRM/IA) populates two primary databases: the IT Asset Baseline (ITAB) and the FISMA Inventory Database. ITAB stores the universe of the Department's IT assets inventory and is used to track and report the IT assets managed by the Department. The FISMA Inventory Database stores information on identified major information systems that are FISMA reportable. IRM/IA analyzes 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 and inputs additional information into the FISMA Inventory Database.

---

[6] FIPs Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. *The Department of State Guidelines on Definitions Related to Federal Information Systems*, May 2007. The overriding standard is Section G of OMB Circular A-130, Management of Federal Information Resources.

Per the Department's inventory policy[7] in effect at the time of OIG's review, the FISMA reportable inventory consists of major information systems in accordance with FIPS Publication 199 and includes agency systems, contractor systems, and websites. Minor applications and subsystems are aligned with related networks based on business functions. Further, the Department determines inclusion of an information system in its inventory by analyzing it in terms of its cost and security risk. In any given year, a system is considered high cost if it is a general support system (GSS);[8] a major acquisition per OMB Exhibit 300[9] submission; a subsystem within a major acquisition; or has labor costs more than $500,000;[10] or total costs of more than $2 million. Based on the Department's methodology, each major information system included in the inventory must also be categorized by its security risk of high-, moderate-, or low-impact level, and meet the cost criteria of high. Except for low impact-low cost systems, all other types are considered by the Department to be major information systems and are included in the FISMA inventory of systems. Systems not categorized by security risk are referred to as "non-categorized." There were none identified by the Department in the inventory for FY 2008.

Based on OIG's review of the Department's inventory process as of the end of the third quarter of FY 2008, the rationale and methodology for identifying the FISMA-reportable inventory appears reasonable. However, OIG noted that the Department's total number of systems may be incomplete because it had not completed its analysis of IT items identified as "pending." Because the data call captures all types of IT assets, OIG believes that it is reasonable to expect that not all pending items will be classified as systems.

Improvements Needed

IRM/IA's FISMA Inventory Database is updated from the annual data call and refreshed/updated quarterly. According to IRM/IA officials, the FY 2008 data call, initiated in April 2008, requested comprehensive IT systems and asset information. As of August 2008, IRM/IA was still analyzing the data provided by domestic and overseas information management personnel. "Pending" items represent agency-owned IT assets captured from the data call in the ITAB database that have not been analyzed sufficiently for IRM/IA to make a decision on whether these items should be included in the FISMA Inventory Database. Because the data call captures all types of IT assets, OIG believes that it is reasonable to expect that not all pending items will be classified as systems.

---

[7] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. *The Department of State Guidelines on Definitions Related to Federal Information Systems*, May 2007.

[8] A general support system is an interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, and people. Sources: NIST SP 800-53 and OMB Circular A-130, Appendix III.

[9] OMB Exhibit 300 refers to Capital Asset Plan and Business Case Summary.

[10] Subsequent to the initiation of OIG's review, the Department updated its definitions policy in July 2008 to change the $500,000 labor cost threshold to more than four full-time equivalent (FTE) IT staff for any given year.

IRM/IA is not expected to complete its analysis of the pending items until the end of FY 2008. OIG notes that as of the preparation of this report, the Department had 355 items listed as "pending." As a result, the Department's agency-owned FISMA reportable inventory for 2008 is based upon the major information systems identified in the database as of the end of the third quarter, rather than for the entire fiscal year, and the inventory may not be complete. IRM/IA has not been able to complete its analysis of the pending items list because of competing priorities for staff to address both the data call responses and the FISMA review and reporting milestones. The Chief Information Security Officer (CISO) stated that IRM/IA may adjust its data call time period so that all evaluation and verification can be completed prior to the next FISMA review.

During its evaluation, OIG submitted a questionnaire to the owners of the 21 selected systems to obtain information on their overall system inventories, which revealed that five contractor-owned and operated systems had not been included in the ITAB database and that IRM/IA had not been notified of the existence of these systems. Specifically, the Global Financial Management System interfaces with the following contractor-owned systems: Citibank, Carlson-Wagonlit ITS/GTS, American Express ITS/GTS, US Bank/PowerTrack, and Carlson-Wagonlit eTravel. These systems had not been reported as inventory by the Bureau of Resource Management (RM), the business unit for these functions. Therefore, OIG initially concluded that these five contractor systems should have been included in the Department's reportable inventory to ensure contractor oversight. When these omissions were discussed with IRM/IA officials, they responded that according to follow-up they subsequently conducted with the business unit, four of the five systems should be considered "corporate systems" and therefore are not subject to FISMA compliance or included in the inventory as contractor systems based on OMB reporting instructions. However, OIG did not separately verify with the system owner that these systems are corporate systems. The fifth system, Carlson-Wagonlit eTravel, was determined by IRM/IA to already be in the FISMA inventory under the name "E2Solutions E-Gov Travel Service."

Per OMB requirements, all National Security Systems (NSS) are to be included in the Department's reportable inventory. NSS are information systems used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency, which involves intelligence activities, cryptologic activities, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or military or intelligence missions. OIG noted that the Department had identified approximately 30 NSS major information systems in its FISMA inventory. However, by reviewing IRM's Systems Integrity Division website—which handles cryptologic services—the OIG determined that three items identified as "systems" were not listed in either the ITAB or the FISMA Inventory Database or identified by IRM/IA as an NSS. As a result, OIG initially believed that the Department was not fully evaluating or reporting a complete systems inventory, to include interfaces and components of larger systems, for FISMA compliance.

In a meeting with IRM/IA and DS officials about this NSS discrepancy, OIG was informed that these three systems are currently considered to be media devices

(hardware) used for processing manually derived information, and should not have been identified as systems on the IRM website. In addition, these three media devices are in the process of being converted to electronic devices and will be combined under one system known as "Communications Security (COMSEC)," which will be included in the FY 2009 Intelligence Community FISMA inventory that DS maintains and which is separate from the FISMA inventory that IRM/IA maintains. During this clarification discussion, OIG observed the need for enhanced coordination and communication within the Department with regard to the proper identification and classification of NSS and intelligence systems inventories.

The data call efforts are a commendable and productive initiative by the Department to reach out to all system owners to obtain comprehensive systems information. However, conducting the annual data call earlier in the fiscal year may enable the Department to complete its analysis earlier and include relevant assets in the FISMA evaluation and reporting period. This may also permit IRM/IA to use ITAB more effectively as an interim repository for data analysis prior to inclusion in the Department's FISMA Inventory Database.

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.

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.

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.

Plan of Action and Milestones Process

Improvements Made

Agencies should use the POA&M process as a management tool for identifying and tracking remedial actions. The POA&M process is designed to resolve IT security control weaknesses with prioritization to ensure vulnerabilities are addressed in a timely and cost-effective manner. An effective POA&M process ensures that security control weaknesses do not result in the unauthorized access, use, disruption, disclosure, modification, or destruction of information.

The Department exercised a focused effort and has markedly improved its POA&M process since last year's FISMA review, specifically in the areas of incorporating and prioritizing known IT security weaknesses; incorporating OIG findings; and centrally tracking, maintaining, and reviewing POA&M activities on a

regular basis. As a result, OIG has increased the status of five of six performance elements for this fiscal year based on results of information as of the end of the third quarter of FY 2008. OIG reviewed information on the bureau-level and Department-wide databases that IRM/IA had developed to centralize and track POA&M actions. As a result, based on an evaluation of the 21 selected systems, OIG concluded that that the Department's POA&M process incorporated over 95 percent of all known security control weaknesses agency-wide. OIG found only one system in its sample that did not incorporate action items resulting from the C&A testing phase into the POA&M. OIG also found that IRM/IA regularly tracked, maintained, and reviewed the POA&M action items; however, it did not always receive timely and updated POA&M information from the system owners throughout the year.

As one of the significant improvements made, IRM/IA developed bureau-level and Department POA&M databases housed on IRM/IA servers for each system owner to use to manage its POA&M progress. IRM/IA also developed a toolkit on its website to assist system owners with the POA&M process for those systems that require C&A. The toolkit contains background information, requirements, and frequently asked questions so that system owners can document and track POA&Ms in a consistent manner. The website contains presentations and information designed to educate system owners on how to use the POA&M database. IRM/IA also provides workshops for system owners to better understand how to use the POA&M database tool.

POA&M action items result from security weaknesses that are identified through tests and audits of security controls, as required by NIST SP 800-53. These tests and audits include independent reviews, such as those conducted by OIG, the Government Accountability Office, and DS; penetration testing; self-assessments; continuous monitoring; and security incidents. For systems requiring C&A, security control weaknesses arise during testing and should be remediated either through the POA&M process or as an immediate action item. A POA&M action should be created when the weakness cannot be corrected immediately.

System owners record identified weaknesses in a POA&M tester database that is submitted to IRM/IA; integrated into IRM/IA's bureau-level database; and finally, uploaded into the Department-wide POA&M database. From this database, IRM/IA tracks, maintains, and reviews the POA&M information for each bureau Department-wide and generates reports for OMB submission. Weaknesses identified from OIG reviews are also electronically transferred into the Department-wide POA&M database via a data extract of information from the OIG Compliance Analysis Tracking Database—a new effort initiated by the Department this year.

OIG reviewed POA&M information for the 21 systems identified for the FISMA evaluation of a subset of systems, including the information contained within the Department-wide POA&M database. OIG also utilized a questionnaire with system owners in nine bureaus to determine whether they used POA&M action items to prioritize and address weaknesses requiring remediation. OIG also met with and gathered supporting information from IRM/IA officials. Based on its review, OIG

observed that the Department's POA&M process is an agency-wide process and that slightly over 95 percent of the 21 systems reviewed incorporated all known IT security weaknesses. The system owners track POA&Ms to completion and use the information to plan and prioritize resources as needed to address systems security. Further, the Department CIO and CISO jointly review POA&M information on a quarterly basis. Additionally, IRM/IA personnel review the POA&M bureau-level databases and contact system owners when corrective actions for POA&M items are overdue. IRM/IA monitors the databases closely and provides assistance where needed to ensure that the POA&Ms are addressed.

During FY 2008, the Department also implemented the pilot phase of a Site Risk Scoring process to measure IT security vulnerabilities and risks at each domestic and overseas site. According to IRM/IA officials during discussions with and demonstrations for OIG, the scoring process provides Information Management Officers, Information Systems Security Officers, and system owners with details of vulnerabilities present on devices at the site and shows managers their relevant risk compared with the risk of the rest of the organization. The scoring process assigns a letter grade to responsible business units and helps identify and analyze the risks present at each site. While OIG did not evaluate this process and cannot provide an assessment of its effectiveness at this time, it received briefings and discussed the process with IRM/IA officials to obtain an understanding of its merits. The Department plans to incorporate the site-risk grading result into the current POA&M process so that it is addressed as a POA&M action item when improvements are needed to increase grading.

Improvements Needed

OIG determined that the Department included the POA&Ms in the bureau level database and in the Department POA&M database, but that the system owners did not always provide timely updates to IRM. To compare POA&M information from the testing phase to the Department-wide POA&M database, OIG obtained POA&M information via the electronic C&A packages in the OIG read-only folder created by IRM/IA for the subset of systems in its FISMA review. Although OIG reviewed the POA&M process and relevant information, it did not substantively test them to ensure that they contained all actions resulting from C&A testing of the NIST SP 800-53 controls and that the actions were consistently prioritized. However, OIG observed that for three systems, several exceptions that resulted from the C&A testing phase were not included as POA&M action items, but that the majority were excluded for valid reasons. OIG discussed the exceptions with IRM/IA officials and was told that the items should have been included in a follow-on POA&M for only one of the three systems because of NIST SP 800-53 specifications in testing discretion. The other two systems had valid exceptions that resulted from testing, and, therefore, were not required to report POA&M action items. One system was a NSS and testing of NIST SP 800-53 security controls was not required, and the other system did not require testing of all controls because of the NIST SP 800-53 discretion given to testers. For the system where POA&M action items were necessary, IRM/IA planned to enter the exceptions into the Department POA&M database and form POA&M action items during the fourth quarter of FY 2008.

Regarding the accuracy and completeness of existing information in the POA&M databases, OIG observed that the bureaus had not always provided all necessary information to IRM/IA to update the bureau-level database and consequently, the Department POA&M database. Previously, IRM/IA used SAFIRE[11] to maintain POA&M data and bureau officials updated relevant information in the application. During the past year, IRM/IA officials transferred the information from SAFIRE into the Department POA&M database. However, during the time of OIG's review, the Department database did not contain current POA&M information in all instances.

OIG observed that the Department-wide POA&M database did not always reflect current information concerning points of contact, closed action items, and milestone changes. IRM/IA officials stated that they have asked bureau officials for this missing information, but that they have not always received it. Also, IRM/IA officials stated that they did not always receive updated POA&M information from the system owners. OIG verified this matter while requesting POA&M information from system owners. For example, OIG noted occurrences of POA&M status for a particular system shown as "open" in the Department-wide POA&M database when in fact the system owner had already addressed and closed the item. OIG also observed that points of contact listed in the POA&M database were incorrect—another issue that IRM/IA officials confirmed and need to address with system owners.

Additionally, OIG determined that the POA&M database did not show an audit trail of milestone date changes. Specifically, the POA&M action items did not contain milestones, and showed only the current scheduled completion dates. Per OMB Memorandum M-04-25,[12] agencies should include milestones and date changes in the POA&M process. IRM/IA officials, however, indicated that the guidance did not require the milestone changes to be listed but only suggested that the agencies include such information. While this is a valid interpretation of the guidance, OIG believes that it would be a good business practice for the Department to consider tracking the milestones for implementing the POA&M action items and document any changes to the milestone dates to ensure an audit trail is available for the Department to identify whether POA&M actions are progressing effectively.

According to IRM/IA, the CIO is contacting system owners via letters and telephone calls to detail their respective POA&M status. The contact advises system owners that they will not be viewed favorably during the FISMA review if they do not provide current information to IRM/IA. OIG agrees with this approach and further encourages the Department to develop a mechanism for ensuring that the system owners provide updated POA&M information to IRM/IA on a regular basis. The Department has made progress with its overall POA&M process; however, these additional measures with

---

[11] The State Automated FISMA Environment Reporting tool was used by the Department to record the inventory of applications prior to using ITAB, the Information Technology Applications Baseline.

[12] Office of Management and Budget Memorandum M-04-25, *Memorandum for Heads of Executive Department and Agencies*, August 23, 2004.

system owners will further strengthen this process, including reporting current and accurate information to Department management and OMB.

Recommendation 4: The Chief Information Officer should coordinate with system owners to develop a method to ensure that each system owner provides timely and complete updates to plans of action and milestones databases and relevant officials, including the Bureau of Information Resources Management, Office of Information Assurance, on a regular basis.

Certification and Accreditation

The Department has made significant improvement this fiscal year in providing the supporting documentation that demonstrates its compliance with C&A of Federal information systems standards under guidance found in OMB Circular A-130, Appendix III, *Security of Federal Information Resources* and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. As such, OIG has increased the overall rating in this discipline from "satisfactory" to "good."

In accordance with OMB and NIST guidance, agency management officials are to provide authorization to process information as a result of the accreditation process. Management's authorization should be based on an assessment of management, operational, and technical controls evaluated during a detailed security review of an information system, referred to as security certification. The security certification and accreditation process consists of four distinct phases: initiation, security certification, security accreditation, and continuous monitoring.

As a part of OIG's review, a subset of 21 systems was judgmentally selected and reviewed from the Department's third quarter FY 2008 inventory listing to assess the Department's C&A process. OIG conducted a risk assessment of the over 500 controls established in Appendix D of NIST SP 800-53, Revision 1[13] to select a sample of 50 specific controls to use to evaluate and rate the Department's C&A process. The specific controls cover a broad breadth of information-security risk areas such as the existence of C&A documentation, quality factors of C&A documentation and related process, annual system testing, contingency plan testing, and contractor system oversight.

For each of the 21 systems evaluated, OIG reviewed the documentation that identified, certified, and accredited the security controls and found that 19 of the 21 subset sample systems had complete C&A documentation in accordance with NIST standards. Based on its review, OIG concluded that the documentation for the sampled systems demonstrated an overall good quality rating for the first three phases of the C&A process (i.e., initiation, security certification, and security accreditation). Further, OIG identified that annual system testing was conducted as part of the continuous monitoring phase for each of the sampled systems. However, OIG identified several areas where the documentation for the quality of testing was missing or not complete. The following

[13] National Institutes of Standards and Technology Special Publication 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

section discusses OIG's C&A results that correspond to OMB's FISMA template questions.

C&A Quality

OIG rated the overall quality of the Department's C&A process as "good." To evaluate the quality of the C&A process, OIG reviewed systems documentation for the 21 subset systems to determine the existence of systems controls testing. The results of the OIG review determined that of the identified key controls, the documentation for all but one control, System Connection Agreements, was adequate. Specifically, OIG identified weak documentation, and no testing for half of the 21 systems for the System Connection Agreement control when it reviewed systems security plans and certification reports.

In accordance with NIST SP 800-53, the agency should authorize all interfaces between information systems through the use of the system connection agreement control (CA-3) and monitor the system connections on an ongoing basis. Some of the systems documentation indicated that the authors of the system security plans expected interconnections for external systems to be addressed by the systems security plan for the OpenNet (the Department's unclassified network); however, OIG did not find that this occurred in documentation reviewed. Further, annual testing for the information systems connection agreement control was not conducted for 11 of the 21 sampled systems. If system connection agreements are not documented and tested, management's knowledge about data interface risks is limited, which could result in unauthorized data changes or unauthorized data use. Development and periodic testing of the CA-3 system connection agreement control between Department system owners and external connection system owners would act as a compensating control for this weakness.

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.

C&A Testing

OIG's review of the Department's documentation for C&A security controls testing demonstrates that annual testing has been completed for the 21 sampled systems. OIG selected a sample of 36 of the NIST SP 800-53 controls. Based on NIST SP 800-53 Revision 1, control CA-7 for Continuous Monitoring requires that those security controls that are volatile or critical to protecting the information system be assessed at least annually. The 36 controls tested were selected as critical controls based on OIG's professional judgment regarding the intent of the NIST criteria. OIG found satisfactory results recorded for 16 of the 36 controls. However, as shown in Table 1, OIG did not find documentation to support whether testing had been conducted for the remaining 20 sampled controls during the annual testing. The scope of OIG's assessment for the FISMA review did not include a review of system control failures or an in-depth review

of DS testing. Consequently, OIG cannot determine whether the control testing weaknesses have resulted in any incidents or failures.

Table 1: Annual C&A Security Control Testing Gaps

C&A Security Controls Without Supporting Test Results Documentation		
AC-2 Account Management	CA-3 System Connections	PS-6 Access Agreements
AC-3 Access Enforcement	IA-2 User ID	PS-7 Third Party Personnel Agreements (Contractors)
AC-5 Separation of Duties	IA-4 Identifier Information	SA-6 Software User Restrictions
AC-6 Least Privilege	IA-5 Authenticator Management	SI-2 Flaw Remediation
AC-13 Supervision	IA-7 Cryptographic Authentication	SI-10 Information Accuracy, Completeness
AU-2 Auditable Events	MA-2 Controlled Maintenance	SI-11 Error Handling
AU-6 Audit Monitoring	PS-5 Personnel Transfers	

Source: NIST Special Publication 800-53, Revision 1.

Legend:
AC – Access Controls
AU – Audit and Accountability
CA – Certification, Accreditation and Security Assessments
IA – Identification and Authentication
MA – Maintenance
PS – Personnel Security
SA – System and Services Agreement
SI – System and Information Integrity

NIST SP 800-37 allows for an annual subset of controls to be tested within the three year C&A authorization cycle. However, critical controls should be tested annually for high- and moderate-risk systems in accordance with the NIST SP 800-53 Revision 1 control standard for continuous monitoring (CA-7). The gaps in testing for the critical controls identified by the OIG appear to be the result of limited testing oversight. The team noted that gaps in testing were present in most of the sampled systems, and appeared to be for critical controls. IRM/IA officials told OIG that their determination of critical controls to be tested is a system-based approach, and that it has not developed a baseline set of critical controls to be tested for all systems. However, OIG believes that the risk for not testing critical controls is that corresponding controls may fail, which could result in unauthorized data changes or use. A centrally maintained record of the testing cycle with results for all NIST SP 800-53 controls would improve monitoring.

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.

C&A Contingency Plans

To evaluate compliance with contingency plan[14] testing for the subset of systems reviewed, OIG considered documentary evidence using NIST SP 800-53 control objective CP-4 (contingency plan testing and exercises) that included a review of management letters to confirm that an annual contingency plan test had been conducted. In addition, as a part of OIG's review, control objective CP-5 (contingency plan update) was also reviewed to determine whether the contingency plan was revised or updated to address problems encountered during plan implementation, execution, or testing. Lastly, the corresponding POA&Ms for these systems were reviewed for control objective CA-5 (Plan of Action and Milestones) to determine whether test results were incorporated and corrective actions were implemented.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* recommends that test results and lessons learned be documented and reviewed. In addition, information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan. Per NIST SP 800-53, POA&M updates should be based on findings from security control assessments, security impact analyses, and continuous monitoring activities that include contingency planning. Further, the Department's policy on contingency plans, contained in Chapter 5 of the Foreign Affairs Manual (FAM), section 1064.2,[15] requires that copies of the contingency plan and test results be retained for review.

Based on the results of its evaluation, OIG found that the documentation for 18 of the 21 subset sampled systems provided evidence that annual contingency plan testing and exercises (CP-4) were completed. However, OIG also found that only 5 of the 21 subset sampled systems had documentation to support that contingency plans had been updated and/or that test results had been incorporated into POA&Ms in accordance with control objective CP-5. IRM/IA has begun implementing a new policy to require an attachment to the management letters that details test results and plan updates. The quality of contingency plans and testing should improve overall once IRM/IA's new attachment and associated quality review are fully implemented.

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.

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.

---

[14] The contingency plan is a coordinated strategy involving plans, procedures, and technical measures to enable the recovery of information systems after a disruption.

[15] 5 FAM 1064.2, *Contingency Planning and Continuity of Operations*, August 1, 2007.

Contractor Operated or Used Systems

As a part of the testing methodology conducted by OIG, responses from system owners and two security controls identified in NIST SP 800-53, Revision 1, were used to evaluate the existence and adequacy of the Department's compliance with respect to performing contractor oversight and evaluation. OMB's instructions for FISMA compliance reporting include identifying contractor systems used or operated by a contractor on behalf of an agency or Department. To corroborate the Department's inventory of contractor systems, OIG administered a questionnaire to system owners regarding the existence of such systems not previously reported for inventory purposes. To evaluate oversight and evaluation of contractor systems, OIG reviewed the system security plans (SSP) and other relevant documentation pertaining to testing conducted during FY 2008 to determine whether the two NIST controls described below were included in testing plans and results for the 21 systems sampled. OIG considered both controls to be critical and subject to annual testing based on OIG's professional judgment regarding the intent of the NIST criteria. OIG considered both annual and C&A testing performed during FY 2008 in its evaluation. Specifically, these evaluation factors were used:

- CA-3 Information System Connections – Certification, Accreditation and Security Assessment Control: This control requires that the organization authorizes all connections from the information system to other information system outside of the accreditation boundary through the use of system connection agreements and that it monitor/control the system connections on an ongoing basis.
- AC-13 Supervision and Review - Access Control: This control requires the organization to supervise and review the activities of users with respect to the enforcement and usage of information system access controls.
- OIG Questionnaire: System owners were asked, "Did your most recent submission to the IRM ITAB include all systems owned by contractors used to support the business processes supported by your sampled system(s)?"

OIG identified four of the 21 sampled systems that did not fully comply with these controls:

- Global Financial Management System (GFMS) – The respondent to OIG's questionnaire identified five unreported contractor-owned systems that interface with the GFMS: Citibank, Carlson-Wagonlit ITS/GTS, American Express ITS/GTS, US Bank/PowerTrack, and Carlson-Wagonlit eTravel. However, in evaluating for compliance with control CA-3, OIG found that the SSP did not include an Interconnection Security Agreements (ISA) or Memoranda of Understanding/Agreement (MOU/A) for system connections for these five contractor systems and that there was no testing for CA-3 controls on GFMS performed during FY 2008. OIG reviewed documentation which supports that the AC-13 control was tested and successfully passed.

- Passport Information Electronic Records System (PIERS) – The OIG's review found that the SSP did not include Memoranda of Understanding (MOU) for system connections with contract users, and that there was no testing of system connection agreements pursuant to control CA-3; although the PIERS system owner indicated that system controls were in place in response to OIG's questionnaire. In a separate review of PIERS[16], OIG found weaknesses in contractor access oversight controls as a result of a security incident involving a privacy breach caused by unauthorized access to data by a contractor with access to PIERS. OIG reviewed documentation which supports that the AC-13 control was tested and successfully passed.
- Student Training Management System (STMS) – OIG found that the AC-13 control was not tested during FY 2008, although the system owner's response to the OIG's questionnaire indicated that contractor access control violations were supervised. STMS is operated largely by contractors with access to PII through an interface with the Department's Global Employee Management System (GEMS). Because AC-13 has not been tested, there is no corroborating evidence that access control violations by contractors are supervised. Regarding control CA-3, OIG found that although the SSP did not include an ISA or MOU for system connections with GEMS, the control was successfully tested.
- Bureau of International Narcotics and Law Enforcement Affairs enterprise network (GINL) – OIG did not receive a response to its management questionnaire for the GINL, despite repeated attempts to obtain it. Based on documentation in the SSP, OIG found that a major contractor for the Department, shares information with GINL. However, no ISA or MOU for this interconnection was referenced in the SSP and there was no test conducted for control CA-3. Consequently, contractor oversight may not be in effect for this critical information-sharing process. OIG reviewed documentation which supports that the AC-13 control was successfully tested.

As detailed above, OIG identified deficiencies for critical contractor oversight controls in these four systems. Federal policy requires federal agencies to establish interconnection agreements. Specifically, OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on an acceptable level of risk. Further, NIST SP 800-47,[17] provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems.

The Department could experience unknown exposure of unauthorized changes or use to Department data if these two critical controls are ineffective. Further, the Department may not have reasonable assurance that controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting

[16] AUD/IP-08-29, *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*, July 2008.
[17] NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

the security requirements of the Department. In addition, the Department may not be fully aware of the security control weaknesses impacting its systems, thereby leaving its information and systems vulnerable to attack or compromise. Therefore, OIG concluded that 4 of the 21 sampled systems (GFMS, PIERS, STMS, and GINL) are not fully compliant with OMB's contractor oversight requirements, resulting in a compliance rate of 81%.

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.

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

Privacy

Since last year's FISMA review, the Department has made progress in addressing its privacy responsibilities, and OIG has raised the overall ratings in this discipline from "satisfactory" to "good." The Assistant Secretary for Administration serves as the Department's Senior Agency Official for Privacy and is the delegated authority for privacy oversight Department-wide. The Assistant Secretary administers this responsibility through the Privacy Protection Governance Board (PPGB), which consists of the CIO and various bureaus, including Consular Affairs (CA) and DS. Further, additional improvements regarding privacy impact assessments (PIA) and protecting PII are underway.

Privacy guidance and provisions for all federal agencies is described in Section 208 of the E-Government Act of 2002[18] and OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. Per the E-Government Act of 2002, agencies are required to conduct PIAs for electronic information systems and collection, and make the assessments publicly available. Further, the agency must post privacy policies on agency websites and translate privacy policies into a standardized machine-readable format. OMB Memorandum M-03-22 provides additional guidance to the agencies and it directs them to conduct reviews of how information about individuals is handled within their agency when they use electronic means to collect new information, or when agencies develop or buy new systems to handle collections of PII.

The Department posted privacy policies on Bureau of Administration's Intranet privacy/PII website, which describe all necessary federal and Department privacy regulations. The website includes the Department's "Privacy Impact Assessment Guide

[18] Pub. L. No. 107-347, 44 U.S.C. §§ 3601-06.

and Template" issued in June 2008. The document contains guidance for writing PIAs and specific instructions to system owners for answering questions contained on the updated template. According to agency officials, the goal for the Department is to have all privacy systems comply with guidance as new assessments are created and existing ones are updated. In addition, the Privacy Office finalized the Department's *Personally Identifiable Information Breach Response Policy* in May 2008. An official in the Privacy Office also stated that PII training has been developed and is available.

OIG reviewed the contents of a sample of ten PIAs from a universe of 61 systems that the Department identified as requiring PIAs to assess compliance with the Department's privacy procedures and policies in effect at the time of its review. The team evaluated the PIAs or summaries for these ten systems for compliance with the E-Government Act of 2002 and OMB guidance. OIG determined that, overall, the Department had complied with the provisions of Section 208 of the E-Government Act while conducting PIAs except for three occurrences which demonstrated that the Department did not provide information on choices available to individuals regarding providing personal information. Department officials advised OIG that these PIAs were conducted prior to the implementation of the updated PIA template and that this information will be provided when the systems are recertified. Further, the Department did not include any analysis for the ten systems to show what decisions were made by the agency regarding the system or collections of information as a result of PIAs. Department officials advised OIG that the updated PIA template requires this type of analysis. Additionally, the Department's Privacy Program Office is taking a strategic three year approach to migrate all of the existing PIAs to the updated template as the systems undergo recertification.

In May 2008, the Department finalized the *Personally Identifiable Information Breach Response Policy* that addresses the provisions of OMB Memorandum M-07-16. Also, the Privacy Protection Governance Board (PPBG) met on a regular basis in FY 2007 and 2008. PPGB is responsible for addressing potential privacy issues impacting Department programs and initiatives. The PPGB is chaired by the Assistant Secretary for Administration as the designated Senior Agency Official for Privacy.

The Computer Incident Response Team (CIRT) coordinates with the Department's Privacy Office for tracking and reporting PII breaches. In March 2008, CIRT notified the U.S. Community Emergency Response Team (US-CERT) of a PII breach regarding passport information belonging to several U.S. senators. The OIG conducted two audits[19] in FY 2008 of passport operations in CA that involved breaches of PII information.

[19] OIG Report AUD/IP-08-19, *Safeguarding Domestic Passport Applications During Transit*, March 2008, and AUD/IP-08-29, *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*, July 2008.

Configuration Management

The Department has made some improvements since last year in implementing common security configurations. The Department has documented its agency-wide policy for configuration management in guidance established by DS and IRM/IA. Based on the documentation provided, the configuration management policies are found in the Computer Security Configuration Guidance standard operating procedures, configuration guidance, 5 Foreign Affairs Handbook 11, and on the IT Change Control Board website. The Department's documentation details policies and procedures that, in part, cover common security configuration management and change management controls required by NIST SP 800-53. Improvements are needed to achieve implementation of the Federal Desktop Core Configuration security settings.

Bureaus within the Department provided configuration management documentation for the systems selected by the OIG, such as SSPs, contingency plans, and certification reports. The analysis of the documentation as of the third quarter of FY 2008 revealed that controls are tested for policies and procedures, baseline configuration, configuration change control, and functionality. The documentation also indicated that controls related to change control monitoring, access restrictions, and configuration settings were tested less frequently. Additionally, control number CM-8 Information System Component Inventory, identified from NIST SP 800-53, Revision 1—details how to determine whether the system owners maintain a component inventory—was tested by only 3 of the 21 subset systems included in the OIG subset sample. IRM/IA responded to OIG by stating that the control template distributed to system owners for configuration management testing was based on NIST SP 800-53A, which did not include the Information System Component Inventory control. However, the configuration management testing conducted should have been based on guidance found in NIST SP 800-53 Revision 1, dated December 2006 and effective December 2007, which includes control CM-8.

OIG also attempted to assess the extent to which the Department has implemented the configuration management policies. The Department utilizes iPost[20] to consolidate vulnerability scanning data to determine security configuration compliance related to security compliance, patch management, and the standard operating environment. However, the reporting information provided from iPost is for network activity by site location, not by application, as required by NIST SP 800-53, Revision 1. As a result, the OIG was unable to determine the extent to which the Department had implemented its configuration management controls.

[20] iPost is a one-stop-shop for support personnel responsible for monitoring the Information Technology infrastructure.

Federal Desktop Core Configuration (FDCC)

OMB Memorandum M-07-11[21] requires agencies to adopt FDCC standards. The policy requires agencies to adopt standard security configurations for desktops when using Microsoft Windows XP and Vista operating systems. DS has developed a configuration guide that documents the compliance requirements for FDCC configuration standards for Windows XP operating systems. Although the Department established an FDCC implementation plan and began its rollout, not all workstations have been successfully implemented with FDCC standards.

According to IRM/IA and DS officials, a FDCC review was performed on the more than 70,000 Windows XP and Vista desktops. IRM/IA and DS assessed 7,500 desktops (10 percent sample of the total universe) to evaluate compliance for FDCC implementation. Based on a presentation provided by IRM/IA, approximately 80 percent of the controls had been successfully implemented for the 7,500 desktops, and another 8 percent were approved for deviations from compliance, for an overall compliance rate of 88 percent. According to IRM/IA, the compliance test for this sample of desktops was performed one week after implementation was conducted. IRM/IA provided examples to OIG of why the reported success implementation percentage was not higher. This included machines not being rebooted, conflicting group policies at the operational level, scan software not scanning accurately through the network, among others.

OIG acknowledges that the Department has made significant progress in complying with FDCC requirements. However, the requirement for FDCC compliance is that implementation is made on *all* Windows XP and Vista desktops, and this has not yet been completed as evidenced from IRM/IA's testing results. IRM/IA and DS officials stated that implementation of FDCC standards on all desktops will be completed by July 2009.

E-Authentication

The Department performed and completed an e-Authentication Risk Assessment Review (e-RAR) for 1,400 systems identified from the data call and the FISMA reportable inventory. System owners completed the E-Authentication Risk Assessment (e-RA) spreadsheets, which IRM/IA officials reviewed for accuracy. Based on the responses provided to OIG, configuration for E-Authentication requirements were performed adequately and in compliance with NIST SP 800-63 requirements.

Incident Reporting

The Department's incident response program continues to operate effectively and is well coordinated. FISMA requires agencies to establish procedures for detecting, reporting, and responding to security incidents. NIST SP 800-61 provides guidance to agencies on establishing an effective incident response program. The guidance focuses

[21] Office of Management and Budget Memorandum M-07-11, *Implementation of Commonly Accepted Security Configuration for Windows Operating Systems,* March 2007.

on four phases—preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Having an effective and well-coordinated incident response program helps the Department improve security, minimize loss and destruction, identify weaknesses, and ensure continuity of operations.

The computer incident response team (CIRT) within DS is the center of the Department's incident response program. CIRT's efforts to safeguard the Department's networks involve collaboration and sharing information with other programs officials within DS, including Cyber Threat Analysis Division (CTAD) and Virus Incident Response Team (VIRT). In addition, CIRT officials coordinate with IRM's Firewall Team and Enterprise Network Management Operations Center, systems managers, information system security officers, regional computer security officers, and the privacy team. CIRT works 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.

Key components of risk management are identifying trends for security incidents and determining effective ways to deal with them. The CIRT team generates several reports to keep Department officials aware of continuing activity and the status of its operations. These reports include daily cyber security briefs and non-malicious events, CIRT monthly report, and adhoc reports as requested. Department officials advised OIG that CIRT reports are used to assess and improve the security of the Department's systems. For example, CIRT's daily reports of non-malicious events are being used by one official to identify trends that may require reminders to information technology staff. Another official advised that intrusion detection measures have been added to the organization's network as a result of CIRT reports. A third official reviews CIRT reports for announcements that may help improve the security of the system. Lastly, privacy officials stated that a breach incident log has been created to generate reports and incorporate lessons learned.

As of August 22, 2008, CIRT opened 2,672 event tickets and closed 2,675 incidents and referred 294 incidents to US-CERT. The types of incidents reported included improper usage, malicious codes, unauthorized access, and privacy breaches, among others. CIRT implemented several new initiatives in FY 2008 to improve it services and provide more effective analyses and reports, including the following:

- paying more attention to cyber events that are potentially malicious rather then non-malicious;
- sensoring coverage on networks to capture more anomalies and viruses;
- aggregating events identified from reports and logs from CIRT, CTAD and VIRT to identify commonalities;
- assessing world events to increase network monitoring activity in affected regions;
- providing mandatory training for CIRT analysts; and

- reporting PII breaches reported to the privacy team and to US-CERT.

CIRT assumed responsibility for tracking and reporting PII breaches in January 2008. In March of 2008, CIRT notified US-CERT of a PII breach regarding passport information pertaining to several U.S. senators. The OIG conducted two audits[22] in FY 2008 (March and July, respectively) of passport operations in CA. The March 2008 report involved the safeguarding of PII in passports during transit, and the July 2008 report involved PII breaches of passport information stored in the Passport Information Electronic Records System (PIERS). As result of the OIG audits, CA has implemented several measures to improve its operations, including the following: 1) developing guidance for incident detection and reporting for PIERS; 2) developing guidelines for reporting missing or loss passport applications; and 3) assembling a security working group that consists of staff from CA and other Department bureaus that provides oversight for PII through enhanced monitoring of systems and databases, reporting and auditing activity, training, and disciplinary actions in the event of a breach in order to minimize PII breaches.

In addition, the Privacy Office issued the Department's Personally Identifiable Information Breach Response Policy in May 2008. Further, officials continue to participate in CA working groups on mitigation strategies. An official in the Privacy Office also stated that PII training has also been developed and is provided to new civil service employees who are enrolled in FSI's *New Civil Service Orientation* and Orientation *for Civil Service Employees with Department of State Experience* courses. In addition, PII training is provided during weekly briefings to information management officers and student employees participating in the Student Cooperative Employment Program. Further, training on how to conduct privacy impact assessments is made available specifically to bureaus and offices.

Having an effective and well coordinated incident response program helps the Department improve security, minimize loss and destruction, identify weaknesses, and ensure continuity of operations.

Security Awareness Training, Peer-to-Peer File Sharing

The Department has made positive progress in its security awareness efforts and has "mostly" ensured that security awareness training is accomplished. Currently, the Department provides two types of awareness training to its system users. This includes security awareness training and role-based training. Security awareness training is offered through an online course developed and coordinated with DS, IA, and Foreign Service Institute (FSI) representatives. Based on documentation OIG received from FSI, the online training material (course number PS800) includes information on user responsibilities, computer risks, threats and vulnerabilities, and privacy issues. The

[22] OIG Report AUD/IP-08-19, *Safeguarding Domestic Passport Applications During Transit*, March 2008, and AUD/IP-08-29, *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*, July 2008.

training content also includes policies on the use of collaborative web technologies and peer-to-peer file sharing. Per 12 FAM 622.2, the responsibility of staff completing security awareness training is placed on the Information Systems Security Officer, Information Management Officer, or system administrator. Notices for annual training requirement are sent via email notifications and Department-wide announcements to system users. As of August 1, 2008, more than 55,000 employees had completed PS800 course for the fiscal year. Role-based training is another awareness training provided to selected individuals, including executives, managers, system administrators, Information Systems Security Officers, and law enforcement employees within the Department. The role-based training is an instructor-led course that can also be taken via distance learning. The training includes supplemental modules focusing on the latest security issues. Documentation received from the Diplomatic Security Training Center showed that more than 900 individuals had enrolled in the role-based training courses as of August 12, 2008.

The universe for those required to take security awareness training is determined by system accounts. The issue of multiple accounts for the same individual is still a matter that needs to be addressed by the Department. By having multiple accounts for the same employee, duplication of training entries can occur, resulting in the Department not having complete assurance of the total number of employees required to take training on an annual basis. OIG has an open recommendation from its FY 2006 FISMA report addressing this matter. Per IRM/IA officials, the Department is planning to include training statistics on iPost for each bureau and overseas post. This will place the burden on the respective bureau or post Information Systems Security Officers to review and eliminate duplicate entries to receive a better FISMA evaluation result on training.

The Department began addressing the awareness training requirement for non-system employees (i.e. drivers, janitors, and gardeners) this fiscal year. In a July 31, 2008, memorandum from the CISO to OIG, the Department states it will provide awareness training to non-system employees by requesting Regional Security Officers to give awareness training to new employees at posts, as well as place posters around the embassy or consulate for display. The Department has taken positive steps in this respect. However, performance metrics would help determine whether the process performed by the Regional Security Officers is working effectively.

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.

RECOMMENDATIONS

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.

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.

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.

Recommendation 4: The Chief Information Officer should coordinate with system owners to develop a method to ensure that each system owner provides timely and complete updates to plans of action and milestones databases and relevant officials, including the Bureau of Information Resources Management, Office of Information Assurance, on a regular basis.

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.

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.

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.

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.

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.

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

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.

APPENDIX A – DEPARTMENT RESPONSE

United States Department of State

Chief Information Officer
Information Resource Management

Washington, D.C. 20520-6311

OCT - 2 2008

UNCLASSIFIED

MEMORANDUM

TO: OIG – Mark W. Duda

FROM: IRM – Susan H. Swart

SUBJECT: Review of the Information Security Program at the Department of State (AUD/IT-08-36)

In accordance with the Federal Information Security Management Act (FISMA), as the Chief Information Officer of The Department of State, I am providing formal comments to the OIG's official recommendations. My comments are attached for inclusion as an appendix to the OIG's Annual Review of the Information Security Program at the Department of State (AUD/IT-08-36, September 2008).

Attached as stated.

UNCLASSIFIED

Management Comments:

The Department appreciates both the opportunity to comment on this report, and also appreciates the effort that the OIG has expended in this year's FISMA review. Under the leadership of Karen Bell, the team of OIG direct hires and contractors has conducted a substantive review which has identified significant opportunities to improve the security of the Department's information.

Notwithstanding these positive results, the Department proposes that there is a collective need to address two outstanding issues to improve the overall FISMA process (including the annual review).

Issue 1: Over the last several years, a different FISMA OIG team has typically conducted the review each year. In each of those years, there have been divergent ideas about the criteria that the Department must meet to satisfy the FISMA grading criteria embodied in the Reporting Template for IGs, and related reporting guidance. Inadvertently, this creates a level of ambiguity that makes it hard (or impossible) for the Department to know what to do to succeed.

OIG Action Requested for Issue 1: As a result, the Department respectfully requests OIG officials and Department security managers meet during the first quarter of FY09 to establish clear criteria for areas that have caused issues in the past because of their ambiguity. These criteria would be documented in a MOA between the OIG and the Department to guide subsequent FISMA reviews. The overall goal of the MOA would be to: a) maintain the independence of the OIG and its staff, and b) provide the Department with a better understanding of how it can best improve security while complying with the FISMA reporting criteria.

Issue 2: Although the OIG recognized significant improvements in all other areas of FISMA oversight for the past two years, the OIG has found issues related to annual testing (specifically, Reporting Template for IGs, Question 3a) which was used to justify reducing the Department's FISMA grade by one full letter grade in each year. While the Department sincerely appreciates the efforts undertaken by the OIG's review of the agency-wide information security program,

the OIG's report notes that it did not have the resources to take a comprehensive look all programs areas related to Question 3a. As a result, the Department is concerned that other weaknesses related to Question 3a may exist that have not been identified.

OIG Action Requested for Issue 2: As a result of Issue 2, the Department requests that the OIG conduct an independent and comprehensive review of the Department's efforts to fulfill the requirements related to Question 3a, and to make such recommendations as necessary to allow the Department to make changes to the program, as needed, to make the program fully compliant. Moreover, the Department urgently requests that this be done early enough in fiscal year 2009 so that implementation of the recommendation(s) could begin in Q2. If the OIG cannot, for some reason, meet the scope or time frame for this review, the Department proposes that the OIG hire an independent reviewer to conduct this study under OIG supervision, consistent with the authorities provided by FISMA.

In its original draft report, the OIG made several suggestions for the Department to consider for improving its current activities in the areas of inventory management, contingency plans, and security awareness training that would be necessary to address the OIG findings. The Department asked that these be expressed as formal recommendations (and they were) to allow the Department to provide a clear management response so that we would know how to properly respond to these items, and so others in the Department would not miss these significant "suggestions".

Notwithstanding these concerns, the Department is pleased to note that the OIG recognized the Department for:

- "Significant effort" in "producing a reliable and accurate inventory under the guidelines of FISMA."
- A "focused effort" that has "markedly improved its POA&M process since last year's FISMA review."
- "Significant improvement this fiscal year in providing the supporting documentation that demonstrates its compliance" with C&A Standard, justifying a "good" rating of the C&A program.
- Raising the overall rating of the Privacy program from "satisfactory" to "good."

- Improvements in implementing common security configurations, including: a) adopting the FDCC standard configurations, b) incorporating required FDCC acquisition language in new contracts, and c) achieving 88% compliance with FDCC requirements by early September 2008.
- Compliance with requirements for e-Authentication Risk Assessments.
- Continuing an incident response program which is operated "effectively and is well coordinated."

Having made "positive progress in its security awareness efforts," we now turn to the significant findings of this review and what steps will be taken to address the specific opportunities for improvement identified by the OIG.

> ***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.*

The Department notes that while implementing this recommendation will not improve the overall high quality of the Department's inventory process, it will reduce ambiguity at the time of the FISMA review. This is a valid and valuable outcome. Thus, the Department concurs with this recommendation.

The Department also notes: a) the need to focus on identifying any missing "contractor systems" and interconnections (see recommendations 2, 5, and 9), and b) conducting more than one full data call in any 12-month period would significantly erode field willingness to participate.

In the light of these considerations, the Department will address this recommendation by taking the following actions:

- The FY2009 inventory data call will provide increased focus on defining and identifying "contractor systems" and "system connections" that may be missing.
- The FY2009 data call will be initiated in early FY2009.
- Routine quarterly inventory data calls will remind bureau and post system owners to report new systems, significant changes, etc.

For comprehensive reporting purposes, the Department's inventory process is described below:

- The inventory data call process is designed as a screening process to identify assets which ***may*** need to be in inventory. It is explicitly designed to prevent those responding not to be able to exclude systems that need to be reported. The result of this focus on avoiding missing systems is a higher rate of false positives. But, importantly, this first step helps significantly to ensure that all Department systems that might need to be added to inventory are considered.
- The second test is the analysis of pending items conducted by system owners after the data call, carefully guided by IRM/IA FISMA inventory experts. This is a rigorous documented process, implemented through careful application of FISMA, OMB, and NIST guidance. Conducting this level of analysis before the data call on all "assets" that might be systems would be prohibitively expensive. Conducting it on the pending items after the data call ensures that false positives are eliminated and that just the right set of missing systems are added to inventory.

In summary, the Department is proud of its overall inventory process, and views the step of identifying a large number of candidate systems for expert screening to be one of the main strengths of the process, not a weakness. If the Department changed the data call to identify fewer pending (candidate) systems for the more rigorous second test stage, the overall confidence in the inventory completeness would likely be significantly compromised.

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.*

The Department concurs with this recommendation. The CIO will direct IRM/IA to review existing laws and regulations regarding criteria to identify which systems are to be included in the Department's inventory. Based on this review, IRM/IA will add appropriate guidance to the Department's "Inventory Toolkit"[1] to ensure accurate and consistent guidance is provided to system owners in this

[1] This toolkit, and others referred to in his document, are designated in Department Notice 2008_02_121 as required procedures to be implemented to conduct the Department's Certification and Accreditation program according to Department policy.

regard. This improvement will provide significantly increased assurance that all Department systems[2] (and only the Department's systems) are included in the Department inventory.

> ***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.*

The Department concurs with this recommendation. The CIO directs IRM/IA to modify the Department's "Inventory Toolkit" to clarify which systems are inventoried by IRM/IA and which are inventoried by DS/SI/IS in support of the Intelligence Community Chief Information Officer's FISMA reporting. This improvement will ensure that system owners will be able to easily verify the correct venue in which to report each system.

> ***Recommendation 4:*** *The Chief Information Officer should coordinate with system owners to develop a method to ensure that each system owner provides timely and complete updates to plans of action and milestones databases and relevant officials, including the Bureau of Information Resources Management/Office of Information Assurance, on a regular basis.*

The Department concurs with this recommendation. The CIO will send formal quarterly grade letters from the CIO to bureau executives on the quality of bureau plan of action and milestones (POA&M) process implementation. This will cover: a) timely and complete identification of weaknesses, b) development of remediation plans, c) implementation of remediation, and d) management of weaknesses (including timely and complete quarterly updates of status). These improvements will help ensure that system owners: a) define actionable tasks to address weaknesses, b) define appropriate priority to each action, and c) allocate appropriate resources to complete those tasks and document them in the POA&M system.

---

[2] Consistent with FISMA and OMB authorities, the term Department systems is used here to refer not just to systems owned and operated by the Department (aka "agency systems"), but also those operated on behalf of the Department by others (whoever they may be, aka "contractor systems"). This term, as used here, does not include systems which are not under the ultimate control and responsibility of the Department, per OMB FISMA guidance.

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.*

The Department concurs with this recommendation. The CIO will also add information to the C&A Toolkit clearly articulating FISMA-compliant policy on: a) identifying, b) assessing the risk of, and c) obtaining connection agreements for such connections. Next, the CIO will modify the FY2009 inventory data call (see recommendation 8) to include a focus on system connections. With respect to the interconnections, this will include: a) reviewing the completeness and content of system connections identified in each existing System Security Plan (SSP), b) accurately assessing the risk those connections pose to other Department systems, and c) verifying (at least annually) that all active connections to/from existing major information systems are completely listed in the systems' SSPs. With regard to the external systems on the other end of each connection, this data call will include: a) verifying whether the connected systems are Department systems (see recommendation 2), and b) adding any interconnected Department systems to inventory, as needed. These improvements will help ensure that the Department fully complies with both NIST SP 800-53 controls, CA-3 and NIST SP 800-47.

The Department notes that the definition of what constitutes a system connection/interconnection is unclear in existing Federal guidance. To address this, IRM/IA will develop guidance in its Inventory and C&A Toolkits to clarify what constitutes an interconnection. This improvement will both help ensure not only that system owners actively address all actual connections, but also that systems owners do not waste time being confused about what constitutes such a connection.

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.*

The Department concurs with this recommendation, and notes that the OIG's finding that all critical controls are to be tested at least annually for high and

moderate risk systems is one of the most significant results from this year's report, and will have positive impact on security when implemented.

The Department notes that in spite of the identified weakness in the policy program related to annual testing, several systems owners (notably the Bureau of Consular Affairs) were conducting annual testing of controls the OIG determined to be critical. This demonstrates the thoughtfulness and good faith of Department system owners.

The Department also notes that its Site Risk Scoring program provides continuous monitoring, more frequently than annually, of a wide range of controls critical to its networks and the applications that operate thereon. This helps demonstrate the good faith of the CIO, CISO, DS and other program officials responsible for information assurance at the Department.

The Department notes that during the FY08 FISMA review the OIG team used their professional judgment to identify a particular set of "critical controls" (as specified by NIST SP 800-53, control CA-3) ***only*** for the purpose of their review this year (since the Department had not done this). However, it is the Department who has the authority and responsibility to determine which controls it will consider to be critical and volatile using a risk-based analysis, ***as long as*** it implements a reasonable process to define such controls in compliance with the guidance from NIST. The controls identified by the Department need not necessarily match those that the OIG identified this year, and may vary among major information systems based on the risks identified.

To address this recommendation, the Department will develop its Annual Control Assessment Toolkit to provide clear criteria and a process for system owners to identify which controls are critical and/or volatile for each particular system. Next, the toolkit will be modified to provide explicit policy that critical and volatile controls are to be tested annually. Finally, the Department will organize workshops to introduce this change to system owners. These improvements will ensure that system owners use a valid and reliable process to identify critical and volatile controls, and that these are tested at least annually.

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.*

The Department concurs with this recommendation. To help ensure implementation of this process, the CIO will issue clear directions to system owners requiring this action, by adding this guidance to its Contingency Plan Test Toolkit. IRM/IA will also add this requirement to its contingency plan test completion checklist process to provide oversight.

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.*

The Department concurs with this recommendation, and agrees with the OIG's finding that implementation of an improved process to document contingency plan test results will largely resolve this recommendation. To help ensure implementation of this process, the CIO will issue guidance to system owners stressing the importance of this improvement and requiring implementation of this process. The Department will also develop its Contingency Plan Test Toolkit to provide clear directions to system owners on this process.

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.*

The Department concurs with this recommendation. The Department believes that the actions proposed to address recommendations 1, 2, and 5 will also adequately address this recommendation. These improvements will help ensure: a) that a reliable and valid process is used to determine which contractor owned and/or operated systems are Department systems (see recommendations 1 and 2), b) that all interconnections are documented and tested before being placed in operation (see recommendation 2), and c) that such interconnections are tested at the required frequency thereafter (see recommendation 5).

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

The Department concurs with this recommendation. The CIO directs IRM/IA to: a) modify the Department's C&A Toolkit to ensure that the system owners understand the need to document interconnections, and b) validate the IRM/IA C&A completion checklists verify that all such agreements that may be required are on file in IRM/IA.

Recommendation 11: *The Chief Information Officer should establish a process to monitor the extent to which security awareness training has been provided to those individuals without access to Department networks.*

The Department concurs with this recommendation. The CISO will select a simple random sample of facilities where such employees are employed. Bureau EX/DIRs and/or post DCMs for these facilities shall be asked to assign staff to review and objectively report whether the designed materials were provided to staff members at each site.

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 website at oig.state.gov

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