~~SENSITIVE BUT UNCLASSIFIED~~

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

Information Technology Memorandum Report

Review of the Information Security Program at the Department of State

Report Number IT-I-06-03, September 2006

~~IMPORTANT NOTICE~~

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

~~SENSITIVE BUT UNCLASSIFIED~~

United States Department of State
and the Broadcasting Board of Governors

Inspector General

PREFACE

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

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

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

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

Howard J. Krongard

Howard J. Krongard
Inspector General

OVERVIEW

The Federal Information Security Management Act (FISMA)[1] requires that all federal agencies develop and implement an agency-wide information security (INFOSEC) program designed to safeguard information technology (IT) assets and data. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over IT that support federal operations and assets, and it provides a mechanism for improved oversight of the INFOSEC programs government-wide. FISMA requires that each agency's INFOSEC program must include policies and procedures and must document the following:

- Periodic risk assessments;
- INFOSEC policies and procedures;
- An assessment of threats, including their likelihood and impact;
- Policies and procedures for detecting security vulnerabilities;
- Evaluation and periodic testing of how well security policies are working;
- An inventory of software and hardware assets;
- Security awareness training and expected rules of behavior for end–users;
- An evaluation of the technical, management, and operational security controls;
- Procedures for reporting and responding to security incidents;
- A process for addressing any deficiencies identified; and
- Contingency plans to facilitate the continuity of operations in a disaster.

FISMA also requires that the Office of Inspector General (OIG) provide an annual independent evaluation of the effectiveness of the agency's INFOSEC programs and practices. FISMA provides a framework and approach designed to assist OIG with:

1. Determining the current status of agency security programs by testing management and technical controls;
2. Assessing management, policies, and guidelines; and
3. Providing feedback to agency management through the annual evaluation process to assist with establishing and achieving improvement goals for INFOSEC.

Details, including the scope and methodology of the review, are discussed in Appendix A. Appendix B includes a list of 2004 and 2005 FISMA recommendations that will be closed and reissued in this report. Appendix C lists all other open recommendations from the 2004 and 2005 FISMA reviews that still require action and compliance from the Office of the Chief Information Officer (CIO).

[1] 44 U.S.C. § 3541 et seq.

BACKGROUND

This review examined how effectively the Department of State ensures the confidentiality, integrity, and availability of information by the agency-wide INFOSEC program. It assessed the coverage of the management, technical, and operational controls identified by National Institutes of Standards and Technology (NIST) in the *Federal Information Processing Standard (FIPS) 199 and 200*[2]. By using FIPS 199 and 200 as the criteria for its tests, OIG sought to maintain the consistency, comparability, and completeness of the results of this evaluation. The evaluation also included program controls identified in numerous NIST publications (NIST 800-53[3], NIST 800-200[4], NIST 800-37[5], NIST 800-55[6], and NIST SP 800-26[7]). These controls are used to implement INFOSEC requirements in accordance with FISMA.

Information must be adequately protected regardless of how it is handled, processed, transported or stored. An effective INFOSEC program addresses the risks, benefits, and processes involved with all information resources. INFOSEC is concerned with all information processes, physical and electronic, and with the overall protection of information at all points within its lifecycle in the organization. INFOSEC deals with all aspects of information whether spoken, written, printed, electronic, or in any other medium regardless of whether it is being created, viewed, transported, stored, or destroyed. It includes the protection of information assets against the risk of loss, operational discontinuity, misuse, unauthorized disclosure, inaccessibility, or damage. It is also concerned with the increasing potential for civil or legal liability that organizations face when information is inaccurate, lost, or not sufficiently protected. This contrasts with IT security, which is concerned with security of information within the boundaries of the technology domain.

The Clinger-Cohen Act[8] of 1996 created the CIO position and assigned it with many responsibilities, including:

1. Provide advice and assistance to senior managers on IT acquisition and management;
2. Develop, maintain, and facilitate implementation of a sound and integrated IT architecture; and
3. Promote effective and efficient design and operation of all major IT (security and operations) processes for the agency, including improvements to work processes.

---

[2] FIPS 199- *Standards for Security Categorization of Federal Information and Information Systems*, February 2004; FIPS 200- *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
[3] NIST 800-53- *Recommended Security Controls for Federal Information Systems*.
[4] NIST 800-200 – *Minimum Security Controls for Federal Information Systems*.
[5] NIST 800-37- *Guide for the Security Certification and Accreditation of Federal Information Systems*.
[6] NIST 800-55 – *Security Metrics Guide for Information Technology Systems*.
[7] NIST SP 800-26- *Guide for Information Security Program Assessments and System Reporting*.
[8] Clinger-Cohen Act , also known as the Information Management Technology Reform Act (Pub. L 104-106).

Like Clinger-Cohen, FISMA assigned the CIO with the authority and responsibility to administer key functions under the statute, including designating a chief information security officer (CISO) to assist in developing and maintaining an agency-wide INFOSEC program. That program should include:

- Developing and maintaining INFOSEC policies and procedures;
- Training and overseeing personnel with significant responsibilities for INFOSEC; and
- Assisting senior agency officials with their responsibilities.

To help administer INFOSEC activities for the Department, the CIO, under the purview of the CISO, created the Office of Information Assurance within the Bureau of Information Resource Management (IRM/IA). In July 2006, the former CISO from the U.S. Agency for International Development joined the Department as the new CISO.

RESULTS IN BRIEF

This review focused on significant INFOSEC initiatives on information and information systems that revealed programmatic and systemic issues, many of which have been cited in previous FISMA reviews dating back to 2004. OIG did not separately assess specific reason(s) why IT policies, procedures, and processes in place may not be adequately resolving recommendations which continue to remain open. However, OIG encourages all program officials and IT stakeholders in the coming year to fully support the CIO in addressing this report's findings.

Progress continues to be made regarding timely and accurate internal and external reporting and handling of computer security incidents and in addressing data privacy requirements. However, other areas remain unresolved and will require further attention by senior management. These areas include:

- (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
- Creating a complete inventory of the Department's IT assets and contractor systems.
- Verifying that appropriate security levels are being assigned to IT applications and systems.
- Addressing issues pertaining to the Information Systems Security Officer (ISSO) function.
- Identifying the number of employees who must take computer security awareness training.
- Evaluating the current approach (including the framework in place) to handle the certification and accreditation (C&A) process.
- Including and addressing IT security findings identified by OIG and all system owners in the Plan of Action and Milestones (POA&M) process.

OIG received formal comments on the draft report from the Department and included them in their entirety in Appendix D. Overall, the CIO agrees with seven of the nine recommendations. For the remaining two, the CIO agrees with the intent of the recommendations but considers the matters closed based on past and current efforts. The OIG will address the CIO's comments during its compliance process.

PROGRESS IN ADDRESSING INFORMATION SECURITY

Agency-Wide Information Security Program

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

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

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

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

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

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

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

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

Recommendation 1: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 2: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Configuration Management

Inadequate Inventory of IT Assets

The OIG 2004 and 2005 FISMA[10] reports noted that the Department continues to have an incomplete inventory of its IT assets. FISMA, the Clinger-Cohen Act, and Office of Management and Budget (OMB) Circular A-130 require that the CIO identify all information systems[11] and assets that support the Department's mission and operations. Using definitions provided by OMB, the Department should identify the network, infrastructure, applications, and all sites and facilities domestically and overseas that are to be included in its inventory.

IRM/IA and the IRM Office of Business, Planning and Customer Service have been participating in meetings to reconcile the inventory in the Information Technology Applications Base (ITAB) toolkit. ITAB is part of the Department's efforts to increase the sharing and reuse of information across the Department. Through ITAB, the Department has reported 252 systems of which 240 are fully authorized. However, it has not verified whether all domestic and overseas systems, applications, sites, and facilities have been properly included.

---

[10] *Review of the Information Security Program at the Department of State*, Memorandum Report IT-A-04-08, September 2004, and *Review of the Information Security Program at the Department of State,* Memorandum Report IT-I-05-09, September 2005.

[11] An information system is a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. *(OMB Guidance M-06-20)*

During this review, the OIG team identified public web applications[12] that had not been included in the Department's inventory. Due to restricted time, the team could not determine whether other items were missing. Therefore, the Department's inventory contains an incomplete listing of IT assets.

Recommendation 3: The Chief Information Officer should verify that all information technology assets of the Department are reported and accounted for within a comprehensive inventory process.

Inadequate Inventory of Contractor Systems

Per OIG 2004 and 2005 FISMA reports, IRM and DS have not adequately identified and accounted for, (1) all contractor-based systems, (2) contractor-provided services, or (3) joint systems or services provided by another agency for their respective program or mission, as required by FISMA, OMB Circular A-130, and NIST guidance. The OIG team located at least one contractor system[13] that was connected to the Department's infrastructure but had not been included in the IT inventory.

Although the Department has created a plan to capture the inventory of contractor systems, the Department still has not agreed upon the parameters to be used for identifying what is to be included in the IT inventory. Although 26 contractor sites have been approved for connection to the network infrastructure, Department officials stated the lack of a uniform interpretation of what should be included as a "contractor system" has affected their ability to adequately capture the universe of systems to be included in the inventory. For example, an L representative said that only information systems operated by the contractor are to be included in the inventory, but DS said that all contractor systems - regardless of whether or not they are used on behalf of the Department - should be included. IA, on the other hand, said Department systems located at contractor facilities, contractor systems connected to the network, and the systems of contractors that perform Department functions regardless of location should be included in the inventory. The CIO has the responsibility to identify which information systems used or operated by a contractor on behalf of the Department should be included in the IT inventory.

Recommendation 4: The Chief Information Officer should implement the parameters defined in the Federal Information Security Management Act for identifying all contractor systems that are to be included in the Department's information technology inventory.

[12] OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, December 17, 2004.
[13] Due to restricted time, OIG could not determine whether other systems exist that have not been accounted for in the Department's IT inventory.

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

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

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

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

Recommendation 5: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Risk Management

Ineffective Information Systems Security Officer Program

Each ISSO is tasked to monitor IT systems, report computer security issues, and educate their respective system users on best security practices and measures to help preserve data integrity, protect confidentiality, and ensure availability. As identified in the 2005 FISMA review, the Department needs to address issues regarding its ISSO program, including the lack of a formalized program plan.

OIG surveyed domestic and overseas ISSOs and program officials regarding the ISSO program and its effectiveness. From the total number of ISSOs (529), OIG received 161 responses. The responses (30 percent) identified the following chief issues:

- Difficulties performing duties - A significant number of respondents indicated difficulties in performing duties "due to insufficient time." The reason for this problem is that many are performing ISSO duties on a collateral basis with other job requirements. Sixty percent of respondents said they are only able to spend five or less hours per week performing ISSO duties due to other work commitments. OIG confirmed this situation during its recent inspections[14]. As a potential solution, the Department has discussed implementing full-time personnel (ISSO) at posts. Although OIG has not issued a recommendation on the matter, it encourages the Department to continue focusing on this proposal as a possible solution.

- Lack of a comprehensive training program – The number of personnel trained (to adequately perform their duties) and the types of training received varies by individual, which could result in inconsistent performance. Although many respondents stated they have received the Department-offered ISSO training, several stated they had not but were performing ISSO duties to the best of their ability.

- Need for uniform ISSO guidance – Respondents reported not receiving uniform guidance from Department officials. For example, some respondents mentioned that they use the Foreign Affairs Manual and Foreign Affairs Handbook as references, while others use checklists and post-issued policies. Some ISSOs said they have created their own guidance. Approximately 52 percent of respondents said they do not have adequate tools and framework to perform their required INFOSEC duties.

To improve the ISSO program, the Department has drafted an ISSO formalization project plan. In March 2006, a document highlighting several initiatives to improve the program was developed. These initiatives included (1) the development of a separate position description for the ISSO, (2) a proposed career path and skill code for the ISSO, (3) a prioritization of duties, (4) a matrix documenting training and certifications required, and, (5) the creation of regional ISSOs.

The Department also drafted a regional training program plan that outlines the responsibilities, training, and associated costs involved with creating regional ISSOs. The Department estimated the training program would consist of 23 weeks of classes with estimated costs per person of more than $36,000.

These personnel are a key component to the defense-in-depth approach of INFOSEC protection for the Department's cyber infrastructure. However, issues with the current program create a risk of not having this needed level of protection in place.

[14] *Office of Inspector General Summary of FY 2005 Information Systems Security Issues*, Report Number IT-I-06-01, May 2006

Recommendation 6: The Chief Information Officer should establish a comprehensive plan for the Information Systems Security Officer program that includes consistent prioritization of duties and training.

Inadequate Employee Information Technology Training Program

An effective training program for employees is vital to adequate maintenance of security for the Department's worldwide networks. In accordance with FISMA, OMB Circular A-130, and NIST guidelines, the CIO should establish a strategy for IT security awareness and training programs so that all personnel who possess significant INFOSEC responsibilities are trained. The Department has made progress in its training program via the formation of the Information Assurance Training Plan, renewed commitment for WebPass,[15] and a monthly newsletter sent to employees. However, concerns remain with certain aspects of the State Automated FISMA Information Reporting Environment (SAFIRE) application tool training. Further, there are concerns related to identifying the total number of Department employees required to take IT security awareness training.

The Department developed SAFIRE to serve as the central repository for agency plans of action and milestones data. As identified in OIG's 2004 and 2005 FISMA reports and in responses to its latest questionnaires, ISSOs and program officials noted that more than 67 percent of the respondents do not use SAFIRE for reporting purposes. Further, many questioned the purpose of the tool and the requirements for completion, as proposed by the Department. The remaining 33 percent who use SAFIRE responded with a poor rating of the tool's usefulness and the training offered. Currently, the Department is providing SAFIRE training via the Information Management Officer conference and online via IRM/IA's web site. However, the Department needs to increase its training and information distribution about SAFIRE if it plans to use SAFIRE as a management tool. Because the Department is making efforts to address the issues identified with SAFIRE, OIG is not making a recommendation at this time.

The Department also needs to determine the total number of employees who must take INFOSEC awareness training. All network users are required to complete annual security awareness training, but Department officials cannot identify the total number of Department employees who have done so. Therefore, it cannot confirm that all employees have completed training requirements. The Department uses a list generated from its online training course as a starting point. Program officials say there are a number of duplicate entries for individuals in the database since many employees rotate between posts. The Department has discussed other options for identifying the total number of Department employees who have taken the training, including using e-mail addressees. However, no plan of action has been issued to address the problem.

Recommendation 7: The Chief Information Officer should develop a process for determining an accurate representation of the total number of Department employees who have received required information security awareness training.

[15] A set of administrative applications that has received a development grant of approximately $500,000.

Cyber Incident Reporting Process

The process of effectively detecting, identifying, resolving, and/or preventing cyber-security incidents is critical to protecting mission critical data. FISMA and OMB Circular A-130 require that the Department maintain a formal incident response program for detecting and reporting security incidents.

Adequate policies and procedures for internal and external reporting of computer security incidents exist. Because the incident reporting procedures have become more mature, the annual number of reported cyber-security incidents increased significantly between 2003 and June 2006. The efforts to strategically locate network sensors have improved the Department's ability to effectively perform network security monitoring.

Other efforts to improve security monitoring of Department networks include expanding the Computer Incident Response Team's (CIRT) capability to 24 hours a day, seven days a week and increasing the vulnerability scanning and penetration testing initiatives. To assist with external incident reporting to law enforcement, the Department assigned a special agent to the CIRT staff to act as a direct liaison to external parties for reporting computer crimes. In 2005, the Department received an award for its efforts in cyber threat analysis and information assurance.

The number of reported incidents will likely start to decrease as the Department becomes even more adept at identifying and resolving real or actualized cyber threats, versus non-threats occurring in real time. Additionally, the Department is implementing a worldwide Cyber Security Incident Program (CSIP) as described in 12 FAM 590. The CSIP program is designed to enhance the protection of the Department's cyber infrastructure by identifying, evaluating, and assigning responsibility to employees who violate cyber security policy. CSIP is intended to focus personnel on their individual system security responsibilities, promote greater cyber security awareness, and deter unauthorized activity.

Progress in Privacy Efforts

The Department is making significant progress in addressing privacy requirements and is improving user awareness by such means as restricted use of Social Security numbers within official cable traffic and memoranda. Furthermore, the Department is developing a computer-based training program, similar to the cyber-security awareness training, which would require each employee have an annual employee refresher on his or her individual privacy responsibilities. Privacy representatives have been discussing a methodology that would require system owners to include privacy information for their respective applications and systems into SAFIRE. They are also requesting additional funds from the Department for increasing outreach and education activities for employees.

Certification and Accreditation Process

The Department is still hampered by a fragmented C&A process. In April 2003, DS and IRM undertook an 18-month pilot project designed to certify and accredit the Department's major applications and general support systems. The project was managed by the CISO and augmented with staff resources from DS. As of September 2004, the Department reported it has processed and approved 92 percent of the general support systems and major applications as part of the initiative. DS and IRM program officials also reported the project had moved the Department forward towards meeting FISMA requirements.

At the completion of the 18-month project, officials attempted to transition the pilot project into an agency-wide C&A program under which IRM and DS would jointly handle the C&A process. Under that program, IRM would be responsible for domestic sites and applications, and DS would be responsible for overseas sites. IRM and DS then presented the results and costs for coordinating and conducting this process to the respective bureau's executive office. A meeting was held with bureau executive offices, the CIO, and other officials to discuss the proposed costs. At the meeting, it was decided to conduct another pilot project, with bureaus performing their own C&A as a potential cost-effective way to perform C&A for the Department's INFOSEC systems and applications.

The pilot project was conducted with participation from the Bureaus of Consular Affairs, Administration, and DS and received IRM/IA's assistance. The pilot project's committee discussed ways to effectively manage the C&A program and improve its time and funding needs, including three low-risk systems with a timeframe of 30 days from start of the process to accreditation. As of May 2006, this pilot project was completed, and the committee considered it successful. The committee found several advantages in this option, including the need for less time to complete the C&A process, the ability to collaborate with risk management consultants sooner in the process, an increased focus on deadlines, and increased senior management attention to the process. The CIO approved the pilot project's continuation, with additional bureaus participating.

OIG has concerns with the current approach used by the Department to handle the C&A process. In addition to bureaus performing their own C&A of their respective systems, DS and IRM are also performing C&A on applications and systems, respectively. OIG believes the current fragmented C&A process does not enable the Department to adequately verify that all potential vulnerabilities are being addressed.

According to NIST SP 800-37, the Department should have an agency-level view of its INFOSEC program to facilitate the identification of common security controls that can be applied to one or more information systems. It would be more effective to have one entity with the ultimate C&A oversight responsibility, supported by the other bureau's capabilities. This would also reduce the risks inherent in the self-certification and accreditation process. Formal comments from the CIO state that this issue should be

closed. However, the various divisions currently performing C&A on Department systems prevent the CIO to effectively manage the C&A process.

Recommendation 8: The Chief Information Officer should assign one entity with responsibility to manage the certification and accreditation process.

Plan of Action and Milestone Process

The Department developed SAFIRE to serve as the central repository for agency POA&M data and improved the POA&M process by drafting a process guide for bureau officials and issuing scorecards quarterly to advise program officials of their compliance status with FISMA. However, the Department has not yet verified that IT security findings identified by all other sources are addressed through the POA&M process. Attention also should be placed on ensuring that bureaus and post personnel are using the process as an effective management tool.

IRM/IA is the central point for collecting, analyzing, managing, and reporting POA&M information to OMB. During this FISMA reporting year, IRM/IA drafted an updated POA&M process guide, intending to provide a comprehensive approach to the POA&M process. IRM/IA wanted to assist bureaus in the compilation and reporting of INFOSEC weaknesses in systems, programs, and sites. The document establishes POA&M criteria for the bureau and system owners and provides guidance and training information. According to the guide, bureaus would collect necessary information via the IRM/IA web site, monthly discussion groups, or from the designated IRM/IA representative for the respective bureau.

These are positive steps. However, the Department has not verified that IT security findings and recommendations from external and internal reviews are being addressed and resolved as part of the POA&M process. OIG reported on this issue in its FISMA 2004 and 2005 reports, and it remains an open issue. The updated POA&M guide does not provide details or instructions on addressing IT security vulnerabilities from all internal and external sources. As a result, the Department cannot demonstrate with certainty that all vulnerabilities, especially those that may affect the network infrastructure, are being addressed and resolved.

Recommendation 9: The Chief Information Officer should revise policies to ensure that information technology security findings and the recommendations from external and internal reviews are being addressed in the plans of action and milestones process.

Formal Recommendations

Recommendation 1: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 2: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 3: The Chief Information Officer should verify that all information technology assets for the Department are reported and accounted for within a comprehensive inventory process.

Recommendation 4: The Chief Information Officer should implement parameters (as defined in the Federal Information Security Management Act) to be used for identifying all contractor systems to be included in the Department's inventory.

Recommendation 5: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 6: The Chief Information Officer should establish a comprehensive plan for the Information Systems Security Officer program that includes consistent prioritization of duties and training.

Recommendation 7: The Chief Information Officer should develop a process for determining an accurate total number of Department employees for all employees required to take information security awareness training.

Recommendation 8: The Chief Information Officer should assign one entity with responsibility to manage the certification and accreditation process.

Recommendation 9: The Chief Information Officer should revise policies to ensure that information technology security findings and recommendations from external and internal reviews are being addressed in the plans of action and milestones process.

Abbreviations

C&A	Certification and accreditation
CIO	Chief Information Officer
CIRT	Cyber incident reporting team
CISO	Chief information security officer
CSIP	Cyber Security Incident Program
Department	Department of State
DS	Bureau of Diplomatic Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
INFOSEC	Information Security
IRM	Bureau of Information Resource Management
IRM/IA	Bureau of Information Resource Management, Office of Information Assurance
ISSO	Information systems security officer
IT	Information technology
ITAB	Information Technology Applications Base
L	Office of Legal Adviser
NIST	National Institutes of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of action and milestones
SAFIRE	State Automated FISMA Information Reporting Environment
SSPP	Systems Security Program Plan

APPENDIX A

Objectives, Scope, and Methodology

This review assessed the overall effectiveness of the Department's information management and INFOSEC programs. Specifically, the review evaluated the Department's information security roles and responsibilities, configuration management, cyber security incident reporting policies, INFOSEC awareness and training, certification and accreditation, and system inventory. The review also assessed how the agency implements patch management, Privacy Act requirements, and contractor systems oversight.

To meet its objectives, the OIG team researched federal laws, regulations and guidance to identify relevant criteria for implementing and managing information security programs. OIG then reviewed previous reports that evaluate the Department's INFOSEC program to identify previous issues and follow up on past recommendations. The OIG team also reviewed documents provided by Department officials, including but not limited to, corrective action plans, standard operating procedures, and process guides.

The OIG team met with officials from DS and IRM to discuss the Department's procedures for approving and overseeing contractor services, inventory, and facilities and implementing and managing INFOSEC awareness and training. The team attended working group meetings regularly with IRM/IA officials to obtain necessary information for completing the OMB FISMA report and OIG's independent evaluation report. In addition, the team selected a subjective sample[16] of the Department's systems to evaluate the certification and accreditation process and the application of its security configuration template.

OIG's Information Technology Office performed this evaluation from May 2006 through September 2006. (b) (6)(b) (6)(b) (6)(b) (6)(b) (6)(b) (6) (b) (6)(b) (6)(b) (6) Comments or questions about the report may be directed to Richard Saunders at saundersrs@state.gov or 703-284-2656. Comments or questions may also be directed to Vandana Patel at patelv@state.gov or 703-284-2647.

[16] The instructions on the OMB template direct all agencies to select a representative subset of systems to evaluate.

APPENDIX B

2004 & 2005 FISMA RECOMMENDATIONS CLOSED BASED ON REISSUANCE IN THIS REPORT

Appendix B lists recommendations from previous FISMA reports (2004 and 2005) that still require Department attention. As a result, they are being closed in previous FISMA reports and reissued in this report.

Review of the Information Security Program at the Department of State Memorandum Report, IT-A-04-08, September 2004

Recommendation 2: The Office of Information Assurance should develop procedures designed to facilitate that information technology security findings and recommendations from external and internal reviews are being addressed in the plans of action and milestones process.

Recommendation 4: The Bureau of Information Resource Management should review the applications and systems reported in the information technology application baseline and determine those to be included in the Department's inventory.

Recommendation 5: The Chief Information Officer should verify that all contractor services and facilities performing work for the Department are identified and are in accordance with established information security requirements.

Review of the Information Security Program at the Department of State Memorandum Report, IT-I-05-09, September 2005

Recommendation 2: The Chief Information Officer should include the requirement to develop a complete and accurate inventory of contractor systems and facilities into the Department's current corrective action plan for information security.

Recommendation 14: The Chief Information Officer should establish mandatory minimum requirements for information systems security officers.

APPENDIX C

OPEN RECOMMENDATIONS FROM 2004 & 2005 FISMA REVIEWS

Appendix C lists those recommendations that remain open from the 2004 and 2005 FISMA reports, and still require CIO's action for closing. The CIO agrees with these previously issued recommendations, and are working on its compliance.

Review of the Information Security Program at the Department of State Memorandum Report, IT-A-04-08, September 2004

Recommendation 1: The Office of Information Assurance and Critical Infrastructure Protection officials should conduct regular meetings to provide a forum for the sharing of information on information technology security vulnerabilities identified in Vulnerability Assessment Reports.

Recommendation 3: The Chief Information Officer should inform regional bureaus and overseas posts on the responsibilities for creating remediation for identified information technology security vulnerabilities and the type of information required for submission to the Department.

Recommendation 6: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 7: The Under Secretary for Management should direct that annual funding be established to meet the Department's full information technology certification and accreditation program requirements.

Recommendation 8: The Chief Information Officer should provide guidance and direct the appropriate bureaus to revise annually, or sooner if significant changes occur, the information security management and technical aspects of the relevant Foreign Affairs Manual and Foreign Affairs Handbook chapters and sections.

Review of the Information Security Program at the Department of State Memorandum Report, IT-I-05-09, September 2005

Recommendation 1: The Chief Information Officer should rewrite change control board procedures to require local change control boards to enter all application information into the Department's applications inventory system.

APPENDIX C (cont.)

Recommendation 3: The Chief Information Officer should require that all information systems policies and guidance use the same definition for the term system.

Recommendation 4: The Chief Information Officer should verify that the State Automated Federal Information Security Management Act Reporting Environment application is certified and accredited.

Recommendation 5: The Chief Information Officer should require that all system owners use the State Automated Federal Information Security Management Act Reporting Environment application and receive the requisite training.

Recommendation 6: The Chief Information Officer should disconnect networks that do not comply with the Department's patch management policies.

Recommendation 7: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2) .

Recommendation 8: The Chief Information Officer should require that a risk assessment be conducted on all subcomponents or a representative sample prior to reaccrediting the Department's unclassified and classified networks.

Recommendation 9: The Chief Information Officer should provide information security requirements that must be addressed during the regional computer security officers' site evaluation and verification visits.

Recommendation 10: The Chief Information Officer should enforce the requirement for penetration testing as part of the certification and accreditation process.

Recommendation 11: The Chief Information Officer should verify the accuracy of certification and accreditation information that is input into the information technology application baseline and the State Automated Federal Information Security Management Act Reporting Environment databases.

Recommendation 12: The Chief Information Officer should implement a process that requires all local administrators comply with the Department's security configuration guidelines, which includes requiring domestic system administrators to provide quarterly security configuration scan results.

APPENDIX C (cont.)

Recommendation 13: The Chief Information Officer should require that the Chief Information Security Officer be included in all operational decisions made in Washington that increase the risk to the Department's information security posture.

Recommendation 15: The Chief Information Officer should develop and implement procedures for enforcing the annual computer security awareness-training requirement.

Recommendation 16: The Chief Information Officer should identify which employees need training for key information security functions and design and deliver the necessary role-based training.

Recommendation 17: The Chief Information Officer should design and implement procedures for ensuring that the privacy impact assessment section in the Department's application inventory system is completed for all applications.

Recommendation 18: The Assistant Secretary for Administration (Senior Agency Official for Privacy), in coordination with the Chief Information Officer and the Office of the Legal Adviser, should update guidance on employee Privacy Act responsibilities.

APPENDIX D

DEPARTMENT COMMENTS

United States Department of State

Washington, D.C. 20520

September 18, 2006

MEMORANDUM

TO: OIG/IT – Richard Saunders, Director

FROM: IRM – Charles D. Wisecarver, Acting

SUBJECT: IRM Response to the Recommendations Made in the OIG Evaluation of the Information Security Program at the State Department

In accordance with the Federal Information Security Management Act (FISMA), IRM is providing as an attachment to this transmittal memoranda are formal comments for inclusion as an annex to OIG's Annual FISMA Review of the Information Security Program at the Department of State (Memorandum Report IT-06-03).

Attachment as stated.

FY2006 FORMAL RECOMMENDATIONS

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

Recommendation 3: *The Chief Information Officer should verify that all information technology assets for the Department are reported and accounted for within a comprehensive inventory process.*

The CIO agrees with this recommendation and believes this recommendation should be considered resolved. This past year, the CIO reassigned governance of the Department's IT systems and applications inventory (Information Technology Asset Baseline - ITAB) to the Enterprise Architecture and Planning office that handles eGovernment, and Capital Planning, strengthening the connections between these essential business processes. The new governance model for the ITAB is coordinating final definitions against the glossary of terms published after reaching consensus among the various agency components. Further, this process is ensuring a common baseline definition for all applicable definitions in Department-wide documentation and regulations. Once definitions are issued, the practical application of the definitions against existing and potential systems and applications will commence, ensuring more comprehensive and accurate reporting. The new governance structure is responsible for completing a review of how the ITAB is currently used, enhancing the understanding of user requirements.

Recommendation 4: *The Chief Information Officer should implement parameters (as defined in the Federal Information Security Management Act) to be used for identifying all contractor systems to be included in the Department's inventory.*

The CIO agrees with this recommendation. A Procurement Information Bulletin (Bulletin) entitled "Requirements for Contractor or Subcontractor Personnel Accessing Department Information Technology Systems" was issued this past year. The purpose of this Bulletin is to advise contracting personnel of information security requirements that apply to information technology resources or services in which the contractor has physical or electronic access to Department sensitive information that directly supports the mission of Department. An update to the Department of State Acquisition Regulations (DoSAR) relating to the same subject matter is to be prepared shortly.

In an effort to communicate the Department's strategic plan for capturing systems operated by contractors as defined by FISMA and clarified by Office of Management and Budget (OMB) guidance, *The Plan to Capture Contractor Systems in the Department of State's Inventory of Information Systems* was provided to the OIG and OMB. The plan consists of four sections with appendices that provide scope, roles and responsibilities, and point of contact, framework overview; quarterly milestones, and an implementation schedule. A Department wide data call was issued to identify all contractor connections, extensions and systems within the Department, as defined in the plan.

As part of its evolving Evaluation and Verification Program, the Department has been performing security configuration compliance scans on contractor connections to the Department's unclassified network. The results of these compliance scans are being shared with system owners for remediation of non-compliant systems. The results were also shared with Information Security Program elements that perform on-site reviews and inspections for contractor connectivity to the Department's OpenNet.

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

Recommendation 6: *The Chief Information Officer should establish a comprehensive plan for the Information Systems Security Officer program that includes consistent prioritization of duties, training, and job performance.*

The CISO developed a comprehensive "ISSO Formalization Project" that includes: a proposal for regionalizing the ISSO duties and responsibilities, provides a recommended functional position description, a prioritized listing of the duties and responsibilities broken down in accordance with NIST guidance (Management, Operational, Technical), an ISSO Training Plan, and recommended placement of regional assets (at large embassies and RIMCs). Under separate cover, the CISO proposed language changes to the 2880/2884 skill codes/standardized field position descriptions (SFPD) that reflect responsibility for implementation of the systems security plan. Lastly, the CISO is proposing implementation of a five-year plan of the Regional Information System Security Officer (RISSO) Program, inclusive of a request that 33% of the 56-positions (18) be provided the first year (FY2007), and the remaining 67% being spread out evenly over the remaining four years.

Full implementation of the regional program will meet the needs of both rightsizing and regionalization efforts within the Department, decrease the need for assigning the critical function of an ISSO as a collateral duty, and provide the opportunity for the Department to be proactive vice reactive to cyber security events, while improving the capability to react quickly and authoritatively when needed.

Recommendation 7: *The Chief Information Officer should develop a process for determining an accurate total number of Department employees for all employees required to take information security awareness training.*

The CIO agrees with this recommendation and considers it resolved. Below please find the methodology utilized by the Department to calculate the total number of employees (FTE, FSN's, badged contractors).

According to the Departments payroll records the total number of employees can be determined:

+ Total Number DoS Employees (From the CAPPS system 8/06)
+ Total Number of FSN's (Charleston Financial and Bangkok Financial System)
+ Department of State Contractors with active badges (DoS Badging Office)

= The total number of DoS Staff, including employees and contractors (Includes employees without access to DoS computer systems. The Bureau of Diplomatic Security, Office of Information Security provides annual generalized security awareness training to this group of Department employees.)

The total number of individuals that access the Department computer systems and thus require IT security awareness training can be determined through the Department of State IT Security Awareness training program. While some level of discretion remains with each Information Security Officer (ISSO) as to when a user's privileges are terminated for failure to timely complete the IT security awareness training, the Department is rapidly completing the necessary policy updates to remove all forms of ISSO discretion.

Recommendation 8: *The Chief Information Officer should assign one entity with responsibility to manage the certification and accreditation process.*

The CIO agrees and believes this recommendation should be closed. The office of Information Assurance's System's Authorization division is the only group in the Department of State charged with assuring a compliant Certification & Accreditation (C&A) program. Through a collaborative effort with DS and eGov, the Information Security Steering Committee (ISSC) has established stronger oversight of the information security governance process building upon the recommendations of the C&A Sub-working group that was charged with identifying and recommending policies and procedures that would allow for a more transparent, effective and cost sensitive approach to C&A.

The CISO is working on a Department-wide plan to provide enhanced security, while reducing the cost of C&A through the collaboration of all responsible Department entities. This new collaboration will include an increase in automation to reduce C&A costs including expansion of the current domestic and overseas scanning of the Department's authorization baseline.

Recommendation 9: *The Chief Information Officer should revise policies to ensure that information technology security findings and recommendations from external and internal reviews are being addressed in the plans of action and milestones process.*

The CIO agrees with this recommendation. Currently, the Office of Information Assurance has just over 100 auditor discovered findings stored and managed in the State Automated FISMA Information Reporting Environment (SAFIRE). To ensure that all possible weaknesses identified through internal Department processes are adequately reported, efforts were made to enlist the support of all Information Security Program components to assist in internal and external weakness identification. It is the Office of Information Assurance's intent to continue to place emphasis on the need to include all weakness, internal and external, identified including but not limited to: OIG reports, GAO audits, Evaluation and Verification (E&V) results into SAFIRE for POA&M remediation tracking. POA&M and SAFIRE data validation will become one of the CISO's primary areas of focus for FY2007. In the coming year, the CISO plans to take a more aggressive approach in ensuring that external weaknesses are reported and that milestones and timelines are adhered to. A "System Vulnerability Checklist" will be utilized to define for the system owner the specific areas where information security weaknesses are discovered and ask the system owner to indicate if each area has been acknowledged as part of their quarterly reporting responsibilities.