

UNCLASSIFIED

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

Office of Audits

**Review of Department of State
Information Security Program**

AUD/IT-11-07

November 2010

UNCLASSIFIED



United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

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

In accordance with the Federal Information Security Management Act of 2002 (FISMA), OIG performed a review of the Department of State Information Security Program for FY 2010. To perform this review, OIG contracted with the independent public accountant Williams, Adley & Company, LLP. The report is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The independent public accountant identified areas in which improvements could be made, including system inventory, risk management framework, plans of actions and milestones, security awareness training, security configuration management, remote access, identity and account management, incident response handling, continuous monitoring, contingency plans, and oversight of contractor systems.

OIG evaluated the nature, extent, and timing of the independent public accountant's work; monitored progress throughout the audit; reviewed supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with the findings, and the recommendations contained in the report were developed on the basis of the best knowledge available and were discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

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

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

Harold W. Geisel
Deputy Inspector General



November 12, 2010

Review of Department of State Information Security Program

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

Williams, Adley & Company, LLP (referred to as “we” in this letter), is pleased to provide the Office of Inspector General (OIG) the results of the review of the Department of State (Department) Information Security Program for FY 2010. We reviewed the Department’s Information Security Program performance in compliance with the Federal Information Security Management Act and Office of Management and Budget (OMB) and National Institute of Standards and Technology regulations, standards, and requirements. Additionally, the review was performed to provide sufficient support for OIG in providing a response to OMB in accordance with OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010.

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

We appreciate the cooperation provided by Department personnel during the review.

Williams, Adley & Company, LLP

Table of Contents

Executive Summary 1

Background 4

Results of Review 5

A. FISMA System Inventory List Contained Retired Systems 5

B. Risk Management Framework Needs To Be Improved 5

C. Plans of Actions and Milestones Were Not Adequately Managed 6

D. Security Awareness Training Requirements Were Not Enforced 8

E. Security Configuration Management Needs Improvement 10

F. Opennet Everywhere Software Package Had Significant Security Weaknesses 11

G. Account Management in Active Directory Needs Improvement 12

H. Personally Identifiable Information Incidents Were Not Reported Timely 14

I. Continuous Monitoring Program Needs Improvement 14

J. Contingency Plans Need To Be Updated 15

K. Oversight of Contractor Systems Requires Improvement 15

List of Recommendations 18

Acronyms 20

Appendix A. Objectives, Scope, and Methodology 21

Appendix B. Follow-up of Recommendations From the FY 2009 FISMA Report 23

Appendix C. Department of State Response 26

Executive Summary

In accordance with the Federal Information Security Management Act of 2002 (FISMA),¹ the Office of Inspector General (OIG) contracted with Williams, Adley & Company, LLP (referred to as “we” in this report), to perform an independent review of the Department of State (Department) Information Security Program’s compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). Additionally, the results are designed to assist OIG in providing a response to OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010.

We reviewed the Department’s remedial actions taken to address the FY 2009 reported Information Security Program control weaknesses identified in OIG’s FY 2009 report *Review of the Information Security Program at the Department of State*. The statuses of the FY 2009 review recommendations are in Appendix B. Since FY 2009, the Department has taken steps to improve management controls to include the following:

- Updated the Contingency Planning, Certification and Accreditation, and Annual Control Assessment Toolkits to provide guidance to system owners.
- Initiated a pilot program for the Plan of Action and Milestones (POA&M) Grading Memorandum.

Overall, we found that the Department has established and is maintaining an information security program. However, to improve the program and to bring the program into compliance with FISMA, OMB, and NIST requirements, the Department needs to make significant improvements to address the following control weaknesses:

- System Inventory List

The Department’s inventory management processes and procedures do not ensure that retired systems are immediately removed from the inventory of FISMA reportable systems. Without an accurate FISMA system inventory list, the Department’s process to support information resources management for technology planning, budgeting, and acquisition may be hampered.

- Risk Management Framework

The security authorization process was not performed on all contractor systems, and the security authorization packages had expired for four systems. These conditions weaken the Department’s risk management framework because changes within the systems and the systems’ control environment may introduce new risks and vulnerabilities into the Department’s environment.

¹ Pub. L. No. 107-347, title III.

UNCLASSIFIED

- Plans of Action and Milestones (POA&M)

The Department did not consistently record required resources for remediation of security weaknesses and update remediation schedules to reflect actual performance, all of which impeded the Department's ability to assess and monitor the progress of corrective actions.

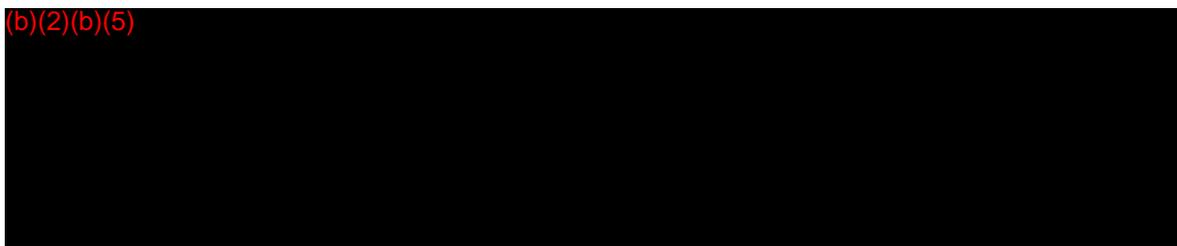
- Security Awareness Training and Personnel Security

The Department did not identify all employees who had significant security responsibilities and provide specialized training, as required by NIST.²

- Security Configuration Management

Twenty-four of 25 Windows systems tested were not compliant with the security configuration guidance provided by the Bureau of Diplomatic Security (DS), and seven of 25 systems did not have the vendor-required critical or high priority software patches to be installed. Without sufficient configuration management, the Department's data may be exposed to loss of integrity and confidentiality because configuration standards may not be implemented.

(b)(2)(b)(5)



- Account and Identity Management Program

From a population of approximately 83,000 Active Directory⁴ accounts, we found approximately 1,000 guest, test, and temporary accounts; 8,000 accounts that had not been used (never logged on); and 600 accounts that had passwords that were set so that they would not expire. Therefore, these accounts are susceptible to being compromised by unauthorized users for unauthorized purposes.

- Personally Identifiable Information Incidents

We found six instances in which the Department did not report personally identifiable information (PII) data incidents to the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour of suspecting or confirming a security breach, as required by OMB. Failure to notify US-CERT within the required timeframe increases the risk to individuals that their PII data may be misused. Also, the Department may be in violation of Federal law.

² NIST SP 800-16, "Information Technology Training Requirements: Role- and Performance-Based Model."

³ NIST SP 800-67, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher."

⁴ Active Directory is a technology created by Microsoft that provides a variety of network services such as identification and authentication, directory access, and other network services.

UNCLASSIFIED

- Continuous Monitoring

The scanning tools do not assess the Oracle configuration, the Department's most common database system, for configuration control weaknesses, which could adversely impact application access controls.

Scanning results for routers, firewalls, and Demilitarized Zone servers were not available in iPost;⁵ therefore, the results were not used in risk scoring.

- Contingency Planning

A contingency plan did not exist for one system, and the Department had not performed a continuity of operations test of that system. Without testing the contingency plan at the system level, the Department cannot evaluate the plan's overall effectiveness, identify significant weaknesses, and ensure that corrective actions are taken.

- Oversight of Contractors

A contract for one contractor system did not contain the required information security clauses from Department of State Acquisition Regulations (DOSAR). The lack of information security requirements increases the risk that contractor systems possess inadequate security controls and make other Department software and hardware vulnerable to unauthorized access, use, disclosure, disruption, modification, or destruction.

The Department did not have an effective mechanism in place to identify the total number of contractors who had access to and privileges within the Department's network, applications, databases, and data. As a result, the Department could not accurately determine whether contractor personnel had received the required information security awareness training and had gone through the proper security clearance process.

Although this report contains 15 recommendations to the Department, the most significant recommendations are highlighted as follows:

- Ensure that contractor systems go through the security authorization process, including completion of a risk assessment and implementation of necessary security controls.
- Develop a process to periodically review the POA&Ms to ensure that the needed resources, including the costs of goods and personnel, required to remediate security weaknesses are accurately recorded and accurate milestones and planned actions are documented.
- Define and identify personnel who have significant security responsibilities and ensure that they receive appropriate training.

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

UNCLASSIFIED

- Ensure that the Department completes the end-to-end configuration management initiative, including implementation of the standard operating environment.
- Install an NIST-approved encryption algorithm that controls access to OpenNet Everywhere (ONE).⁶ Also, procedures should be established to efficiently and effectively identify the total number of contractor personnel who have access to the Department's systems.

We provided copies of the draft report to Department officials on October 29, 2010, and a revised draft on November 5, 2010. In its November 8, 2010, response (see Appendix C) to the draft report, the Department generally concurred with nine recommendations but did not indicate concurrence or nonconcurrence with six recommendations. Based on the response, OIG modified two recommendations (Nos. 3 and 12), both of which are considered resolved, pending further action. Also based on the response, OIG considers 10 additional recommendations resolved, pending further action; two recommendations closed; and one recommendation unresolved.

The Department's responses to the recommendations and OIG's replies to the responses are presented after each recommendation.

Background

FISMA recognized the importance of information security to the economic and national security interests of the United States. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

FISMA assigns specific responsibilities to Federal agencies, NIST, and OMB in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to OMB.

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

⁶ OpenNet Everywhere (ONE) is a program that allows users to access OpenNet from any computer with an Internet connection, allowing access to email and Intranet resources.

Results of Review

Overall, based on our review, we concluded that the Department had established and is maintaining an Information Security Program. However, the Department needs to make significant improvements to address the control weaknesses noted to improve the program and to bring the program into compliance with FISMA, OMB, and NIST requirements.

A. FISMA System Inventory List Contained Retired Systems

We found that the Department did not maintain an accurate inventory of FISMA-reportable systems. Specifically, both the third and the fourth quarter FISMA inventory lists consisted of six systems that were designated as retired systems in the ITAB. The six systems are Case Management System, Compliance Analysis & Tracking System, Cultural Connect Envoy Workflow, Post Exchange Visitor Database, Exchanges Information System, and Gifts Tracking Database. OMB Memorandum M-10-15 states that all of the agency's information systems should be included as part of the FISMA inventory report.

The inventory was inaccurate because the ITAB team did not consult with the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), on the FISMA-reportable systems that were being retired. In addition, IRM/IA officials manually reconciled the FISMA inventory report to the ITAB reports, which resulted in errors that may not have occurred under electronic processes.

Without an accurate FISMA system inventory list, the Department's process to support information resources management for technology planning, budgeting, and acquisition may be hampered.

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

Management Comments: The Department concurred with the recommendation, stating that it "expect[s] to remove the retired systems in the FISMA inventory in the next quarter in which action such as an annual test or security authorization is required for that system."

OIG Analysis: Based on the response, OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the retired systems have been removed from the FISMA inventory.

B. Risk Management Framework Needs To Be Improved

The Department's risk management framework includes an enterprise-wide security authorization process and ongoing efforts to use automated tools for continuous monitoring.

UNCLASSIFIED

However, we found weaknesses related to the security authorization process, including the security authorization packages.

- (b)(2)(b)(5) [REDACTED]
[REDACTED]
[REDACTED] The security authorization process was not performed for contractor systems because the current Certification and Accreditation Toolkit (a procedure) does not require a separate security authorization for unclassified systems that are rated low impact and low cost. OMB Memorandum M-10-15 states that security controls “are required for all federal information systems” and that the security controls “must be assessed against the same NIST criteria and standards as if they were a Government-owned or –operated system.”
- Also, of a sample of 30 systems, we found that security authorization packages⁸ for four systems (b)(2)(b)(5) [REDACTED]
[REDACTED] had expired on May 31, 2010, which exceeded their 3-year timeframe for authorization to process in accordance with OMB Circular A-130, Appendix III.⁹ Officials from IRM/IA stated that the four security packages had expired because of contractual issues with the vendor, which delayed the security testing and impacted the timelines of the security authorization process.

The lack of current security authorization packages weakens the Department’s risk management framework because changes within the systems and the systems’ control environment may introduce new risks and vulnerabilities into the Department’s environment.

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

Management Comments: In its response, the Department requested that references to low-cost and/or low-impact systems be removed because NIST SP 800-37 “gives federal agencies considerable discretion in the selection of system accreditation boundaries” and OMB A-130, Appendix III, “only requires certification and accreditation . . . for major

⁷ A system is considered high cost if any one of the following conditions is true: (a) The system is a general support system, (b) the system is an OMB A-11 Exhibit 300 submission or its components, (c) the system requires more than four full-time-equivalent staff in a single year, or (d) the total costs are more than \$2 million in a fiscal year. If a system’s cost does not meet any of these criteria, it is considered low cost.

⁸ The security authorization package contains key documents such as the security plan, security assessment report, and POA&Ms (if applicable). The senior organization official uses content from the security authorization package and input from key officials to make a security authorization decision.

⁹ OMB Circular A-130, *Management of Federal Information Resources*, app. 3, *Security of Federal Automated Information Resources*.

UNCLASSIFIED

information systems.” The Department further stated that it had included low impact and low cost systems within the accreditation boundary of the systems on which they run.

OIG Analysis: OMB Memorandum M-10-15 states, “Smaller ‘systems’ and ‘applications’ [which are not major applications or general support systems] may be included as part of the assessment of a larger system-as allowable in NIST guidance and provided [that] an appropriate risk assessment is completed and security controls are implemented.” Subsequent inquiries indicated that security assessments were not conducted on the three contractor systems during FY 2010. Since the Department did not address the issue of security assessments for the contractor systems, OIG considers the recommendation unresolved. This recommendation can be considered resolved when the Department shows that the contractor systems were tested as part of a major application or general support system and the security application packages have been completed for the four systems.

C. Plans of Action and Milestones Were Not Adequately Managed

We found that the Department had not adequately developed a POA&M process. OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plan of Action and Milestones*, states that POA&Ms should include the estimated funding resources required to resolve the weakness as well as the anticipated source of funding. The original milestone completion date should not be changed, but a new completion date should be added instead. Further, this guidance requires the POA&M to also identify other non-funding obstacles and challenges to resolve the weakness, for example, the lack of personnel or expertise or development of a new system to replace insecure legacy systems.

The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems. The POA&M is used by OMB to assist in its oversight responsibilities and to inform the budget process.

As part of its efforts to improve the POA&M process, IRM/IA has a pilot program that issues POA&M report memorandums to bureaus and offices. However, we found that the Department had not taken the following actions required by OMB:

- Consistently recorded required resources for remediation of security weaknesses.
- Updated remediation schedules to reflect actual performance. Specifically, five of 13 security weaknesses tested were 120 or more days behind schedule, and the milestone changes, if applicable, were not recorded.

These conditions occurred because the Department had not consistently reviewed and maintained POA&M corrective actions for security weaknesses.

UNCLASSIFIED

OMB¹⁰ requires the cost to close actions to be tracked, including the cost of resources required, and a determination to be made as to whether the costs are already within the budget. The cost to close actions should also include all goods (things) and services (people) needed to close the action. Without the proper review and maintenance of POA&M activities, IT management may not be aware of the status of corrective actions. As a result, delays in the implementation of corrective actions may not be appropriately identified and resolved in a timely manner.

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

Management Comments: The Department stated, “Given the changes to reporting requirements under CyberScope [the CyberScope web application supports an OMB initiative to automate collection and reporting of FISMA requirements], the Department will seek [Department of Homeland Security] . . . clarification on the desired timeliness and level of aggregation of these updates.”

OIG Analysis: Based on the response, OIG modified this recommendation to delete reference to POA&M prioritization. This recommendation can be closed when OIG reviews and accepts documentation showing the process the Department has developed regarding updates in the POA&Ms.

D. Security Awareness Training Requirements Were Not Enforced

In the FY 2009 FISMA review, OIG reported that the Student Training Management System (STMS) does not track courses that employees take annually to meet continuing professional education requirements. In addition, management did not receive a report periodically showing which training courses employees who had significant security responsibilities had attended.

The Department is working to address the findings identified in the FY 2009 FISMA review. For example, IRM/IA, DS, and FSI have reestablished the Awareness, Training, Education, and Professionalism Working Group, which addresses both the awareness training and the training of staff who have significant IT security responsibilities.

However, during the 2010 FISMA review, we found that the Department did not identify all employees who had significant security responsibilities and had not provided all of those employees with specialized training, as required by NIST SP 800-16.¹¹

By not properly training its employees who have significant security responsibilities, the Department increases its risk of security incidents, breaches, or loss of sensitive data. Training

¹⁰ OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.

¹¹ NIST SP 800-16, “Information Technology Training Requirements: Role- and Performance-Based Model.”

UNCLASSIFIED

enhances the awareness of all personnel and ensures the protection of the Department's information systems.

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

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

Management Comments and OIG Analysis: The Department provided additional information for Recommendations 4 and 5 showing that only one user had not taken the required security awareness training. Based on the response, OIG considers both recommendations closed.

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

Management Comments: The Department agreed with the recommendation, stating that DS will have "primary responsibility for identification of personnel with significant security responsibility" and that IRM "will be consulted for policy guidance." The Department further stated that DS had set aside funding in FY 2011 to conduct an analysis of the best method for identifying and tracking personnel with significant security responsibility and that the Department will use existing resources, such as STMS and a Bureau of Human Resources system (GEMS), "to determine the most cost-effective method of extracting and presenting relevant data from these systems" after the personnel with significant security responsibility have been identified.

OIG Analysis: Based on the response, OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that personnel with significant security responsibility have been identified and trained and that STMS has been modified to capture the information requested.

E. Security Configuration Management Needs Improvement

In the FY 2009 FISMA review, OIG reported that the implementation and monitoring of configuration management controls, including the scanning process, were decentralized and were shared among bureaus, ISSOs, and IRM/IA. Furthermore, the prior year's review found that more than half of the 23 in-scope systems reviewed had exceptions. The Chief Information Officer has been working on addressing the findings identified in the FY 2009 FISMA review. For example, the Department is drafting guidance on cyber security architecture, which will include the current need for strong configuration management. In addition, the Department is working on an initiative for end-to-end configuration management, which will provide a secure operating environment, centralized management of enterprise workstations and server configurations, and implementation of central patch management.

Although the Chief Information Officer is taking actions, we found deficiencies in the configuration management process as follows:

- Of a sample of 25 systems, 24 systems were not fully compliant with the security configuration guidance provided by DS. For example, some systems did not contain the registry settings¹² required by DS. For all systems that had deficiencies, there was no evidence of exceptions or waivers by the Chief Information Security Officer. According to the FAM,¹³ system owners are required to obtain approval from the Chief Information Security Officer for waivers, exceptions, and deviations from information security controls. In addition, the FAM¹⁴ requires hardware and software to be “approved and configured in accordance with Department security configuration guidelines.”
- Of another sample of 25 systems, seven systems did not have the vendor-required critical or high priority software patches installed.

FISMA requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Standard security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources.

Responsibility for the implementation of configuration management controls for the systems, operating systems, databases, and network, including the scanning process, was decentralized because of the IT architecture. Even though DS and IRM may identify security configuration deficiencies and out-of-date software patches, the system owners are responsible for the operations to bring their systems into compliance. To correct these weaknesses, the Department is in the process of implementing the end-to-end configuration management initiative, which includes a standard operating environment to support development of strong

¹² Registry settings store the configuration settings and options on Microsoft Windows systems.

¹³ 5 FAM 1065.3-2, “Requests for Waivers, Exceptions, and Deviations.”

¹⁴ 12 FAM 625.2, “Administrative Security,” and 12 FAM 635.2, “Administrative Security: Authorized Use of Microcomputers.”

UNCLASSIFIED

In addition, the Department did not maintain documentation that supported the electronic authentication level assessment for ONE. OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance.

(b)(2)(b)(5)

In addition, the Department did not follow its policy to approve in writing all user requests for remote access.

(b)(2)(b)(5)

Recommendation 8. We recommend that the Chief Information Officer (b)(2)(b)(5)

and document the necessary risk assessment to determine the electronic authentication level for ONE.

Management Comments: The Department concurred with the recommendation, stating that ONE will be replaced by a new system, Global OpenNet, (b)(2)(b)(5)

OIG Analysis: Based on the response, OIG considers this recommendation resolved.

(b)(2)(b)(5)

G. Account Management in Active Directory Needs Improvement

The Department needs to improve account management procedures and processes in Active Directory, which is used to manage all network users' accounts. For example, we found three active accounts for 25 separated personnel. According to the FAM,¹⁸ personnel officers

¹⁸ 12 FAM 621.3-3, "System Access."

UNCLASSIFIED

must notify the data center manager, the system manager, and the ISSO immediately of any employee or contractor who has access to the system whose employment is being terminated for any reason so that access privileges can be revoked. In addition, from a population of approximately 83,000 Active Directory accounts, we found the following:

- Approximately 1,000 guest, test, and temporary accounts. The FAM¹⁹ requires the removal of default user accounts and passwords. The FAM²⁰ states that the Department may not maintain permanent user accounts and passwords on systems for visitors, training, demonstrations, or other purposes.
- Approximately 8,000 accounts that have not been used (never logged on). The FAM²¹ requires user privileges to be reviewed annually to verify that privileges are still appropriate.
- Approximately 600 accounts with passwords set not to expire. The FAM²² requires passwords to be changed at least every 60 days.

The Active Directory weaknesses occurred because the Department did not perform an annual review and recertification of users' privileges. In addition, the Active Directory administrator did not use the Active Directory automated account management tools to identify accounts that had not been used for an extended period of time.

As a result of these weaknesses, the Department increases its risk that guest, test, temporary accounts, and active accounts that are no longer needed may be used by unauthorized users for unauthorized purposes. Additionally, accounts set with passwords that do not expire increases the potential for an account password to be obtained by unauthorized users.

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

Recommendation 10. We recommend that the Chief Information Officer ensure that program managers and office managers annually review access privileges of users under their supervision so that the number of guest, test, and temporary accounts and accounts that have not been used is reduced.

Management Comments: IRM concurred with both recommendations, stating that the continuous monitoring approach (described in Finding I) will include accounts with passwords set to expire in 60 days and passwords set never to expire. The Department further stated that accounts not compliant with this standard “negatively impact site scores” and that the “‘manager’ field in Active Directory identifies the individual responsible for all accounts.”

¹⁹ 12 FAM 629.2-2, “Administrative Security”

²⁰ 12 FAM 622.1-3, “Password Controls.”

²¹ Ibid.

²² Ibid.

UNCLASSIFIED

OIG Analysis: Based on the response, OIG considers both recommendations resolved. These recommendations can be closed when OIG reviews and accepts documentation showing that the continuous monitoring program includes accounts with passwords exceeding 60 days and passwords set to never to expire.

H. Personally Identifiable Information Incidents Were Not Reported Timely

We found six of 10 instances in which the Department did not report PII data incidents to the US-CERT within 1 hour of suspecting or confirming a security breach, as required by OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. Memorandum M-06-19 requires agencies to report all incidents involving PII to the US-CERT within 1 hour of discovering an incident. The memorandum also clarifies that the reporting of all incidents involving PII should be in electronic or physical form and should not distinguish between suspected and confirmed breaches.

However, failure to notify US-CERT within the required timeframe increases the risk to individuals that their PII data may be misused. Additionally, the Department may be in violation of Federal law because of untimely notification of PII incidents.

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

Management Comments: In its response to the recommendation, the Department stated that it is “committed to meeting the requirement of reporting PII data incidents to US-CERT” in accordance with “Department policy . . . and the Computer Incident Response Team’s (CIRT) standard operating procedures.” The Department further stated that the CIRT has assigned an analyst who will monitor the incident in-box for PII reports and assign incoming PII reports’ priority status for evaluation. In addition, according to the Department, DS is continuing to develop its new “ticket tracking database,” which will enable CIRT “to automatically designate incoming PII reports priority status.”

OIG Analysis: Based on the response, OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that PII incidents are being sent to US-CERT within the 1-hour timeframe.

I. Continuous Monitoring Program Needs Improvement

To fulfill OMB and NIST continuous monitoring requirements, the Department is taking actions by using iPost to monitor its security controls, implement configuration management, and report on security status to appropriate Department officials. iPost routinely makes scanning results available to system owners, and the risk scoring reports and associated quarterly

UNCLASSIFIED

notifications to responsible system owners raise the visibility of configuration management weaknesses and provided plans for correction.

However, as identified in the FY 2009 FISMA review, continuous monitoring controls did not address the following significant risks:

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

As stated in NIST's "Frequently Asked Questions: Continuous Monitoring, June 1, 2010,"²³ organizations are required to develop a continuous monitoring strategy for their information systems and environments in which those systems operate.

Because of the lack of an enterprise-wide continuous monitoring strategy, security weaknesses of relevant IT components, such as databases and network devices, were not included in iPost.

A rigorous and well-executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. Senior officials can use this information to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of their respective information systems.

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

Management Comments: In its response to the recommendation, the Department stated that documentation supporting the continuous monitoring strategy had been provided to OIG.

OIG Analysis: Based on the response, OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and accepts documentation showing that the Risk Scoring Program dashboard includes the systems components shown in the recommendation.

J. Contingency Plans Need To Be Updated

We found that a contingency plan did not exist for the State Messaging and Archive Retrieval Toolset (SMART) system and that the Department had not performed a continuity of

²³ NIST SP 800-37, rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems."

UNCLASSIFIED

operations test of the SMART system. According to the FAM,²⁴ the data center manager and the system manager must update each contingency plan annually or when major modifications occur.

According to the Bureau of Administration, Office of Emergency Management, the Continuity of Operations–Communications Plan is undergoing revision. The plan was evaluated and discussed during an OIG inspection²⁵ and by the Department of Homeland Security’s Federal Emergency Management Agency during Continuity Exercise Eagle Horizon 2010. The SMART contingency plan is still in draft form because a secondary (or backup) site for SMART has not been identified, causing the delay in finalizing the contingency plan.

Without testing the contingency plan at the system level, the Department cannot evaluate the plan’s overall effectiveness, identify significant weaknesses, and ensure that corrective actions are made.

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

Management Comments: The Department concurred with the recommendation, stating that a secondary site had been identified and the completed contingency plan and contingency system would be developed and tested by September 2011.

OIG Analysis: Based on the response, OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that the contingency plan and system were tested by the date specified.

K. Oversight of Contractor Systems Requires Improvement

The Department did not consistently maintain required documentation for contractor systems; for example, a contract for one system did not contain the required information security clauses from the DOSAR. The DOSAR²⁶ states that all offers and bids submitted in response to solicitations must address the approach for completing the security plan and certification and accreditation requirements as required.

We also found that the Department did not have an effective mechanism in place to identify the total number of contractors who had access to and privileges within the Department’s network, applications, databases, and data. According to OMB Memorandum M-10-15, “Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems.”

²⁴ 12 FAM 622.3-2, “Contingency Plan Preparation.”

²⁵ *The Bureau of Administration’s Office of Emergency Management* (ISP-I-10-43, July 2010).

²⁶ DOSAR 652.239-70, “Information Technology Security Plan and Accreditation.”

UNCLASSIFIED

The process to provide oversight to contractor systems and personnel by bureaus and offices is decentralized, and the system to provide better contractor oversight has not been completed. For instance, to obtain information on the total number of contractor personnel, personnel from each bureau and office would have to be contacted. DS and the Bureau of Human Resources began collaboration on the development of the Contractor Personnel Support System. According to DS, once the system is fully implemented and integrated with other systems, it will provide more contractor oversight information for the Department.

The lack of information security requirements increases the risk that contractor systems have security controls that are inadequate and makes other Department software and hardware vulnerable to unauthorized access, use, disclosure, disruption, modification, or destruction. Additionally, without adequate contractor oversight, the Department has minimal assurance that the contractor's information security controls are compliant with FISMA, OMB requirements, and NIST standards.

Without an effective mechanism to identify and track contractor personnel who have been granted access and privileges within the Department's network and access to the Department's software, data, and databases, the Department cannot accurately assess whether contractor personnel have received the required information security awareness training and have gone through the proper security clearance process.

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

Recommendation 15. We recommend that the Bureau of Diplomatic Security, in coordination with the Bureau of Administration, establish procedures to identify the total number of contractors who have access to Department of State systems.

Management Comments: In its response, the Department agreed with both recommendations, stating that the Bureau of Administration will review contract processes to ensure that contracts are reviewed before they are signed and that a copy of the updated Quality Assurance Plan will be provided to OIG. The Department further stated that the CIO had developed a procedure to use Active Directory accounts to identify the total number of individuals (including contractors) who have access to the Department's network and that compliance with this procedure, which is being enforced by the site scoring process, had begun on November 1, 2010.

OIG Analysis: Based on the response, OIG considers both recommendations resolved. These recommendations can be closed when OIG reviews and accepts documentation showing that the contracts contain the required DOSAR clauses and verifies that the Department can identify the total number of contractors who have access to the Department's network.

List of Recommendations

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

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

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

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

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

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

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

Recommendation 8. We recommend that the Chief Information Officer install an NIST-approved encryption algorithm that controls access to support controls access to OpenNet Everywhere (ONE), reconfigure the ONE session timeout setting to 20 minutes, retain remote access authorization forms to show supervisory approval, and document the necessary risk assessment to determine the electronic authentication level for ONE.

Recommendation 9. We recommend that the Chief Information Officer enhance the Active Directory account management automated tools to flag accounts that have not been used within

UNCLASSIFIED

the past 60 days and ensure that all accounts are configured with passwords that expire every 60 days.

Recommendation 10. We recommend that the Chief Information Officer ensure that program managers and office managers annually review access privileges of users under their supervision so that the number of guest, test, and temporary accounts and accounts that have not been used is reduced.

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

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

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

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

Recommendation 15. We recommend that the Bureau of Diplomatic Security, in coordination with the Bureau of Administration, establish procedures to identify the total number of contractors who have access to Department of State systems.

UNCLASSIFIED

Acronyms

Department	U.S. Department of State
DOSAR	Department of State Acquisition Regulations
DS	Bureau of Diplomatic Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IRM/IA	Bureau of Information Resource Management, Office of Information Assurance
ISSO	Information System Security Officer
IT	information technology
ITCCP	Information Technology Change Control Board
ITSP	Information Technology Strategic Plan
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONE	OpenNet Everywhere
PII	personally identifiable information
POA&M	Plan of Action and Milestones
SMART	State Messaging and Archive Retrieval Toolset
US-CIRT	U.S. Computer Information Readiness Team
US-CERT	U.S. Computer Emergency Readiness Team

Objectives, Scope, and Methodology

In order to fulfill its responsibilities related to the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) contracted with Williams, Adley & Company, LLP (referred to as “we” in this appendix), an independent public accountant, to review the Department of State’s information security program and practices to determine the effectiveness of such programs and practices for FY 2010.

FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to the Office of Management and Budget (OMB). OMB uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

We conducted the review from June through September 2010. In addition, we performed the review in accordance with FISMA, OMB, and NIST guidance. We and OIG believe that the evidence obtained provides a reasonable basis for the findings and conclusions represented in this report.

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

- OMB Memorandums M-02-01, M-04-04, M-06-19, and M-10-15.
- Department policies and procedures.
- Federal laws, regulations, and standards (such as the Computer Security Act of 1987, FISMA, and OMB Circular A-130, Appendix III.)
- National Institute of Standards and Technology (NIST) Special Publications, Federal Information Systems Processing Publications (FIPS), other applicable NIST publications, and industry best practices.

The review evaluated the Department’s information security program policies, procedures, and processes in the following areas:

- System inventory.
- Risk management framework (formerly Certification & Accreditation).
- Security configuration management.
- Incident response and reporting.
- Security training.
- Plans of action and milestones (POA&M).
- Remote access.

UNCLASSIFIED

- Account and identity management.
- Continuous monitoring.
- Contingency planning.
- Oversight of contractor systems.

The audit covered the period October 1, 2009, to September 30, 2010. During the fieldwork, we took the following actions:

- Determined the extent to which the Department's information security plans, programs, and practices complied with FISMA requirements; applicable Federal laws, regulations, and standards; relevant OMB Circular A-130, Appendix III, processes and reporting requirements; and NIST and FIPS requirements.
- Reviewed all relevant security programs and practices to report on the effectiveness of the Department's agency-wide information security program in accordance with OMB's annual FISMA reporting instructions. The evaluation approach addressed OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, which outlines changes to both reporting processes and changes to the questions.
- Assessed programs for monitoring of security policy and program compliance and responding to security events (that is, unauthorized changes detected by intrusion detection systems).
- Performed testing of major systems at the discretion of OIG. We tested 30 systems for our sample.
- Assessed the adequacy of internal controls related to the areas audited. Significant deficiencies identified during the review are reported in the report.
- Evaluated the Department's remedial action taken to address the previously reported Information Security Program control weaknesses identified in OIG's report *Review of the Information Security Program at the Department of State* (AUD/IT-10-10, Nov. 2009).

Follow-up of Recommendations From the FY 2009 FISMA Report

The review team reviewed actions implemented by management to mitigate the findings identified in the FY 2009 FISMA report. The current status of each of the recommendations is as follows:

Recommendation 1: The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to identify critical and volatile controls that should be tested for each application and system; expand the quality control program to include analysis of how well certification testing addresses critical, volatile, and inherited controls; and ensure all controls are tested over a 3-year C&A [Certification and Accreditation] cycle.

2010 Status: Partially implemented. The Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), has updated the Annual Control Assessment Toolkit to incorporate the changes regarding Critical and Volatile Controls. The Annual Control Assessment exit criteria checklist has been modified to advise the reviewer to be especially vigilant in reviewing all of these controls.

Recommendation 2: The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should supplement the current information provided in the C&A Main Toolkit and Inventory Toolkit to include additional guidance for annual testing of critical and volatile controls and be more proactive in reviewing Systems Security Plans and test results to ensure compliance with the methodology in the C&A Toolkits.

2010 Status: Closed. Annual Control Assessment Toolkit was modified to include information on the rationale for selecting Critical & Volatile Controls at the Department level. A note was added indicating that the Department has identified CA-3 as a mandatory critical control. Main Certification and Accreditation Toolkit was also modified to provide more guidance to system owners.

Recommendation 3: The Chief Information Security Officer, Bureau of Information Resource Management, and systems owners should update the Contingency Plan (CP) Toolkit to include requirements that systems owners should review and revise CP following CP failed test results, create POA&M [Plans of Action and Milestones] for failed CP control tests, and include verification by the Office of Information Assurance that systems owners are complying with CP Toolkits and methodology.

2010 Status: Closed. Improved guidance was provided in the Contingency Plan Toolkit and the exit checklist.

UNCLASSIFIED

Recommendation 4: The Chief Information Security Officer, Bureau of Information Resource Management, and the Senior Coordinator for Security Infrastructure Directorate should work in an initiative for end-to-end configuration management which will provide a secure operating environment, centralized management of enterprise workstations and server configurations, and implementation of central patch management. Create an Information Security Architecture that outlines information security responsibility for the Department of State's decentralized information security environment.

2010 Status: This is a repeat recommendation from the FY 2009 report. It has become Recommendation 7 (Finding E) in the FY 2010 report.

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

- Record and report systemic security weaknesses identified through the iPost/ site Scoring process as POA&M actions to ensure that these weaknesses are tracked, prioritized, and remediated.
- Report POA&M actions on a quarterly basis for sites that have low scores, requiring them to raise those scores.
- Report POA&M actions for risk covered by iPost scoring "exceptions."

2010 Status: Closed. The pilot POA&M Grading Memorandum has been created. The systemic weaknesses and exceptions data are captured in the POA&M.

Recommendation 6: The Chief Information Security Officer, Bureau of Information Resource Management, should work with systems owners to implement a method that provides timely and complete updates to the POA&M database. Validate the information in the Department POA&M database, and review the Corrective Action Plan report before it is submitted to OMB.

2010 Status: This is a repeat recommendation from the FY 2009 report. It has become Recommendation 3 (Finding C) in the FY 2010 report.

Recommendation 7: The Chief Information Officer, Bureau of Information Resource Management and systems owners should work together to develop, publish, and implement detailed Standard Operating Procedures (SOP) for addressing Information Technology (IT) audit related weaknesses and findings.

Status: Closed. An SOP was created.

UNCLASSIFIED

Recommendation 8: The Director of the Office of Computer Security, Bureau of Diplomatic Security in coordination with the Director of the Foreign Service Institute should implement methods to globally enforce the security awareness policies and enhance existing methods to identify users who should take the Cyber Security Awareness Training Course.

2010 Status: This is a repeat recommendation from the FY 2009 report. It has become Recommendations 4 and 5 (Finding D) in the FY 2010 report, of which both recommendations are closed.

Recommendation 9: The Bureau of Diplomatic Security, Assistant Director of Training, the Bureau of Information Resource Management, Chief Information Officer, and the Bureau system owners should improve methods to identify individuals with significant security responsibilities, ensure that they take the required training every 3 years, record the training records in the Office of Personnel Management-approved centralized system, and provide management with tools to monitor compliance with the training requirement.

2010 Status: This is a repeat recommendation from the FY 2009 report. It has become Recommendation 6 (Finding D) in the FY 2010 report.

Recommendation 11 (from FY 2008): The Chief Information Officer should establish a process to monitor and validate security awareness training provided to those individuals without access to Department networks.

2010 Status: Open. The Department is in the process of developing a program.

UNCLASSIFIED

Appendix C



United States Department of State

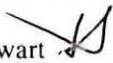
Chief Information Officer
Information Resource Management

Washington, D.C. 20520-6311

November 8, 2010

UNCLASSIFIED
MEMORANDUM

TO: OIG – Mr. Harold W. Geisel

FROM: IRM – Susan H. Swart 

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

REF: OIG Memo Dated Nov. 1, 2010 Subject: Draft Report on *Review of Department of State Security Program*

Thank you for the opportunity to provide comments on the draft FISMA Report for 2010. Our response to the annual FISMA review is attached, and was coordinated with the Bureau of Diplomatic Security, Bureau of Administration, Bureau of Human Resources and the Foreign Service Institute. Please consider this a consolidated reply to your request.

We have focused our comments on whether or not the Department accepts the recommendation as part of this annual FISMA audit, as requested.

When we agreed with a recommendation, we have described how we plan to close it. We propose these recommendations be considered resolved.

With regard to the factuality of the detailed findings, the Department's response primarily focused upon those issues that were material to Recommendations due to our mutual desire to give the Secretary time for review of this response.

We especially appreciate the professionalism of Ms. Klemstine throughout this review. We look forward to planning the 2010 review with the members of your team at your convenience.

UNCLASSIFIED

UNCLASSIFIED

2

Attachment: Department Response to Draft Report on Review of Department of
State Security Program

UNCLASSIFIED

UNCLASSIFIED

Department Response to Draft Report on *Review of Department of State Security Program*

FISMA Inventory:

Summary Finding: The Department's inventory management processes and procedures do not ensure that an accurate inventory of FISMA reportable systems is maintained. Without an accurate FISMA system inventory list, the Department's process to support information resources management for technology planning, budgeting, and acquisition may be hampered.

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

Department Response: *We accept this recommendation and request that it be closed.* – We are pleased the OIG found all systems needed in inventory were present. Based upon the OIG's findings related to this Recommendation, namely the Department's inclusion of retired systems in its asset and FISMA inventory, the Recommendation should be closed. As a matter of policy, retired systems are not removed from the asset inventory (ITAB), but marked as retired, when appropriate. This ensures maintenance of historical records. The closure of the recommendation is warranted because there is no prohibition of inclusion of retired systems in inventory. The Department would expect to remove retired systems in FISMA inventory in the next quarter in which action such as an annual test or C&A was required for that system. Having the system remain in inventory until this trigger event causes review (and change to retired status) has no harmful effect on security. The Department would be happy to meet with OIG staff to discuss how we might improve this process. We recommend that the recommendation be closed.

Risk Management Framework:

Summary Finding: The security authorization process was not performed on all contractor systems, and the security authorization packages had expired for four systems. These conditions weaken the Department's risk management framework because changes within the systems and the systems' control environment may introduce new risks and vulnerabilities into the Department's environment.

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

Department Response: *Request Revision to Recommendation.* – The Department requests the Recommendation and findings be revised to remove references to low-cost/low-impact systems. NIST SP 800-37 gives federal agencies considerable discretion in the selection of system accreditation boundaries. Moreover, OMB A-130 only requires certification and accreditation

UNCLASSIFIED

(vice control definition and testing) for major information systems. Consistent with OMB and accepted by previous OIG reviews, the Department has defined low-impact/low-cost systems in such a manner they are included within the accreditation boundary of the network on which they run. The Department can provide detailed documentation and justification of this decision, which has been used since 2007. If the Recommendation is revised as requested, the Department will request closure of the recommendation when all applicable systems, as defined by the Department have completed C&A.

Plans of Actions and Milestones:

Summary Finding: The Department did not prioritize the severity of security weaknesses, consistently record required resources for remediation of security weaknesses, and update remediation schedules to reflect actual performance, all of which impeded the Department's ability to assess and monitor the progress of corrective actions.

Recommendation 3. We recommend that the Chief Information Officer develop criteria for system owners to prioritize Plan of Action and Milestones (POA&M) corrective actions; develop a process to periodically update the resources recorded in the POA&Ms; and update, in the POA&Ms, those completion dates for corrective actions that have expired.

Department Response: *Request Revision to Recommendation.* – The Department of State POA&M system prioritizes all findings as high, moderate and/or low. Thus, the Department requests the OIG remove references to a lack of prioritization from its Findings and Recommendation. Given the changes to reporting requirements under cyber-scope, the Department will seek DHS (with OIG, if the OIG so desires) clarification on the desired timeliness and level of aggregation of these updates, and request closure of this revised Recommendation when the Department's performance meets current DHS requirements.

Security Awareness Training:

Summary Finding: Four of 25 employees tested had completed the initial information security awareness training. The Department did not identify all employees who had significant security responsibilities and provide specialized training, as required by NIST. One employee in our test of employees hired in FY 2010 did not have the required security clearance.

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

Recommendation 5. We recommend that the Chief Information Officer, the Foreign Service Institute, and the Bureau of Diplomatic Security complete the Department of State's corrective action plan (which involves Active Directory, security awareness

UNCLASSIFIED

completion data, and iPost) to enforce the security awareness policy to suspend a user's access if the Cyber Security Awareness course is not taken within the required timeframe.

Department Response: *Request Recommendation Be Closed.* – The Department agrees that the means for ensuring completion of awareness training should be strengthened. However, examination of the data provided regarding the four users found not to have completed awareness training indicates that of the four, only one user had not taken the training. Of the three remaining users, two had expired accounts and one did not yet have an active account.

The Department has recently implemented the corrective action plan by taking the following actions: (1) the PS800 Annual Cyber Security Awareness course is being updated to automatically reset user accounts to expire 365 days from successful completion of the course; and (2) PS800 course completion data is being posted in iPost and incorporated into site risk scoring. This allows the ISSOs to identify users who are not in compliance and enforce Department policy. Given these actions, the Department requests the recommendation be closed and the associated Executive Summary language be revised.

Recommendation 6. [6.1:] We recommend that the Chief Information Officer and the Bureau of Diplomatic Security define and identify personnel who have significant security responsibilities and ensure that they receive the appropriate training. **[6.2:]** Also, the Student Training Management System should be modified to capture other training systems, such as those paid for by the Department of State, to meet continuing professional education requirements.

Department Response for 6.1: *Agree with Recommendation.* – The Department agrees with this part of the Recommendation. The Department will assign primary responsibility for identification of personnel who have significant security responsibilities to the Bureau of Diplomatic Security, and the Bureau of Information Resource Management will be consulted for policy guidance. DS has set aside funding in FY11 to conduct an analysis of the best method for identifying and tracking these personnel.

Department Response for 6.2: *Agree with Recommendation.* – The Student Training Management System is the only official authorized management training system for the Department of State records and includes training funded by the Department. HR's GEMS provides a mechanism called Employee Profile for individuals to record other training taken. Duplication of either function is unnecessary. In determining if those with significant security responsibilities have met the training and development criteria, the Department will make use of these existing resources and determine the most cost-effective method of extracting and presenting all relevant data from these systems. This will be done after 6.1 is completed. Upon completion of Part 6.2, the Department will request closure of this Recommendation.

Security Configuration Management:

Summary Finding: Twenty-four of 25 systems tested were not compliant with the security configuration guidance provided by the Bureau of Diplomatic Security (DS), and seven of 25 systems did not have the vendor-required critical or high priority software patches to be installed. Without sufficient configuration management, the Department's data may be exposed to loss of integrity and confidentiality because configuration standards may not be implemented.

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

Department Response: *Agree with this Recommendation.* – The end-to-end configuration management initiative has several elements including centralization of patching and automated enforcement of configuration standards. Patch support has now been centralized to over half of the Department with full coverage scheduled for completion in fiscal year 2011. Automated enforcement of configuration standards is currently being piloted with broader deployment expected over the next two fiscal years. Further, the Department's continuous monitoring has brought significant results. The iPost risk scoring mechanisms are designed to score systems against the recommended and mandatory standards for the owners, who retain responsibility for the compliance and patching of their systems. Any individual system may have some minor variations and not represent a substantial cyber risk, but will be flagged by our risk scoring methodology.

Without knowing the cumulative risk score for the 25 sampled systems, the risk cannot be properly assessed. It should be noted this approach has significantly reduced the number of configuration and patch problems over the last two years (by 90%). The Department's policy and configuration guidance are part of a Risk Management approach balancing business need with cyber risk. The Department will request closure when implementation of these initiatives has made significant progress.

OpenNet Everywhere:

(b)(2)(b)(5)
[Redacted text block]

Recommendation 8. We recommend that the Chief Information Officer (b)(2)(b)(5)
[Redacted text block]

(b)(2)(b)(5) and document the necessary risk assessment to determine the electronic authentication level for ONE. completion data, and iPost) to enforce the security awareness policy to suspend a user's access if the Cyber Security Awareness course is not taken within the required timeframe.

Department Response: Request Recommendation Be Closed. – The Department agrees that the means for ensuring completion of awareness training should be strengthened. However, examination of the data provided regarding the four users found not to have completed awareness training indicates that of the four, only one user had not taken the training. Of the three remaining users, two had expired accounts and one did not yet have an active account.

The Department has recently implemented the corrective action plan by taking the following actions: (1) the PS800 Annual Cyber Security Awareness course is being updated to automatically reset user accounts to expire 365 days from successful completion of the course; and (2) PS800 course completion data is being posted in iPost and incorporated into site risk scoring. This allows the ISSOs to identify users who are not in compliance and enforce Department policy. Given these actions, the Department requests the recommendation be closed and the associated Executive Summary language be revised.

Recommendation 6. [6.1:] We recommend that the Chief Information Officer and the Bureau of Diplomatic Security define and identify personnel who have significant security responsibilities and ensure that they receive the appropriate training. [6.2:]Also, the Student Training Management System should be modified to capture other training systems, such as those paid for by the Department of State, to meet continuing professional education requirements.

Department Response for 6.1: Agree with Recommendation. – The Department agrees with this part of the Recommendation. The Department will assign primary responsibility for identification of personnel who have significant security responsibilities to the Bureau of Diplomatic Security, and the Bureau of Information Resource Management will be consulted for policy guidance. DS has set aside funding in FY11 to conduct an analysis of the best method for identifying and tracking these personnel.

Department Response for 6.2: Agree with Recommendation. – The Student Training Management System is the only official authorized management training system for the Department of State records and includes training funded by the Department. HR's GEMS provides a mechanism called Employee Profile for individuals to record other training taken. Duplication of either function is unnecessary. In determining if those with significant security responsibilities have met the training and development criteria, the Department will make use of these existing resources and determine the most cost-effective method of extracting and presenting all relevant data from these systems. This will be done after 6.1 is completed. Upon completion of Part 6.2, the Department will request closure of this Recommendation.

Security Configuration Management:

Summary Finding: Twenty-four of 25 systems tested were not compliant with the security configuration guidance provided by the Bureau of Diplomatic Security (DS), and seven of 25 systems did not have the vendor-required critical or high priority software patches to be installed. Without sufficient configuration management, the Department's data may be exposed to loss of integrity and confidentiality because configuration standards may not be implemented.

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

Department Response: *Agree with this Recommendation.* – The end-to-end configuration management initiative has several elements including centralization of patching and automated enforcement of configuration standards. Patch support has now been centralized to over half of the Department with full coverage scheduled for completion in fiscal year 2011. Automated enforcement of configuration standards is currently being piloted with broader deployment expected over the next two fiscal years. Further, the Department's continuous monitoring has brought significant results. The iPost risk scoring mechanisms are designed to score systems against the recommended and mandatory standards for the owners, who retain responsibility for the compliance and patching of their systems. Any individual system may have some minor variations and not represent a substantial cyber risk, but will be flagged by our risk scoring methodology.

Without knowing the cumulative risk score for the 25 sampled systems, the risk cannot be properly assessed. It should be noted this approach has significantly reduced the number of configuration and patch problems over the last two years (by 90%). The Department's policy and configuration guidance are part of a Risk Management approach balancing business need with cyber risk. The Department will request closure when implementation of these initiatives has made significant progress.

OpenNet Everywhere:

Recommendation 8. We recommend that the Chief Information Officer

UNCLASSIFIED

and document the

necessary risk assessment to determine the electronic authentication level for ONE.

Department Response: *Agree with Recommendation.* – The Department is currently replacing ONE with a new system called Global OpenNet (GO) (b)(2)(b)(5) [REDACTED]
[REDACTED] We will request closure when GO has been implemented and meets the intent of this recommendation.

Account Management:

Summary Finding: From a population of approximately 83,000 Active Directory accounts, we found approximately 1,000 guest, test, and temporary accounts; 8,000 accounts that had not been used (never logged on); and 600 accounts that had passwords that were set so that they would not expire. Therefore, these accounts are susceptible to being compromised by unauthorized users for unauthorized purposes.

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

Recommendation 10. We recommend that the Chief Information Officer ensure that program managers and office managers annually review access privileges of users under their supervision so that the number of guest, test, and temporary accounts and accounts that have not been used is reduced.

Department Response: *Agree with Recommendations 9 & 10.* – Service accounts are critical to the operations of systems and applications. These accounts are necessary but are strictly administered and monitored. Deleting or expiring these accounts would have serious, negative impact on operations. Shared accounts are often created to provide shared access to organizational or functional mailboxes. These accounts are also strictly administered and monitored. Individuals do log on using either type account, thus creating a sizable numbers of accounts that never register a log-on. Flagging these accounts as directed by the applicable Recommendation would be overly cumbersome and would prove of little security value.

However, in the interests of addressing the underlying issue, the continuous monitoring approach takes the password expiring after 60 days into consideration. Any accounts not compliant with this standard negatively impact site scores. This includes accounts with passwords set never to expire. The Department believes this meets the second half of Recommendation 9. The Department believes the ‘manager’ field in Active Directory identifies the individual responsible for all accounts, including service, guest, and test accounts and as such, the Department will use this foundation to act upon Recommendation 10.

Personally Identifiable Information:

Summary Finding: We found six instances in which the Department did not report personally identifiable information (PII) data incidents to the U.S. Computer Emergency

UNCLASSIFIED

Response Team (US-CERT) within 1 hour of suspecting or confirming a security breach, as required by OMB. Failure to notify US-CERT within the required timeframe increases the risk to individuals that their PII data may be misused. Also, the Department may be in violation of Federal laws.

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

Department Response: *Request Recommendation be Closed.* – The Department is committed to meeting the requirement of reporting PII data incidents to US-CERT as expeditiously as possible and has explicitly stated as such in Department policy (5 FAM 460) and the Computer Incident Response Team’s (CIRT) standard operating procedures, which delineate in detail how PII incident reports are handled internally and routed to US-CERT. The CIRT procedures are designed to ensure that incoming reports of missing PII are reviewed and validated so as to avoid false positives and address simultaneously any related network security issues. Once this evaluation is completed, CIRT generates a PII ticket and relevant incident information is referred to US-CERT within 1-hour.

During the course of this FISMA evaluation, CIRT undertook the following steps to further enhance the Department’s ability to review and report PII incidents:

- As of July 1, 2010 the CIRT team assigned an analyst to monitor the incident in-box for PII reports and assign incoming PII reports priority status for evaluation.
- DS is continuing to develop its new ticket tracking database which will enable CIRT to automatically designate incoming PII reports priority status.

Given these actions, the Department requests this recommendation be closed.

Continuous Monitoring Program:

Summary Finding: The scanning tools do not assess the Oracle configuration, the Department’s most common database system, for configuration control weaknesses that could adversely impact application access controls. Scanning results for routers, firewalls, and Demilitarized Zone servers were not available in iPost; therefore, the results were not used in risk scoring.

Recommendation 12. We recommend that the Chief Information Officer develop a continuous monitoring strategy.

Department Response: *Request Modification of Recommendation and Associated Text.* – The Department has previously provided documentation to the OIG that the Department’s strategy includes these elements. Moreover, the Department performs this kind of monitoring during annual testing and C&A, as required. The Department requests that the Recommendation be revised to say that “the Risk Scoring Program implement the Department’s CM strategy to

UNCLASSIFIED

include scanning of databases, firewalls, routers, and switches on a more frequent basis and inclusion of the results into its dashboard". The Department also notes that the level and frequency of continuous monitoring being requested is not required by FISMA or its associated authorities.

Partial Finding: The SMART contingency plan is still in draft form because a secondary (or backup) site for SMART has not been identified, causing the delay in finalizing the contingency plan.

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

Department Response: *Agree with Recommendation.* – The Department has identified ESOC East as the secondary site for SMART. The Department is implementing our contingency plan in stages. Stage 1 of the plan is complete and includes daily full backups of SMART data offsite at ESOC East. Stage 2 of the plan will greatly reduce the length of time required to restore SMART functionality offsite. SMART's contingency system design documentation has successfully passed a peer review including external stakeholders. The design documentation describes a contingency solution that will provide SMART functionality within hours of either a planned or emergency failover. The completed contingency plan as well the contingency system itself will be developed and tested by September 2011. Upon completion of the contingency plan, the Department will request closure of this Recommendation.

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

Department Response: *Agree with Recommendation.* – The Bureau of Administration will review contract processes to ensure contracts are reviewed prior to final signatures. Such reviews will include whether or not the applicable provisions are included in relevant information technology and professional service contracts. Upon completion of this review, AQM will issue an updated Quality Assurance Plan and provide a copy to the OIG. Upon documented establishment of these processes, the Department will request closure of the Recommendation.

Recommendation 15. We recommend that the Bureau of Diplomatic Security, in coordination with the Bureau of Administration, establish procedures to identify the total number of contractors who have access to Department of State systems.

Department Response: *Agree with Recommendation.* – The Chief Information Officer has developed a procedure to use Active Directory accounts to identify the total number of persons (including contractors) who have access to the Department's network. Compliance with this procedure is being enforced by a process of site scoring, which started on November 1, 2010. Upon implementation of this process, the Department will request closure of this Recommendation.