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-A-04-08, September 2004

~~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.~~

Section 3545 of the Federal Information Security Management Act of 2002 (FISMA)[1] directs each agency to conduct an annual independent evaluation of its information security program and practices. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information technology (IT) that support federal operations and assets, and it provides a mechanism for improved oversight of federal agency information security programs. Also, Office of Management and Budget (OMB) implementation guidance for FISMA requires the Office of Inspector General (OIG) to assess the development, implementation, and management of the agency-wide plans of action and milestones (POA&M) process and to focus on performance measures. In response, OIG performed an independent evaluation of the information security program and practices of the Department of State (Department).

The objective of this review was to assess the overall effectiveness of the Department's information security program. More details on the scope and methodology for this review are discussed in Appendix A. OIG received comments from the Department and incorporated them as appropriate within the body of the report. Comments from the Department are reprinted in Appendix B.

## RESULTS IN BRIEF

OIG found that the Department has taken a number of actions directed at improving the effectiveness of the Department's information security program since last year's independent evaluation. For example, the Department implemented a bureau-level Department FISMA scorecard. This performance scorecard, shared internally with senior management, is a one-page snapshot of a bureau's progress in information assurance. The Department has deployed an automated application tool to be used by the bureaus in an effort to automate the FISMA reporting process. The automated tool is designed to allow the Department to standardize web management of self-assessments, POA&Ms, and performance measures. Further, the Department developed a web-based training tool that is used to meet the requirement that all employees receive annual IT security awareness briefings. By using this web-based tool, the Department has the ability to track completion of annual awareness briefings electronically for each employee worldwide.

The Department has improved its POA&Ms process at headquarters since last year's evaluation. Restructuring of the certification and accreditation process, automation of FISMA data submissions, and the development of a draft POA&Ms process guide have been instrumental in helping the Department improve identification of its IT security vulnerabilities and address these issues through the POA&Ms process. In addition, the Department undertook an 18-month project to certify and accredit its major applications and general support systems. As of the first week in September, the Department had processed and approved 92 percent of the general support systems and major applications included in the project. The 18-month project has been coordinated with OMB, and has moved the Department constructively forward to begin meeting FISMA requirements in a key area where it previously had been failing.

[1] Pub. L. No. 107-347, Title III, Sec. 301(b)(1); 44 U.S.C. 3545.

However, OIG found several key areas that still require senior management attention. The Department has not adequately coordinated and shared information with relevant Department parties, such as Critical Infrastructure Protection (CIP) officials, involved in identifying and addressing IT security vulnerabilities for the POA&Ms process. At the time of this evaluation, the Department had not developed procedures to ensure that IT security findings were being addressed in the POA&Ms process nor had it extended the process to include its domestic and overseas sites.

Further, the Department inventory of IT systems remains incomplete and needs to be updated by the responsible Department officials, as required by FISMA. Whereas 92 percent of the general support systems and major applications included in the Department's 18-month systems authorization project completed certification and accreditation, the total universe of applications and systems for the Department has still not been identified fully. As a result, the percentage of systems and applications that have been certified and accredited for the Department are substantially less than the 92 percent reported for the project. Also, the Department lacks procedures to identify the number of contractor services or facilities performing work for the Department using their own systems or connecting to the Department networks. The Department's patch management program needs improvement. Patch management roles and responsibilities still remain unclear to post officials, and posts are unsure of the procedures for installing patches or obtaining assistance.

The Department continues to fragment responsibility for information systems security and to date has developed no effective coordinating or monitoring mechanism to ensure that delegated responsibilities are effectively accomplished. Further, the implementation of information security at overseas posts requires increased Department attention.

## BACKGROUND

Information security is imperative to any organization that depends on information systems and computer networks to carry out its mission. The expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way the government, private sector, and much of the world communicate and conduct business. However, without proper safeguards, these developments pose serious risks that make it easier for people and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer networks and systems. Further, the number of people with computer skills is increasing, and intrusion techniques and tools are readily available and relatively easy to use.

Faced with continued concerns about information security risks to the federal government, Congress passed and the President signed the FISMA into law in December 2002. The new law recognizes the highly networked nature of the current federal computing environment and provides for a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA requires agencies, at a minimum, to develop and maintain controls to protect federal information and information systems; improve oversight of federal agency information security programs; develop an agency-wide information security plan; incorporate information security principles and practices throughout the life cycles of the agency's information systems; and ensure that the information security plan is practiced throughout all life cycles of the agency's information systems.

FISMA also assigns the agency's Chief Information Officer (CIO) the authority and responsibility to administer key functions under the statute, including designating a senior agency information security official (CISO) who possesses professional qualifications and reports to the CIO and assists the CIO in developing and maintaining an agency-wide information security program; developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; training and overseeing personnel with significant responsibilities for information security; and assisting senior agency officials with their responsibilities.

Finally, in addition to a number of other provisions, FISMA requires each agency to have performed an independent evaluation of its information security program and practices. The OIG or the independent evaluator performing a review may use any audit, evaluation, or report relating to the effectiveness of the agency's information security program to do so. The agency is required to submit the independent evaluation, along with its own assessment, to OMB as part of its annual budget request.

## REVIEW FINDINGS

### Department's Progress in Addressing Information Security

#### Enhanced Performance Measures

Performance measures are a key requirement of FISMA. Since last year's evaluation, the Department has made significant progress in enhancing its process for developing performance measures. For example, the Department implemented a bureau-level Department FISMA scorecard. This performance scorecard, shared internally with senior management, is a one-page snapshot of a bureau's progress in information assurance. Ratings for performance measures are based on information provided by the bureaus on the POA&Ms process, certification and accreditation process, and training statistics.

The Department has deployed an automated application tool to be used by the bureaus in an effort to automate the FISMA reporting process. The tool, which is in the pilot stages, is a commercial product that the Department modified to fit the FISMA reporting needs. The tool is expected to be used by the Department by FY 2005. The automated tool will allow the Department to standardize web management of self-assessments, POA&Ms, and performance measures. Further, the tool will allow the Department to identify weaknesses and performance metrics, as well as generate FISMA and other legislative reports. These initiatives have addressed a previous OIG recommendation for establishing performance measures and linking them to the POA&Ms process.

## Effective Information Security Management Procedures

OIG selected five systems using a subjective sample to assess the Department's information security management procedures. The systems reviewed are used for system operations by various bureaus within the Department, including the Bureau of Administration's Employee Services Center (ESC), Bureau of Consular Affairs' Passport Information Electronic Records System (PIERS), Bureau of Diplomatic Security's (DS) Report Management Subsystem (RMS), Bureau of Human Resources' Global Employment Management System (GEMS), and Office of Medical Services' Electronic Medical Record (EMR). The OIG assessment pertained to management and operational controls and focused on security control reviews, personnel security, contingency planning, data integrity, security awareness, training, and education.

As shown in Table 1, the five systems have completed the certification and accreditation process. All five had a security-level determination, documented risk assessments, and tested security controls. Also, the selected systems had a security plan in place. For the certification and accreditation process, system owners complied with the Department's Systems Authorization Process Guide and System Authorization Plan, approved in May 2003 and March 2003, respectively. The guides provide information on the steps that should be taken by the system owners and the required documentation for a system to be granted accreditation.

**Table 1: Major Information Systems Results for Key System Security Elements**

| System | Risk Assessment | Security-Level Determined | Security Plans | Certified and Accredited | Tested Security Controls |
|---|---|---|---|---|---|
| ESC | Yes | Yes | Yes | Yes | Yes |
| PIERS | Yes | Yes | Yes | Yes | Yes |
| RMS | Yes | Yes | Yes | Yes | Yes |
| GEMS | Yes | Yes | Yes | Yes | Yes |
| EMR | Yes | Yes | Yes | Yes | Yes |

Further, Table 2 shows that all five systems have a trained information systems security officer (ISSO) assigned. A further analysis of the ISSO program is discussed later in the report. The systems also have documented IT system security self-assessments that were performed using the National Institutes of Standards and Technology (NIST) Special Publication 800-26 as criteria. The systems also had updated and tested contingency plans, which were completed as part of the certification and accreditation process.

**Table 2: Results for Training, Planning, and Self-Assessment Elements**

| System | Trained ISSO | Contingency Plans Developed, Tested, and Updated | Security Self-Assessments |
|---|---|---|---|
| ESC | Yes | Yes | Yes |
| PIERS | Yes | Yes | Yes |
| RMS | Yes | Yes | Yes |
| GEMS | Yes | Yes | Yes |
| EMR | Yes | Yes | Yes |

OIG's further review of each of these systems revealed the following.

### Employee Services Center

ESC, managed by the Bureau of Administration, is the primary check-in and checkout point for all transferring and in-transit Foreign Service officers and civil service employees on excursion tours. OIG found that the system received full accreditation to operate in March 2004 for 36 months. As part of the certification process, the bureau completed the system security plan and the contingency plan. The bureau completed the NIST self-assessment and the security controls for the system, and contingency plans were tested as the system went through the certification and accreditation process.

### Passport Information Electronic Records System

PIERS, within the Bureau of Consular Affairs, is an intranet-based interface for recording, tracking and managing the core data related to passport issuance. PIERS operates on the Department's OpenNet network and offers users from both domestic bureaus and the overseas posts the ability to query information pertaining to passports and vital records as well as to request original copies of the associated documents. PIERS users are able to create, amend, and print vital records. The systems provide both case-based and user-based views of information as well as support for electronic tracking and reporting of work processes.

The bureau completed a self-assessment on the system using NIST guidance and tested and evaluated the security controls. In addition, the system security and contingency plans for PIERS were updated and tested as part of the certification and accreditation process. The system received full accreditation to operate for 36 months in April 2004.

### Report Management Subsystem

RMS, managed by DS, is a comprehensive software suite that provides an efficient means for the bureau to conduct background investigations on individuals referred for security clearances and suitability reviews. DS conducted and documented a risk assessment and developed and tested a system security plan and contingency plan as part of the certification and accreditation process. DS also tested security controls. RMS received full accreditation to operate for 36 months in August 2003.

### Global Employment Management System

GEMS, managed by the Bureau of Human Resources, is the primary human resources application and centralized personnel database for managing the Department's human resources. The application is based on a suite of applications used for processing all Department employees' position management transactions. OIG found that the bureau completed the NIST self-assessment as the system went through the certification and accreditation process. In addition, the bureau updated and tested security and contingency plans. GEMS received full accreditation for only 18 months in December 2003 because it will be completing the certification and accreditation process once a system upgrade is completed.

### Electronic Medical Records

EMR, within the Office of Medical Services, establishes the essential medical record infrastructure that the Department must have to provide quality health care services for all U.S. foreign affairs agencies worldwide. The EMR provides a single authoritative source of information that is readily retrievable for patient care, medical evacuations and hospitalizations, medical clearance decisions, medical record release actions, and medical program planning and management. It provides a standard, rapid, and secure way to enter new medical record information into a Department patient's medical record.

OIG found that the bureau completed the NIST self-assessment as the system went through the certification and accreditation process. In addition, the application has updated and tested security and contingency plans. EMR received full accreditation for 18 months in March 2004 and will be recertified and accredited in 2005 after a planned upgrade is completed.

## Improved Security Awareness and Role-Based Training

The Department divides training into security awareness and role-based activities. Security awareness briefings help to ensure the confidentiality, integrity, and availability of Department information by guaranteeing that employees with access to information systems have been made aware of how to protect the Department's information. Role-based training is designed to provide specific training to employees that have been identified as having significant security responsibilities.

### Security Awareness Training

Since September 2003, the Department has made significant progress in ensuring that employees receive security awareness training domestically and overseas. The Department developed a web-based training tool that is used to meet the requirement that all employees receive annual IT security awareness briefings. With the approval of the Department CISO, elements of DS and Bureau of Information Resource Management Office of Information Assurance (IRM/IA) worked with the Office of Distance Learning at the Foreign Service Institute to take advantage of its distance learning system. By using this web-based tool, the Department has the ability to track completion of annual awareness briefings electronically for each employee worldwide. Training is tracked at every step from registration through presentation and assessment. The training record expires annually and must be renewed. As of the beginning of September 2004, more than 49,000 of the Department's 49,709 full-time employees, Foreign Service nationals, and contractors (approximately 99 percent) had taken the online security awareness training. The CISO, supported by CIO, has made annual awareness training mandatory and ensures integration of results into the annual FISMA report for the Department.

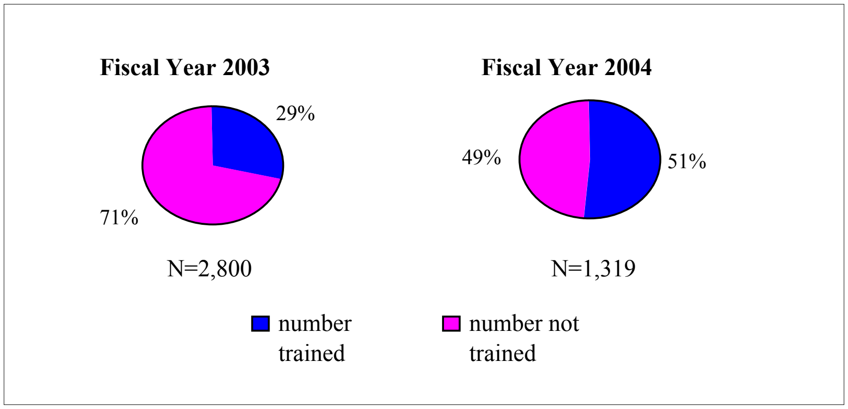
The Department's online security awareness briefings do not address peer-to-peer file-sharing policies as suggested by OMB. These policies are discussed with employees only during live security awareness briefings. The Department plans to include file-sharing policies, among other relevant policies, in future security awareness briefings.

### Role-Based Training

The Department has also made progress in ensuring that employees receive training based on their respective IT security roles. The DS training center has a total of seven automated information system security-related courses and is developing additional courses tailored for specific IT security responsibilities. The CISO approves training curricula for all IT security training courses. For example, a new training course is being developed for software application developers, and it is expected to be ready in FY 2005. Further, other proposed training courses for specific security responsibilities are in preliminary discussions with Department representatives.

The Department identified 1,319 employees with significant IT security responsibilities. Of the employees identified, approximately 51 percent, or 673 employees, had received specialized training. As illustrated in Figure 1, this is an increase from last year's reported numbers of 819 employees out of 2,800, approximately 29 percent, attending the courses.

**Figure 1: Role-Based Training Taken by Department IT Security Employees**



The decrease in the number of employees with significant IT security responsibilities in FY 2004 is attributed to the Department's reassessing job responsibilities for those employees reported in FY 2003. The Department credits enhanced reporting of performance measures, implementing the FISMA scorecard, and increasing awareness on training as reasons for the increase in role-based training attendance for this fiscal year.

# Improvements Needed in Addressing Information Security

## Plans of Action and Milestones Process Needs Improvement

The Department has improved its POA&Ms process since last year's evaluation. Restructuring of the certification and accreditation process, automation of FISMA data submissions, and the development of a draft POA&Ms process guide have been instrumental in helping the Department improve identification of its IT security vulnerabilities and address these issues through the POA&Ms process. In addition to these efforts, the Department must ensure better coordination and sharing of information with relevant Department components involved in identifying and addressing IT security vulnerabilities.

For example, IRM/IA serves as the central point for collecting, analyzing, managing, and reporting POA&Ms information to OMB. The current process for collecting POA&Ms data requires each bureau's program officials and system owners to identify all systems and programs for which they are responsible. These systems and programs are approved through the systems authorization process, which includes certification and accreditation. As part of the systems authorization process, bureau officials conduct self-assessments of their systems and programs to identify vulnerabilities, for which POA&Ms are created to remediate the weaknesses. Further, when IT security vulnerabilities are identified as a result of IRM/IA's verification during the certification and accreditation process, external and internal audits, evaluations and inspections, or CIP assessments, bureau officials are responsible for creating POA&Ms to mitigate the vulnerabilities.

In an effort to improve the process for creating, analyzing, and reporting POA&Ms information to IRM/IA and addressing FISMA reporting requirements, the Department developed a tool—State Automated FISMA Information Reporting Environment (SAFIRE) system. Bureau officials are currently using Excel Workbooks to create and submit their POA&Ms data to IRM/IA on a quarterly basis. With the SAFIRE system, bureau officials in FY 2005 will be able to create new POA&Ms and modify existing ones as needed. This process ensures that POA&Ms data are current and up-to-date. In addition, the SAFIRE system is connected to capital planning—exhibits 300 and 53 budget submissions—through a unique identifier. IRM/IA officials reported that having this identifier allows for the generation of reports to OMB that are indicative of how bureaus are performing. Officials in IRM/IA conducted workshops and also provided individual training for bureau officials at domestic locations on how to prepare POA&Ms in the Excel Workbooks, and relied on the regional bureaus to share training information with overseas staff. IRM/IA officials are currently training Department employees on the SAFIRE system and anticipate completing training by the first quarter of FY 2005, at which time the bureaus and posts will be required to use SAFIRE for data submissions.

Regardless of the efforts described above, the Department needs to ensure better coordination and sharing of information with relevant Department components involved in identifying and addressing IT security vulnerabilities. Specifically, CIP officials need better coordination and sharing of information with IRM/IA to report and track remediation of IT security vulnerabilities discovered during CIP assessments, i.e. Vulnerability Assessment

Reports. For example, CIP officials reported to OIG that they notify bureau officials of vulnerabilities found during assessments, but have only recently begun to share relevant IT security vulnerability findings with IRM/IA. As a result, the Department does not know if POA&Ms were generated to address all identified IT weaknesses.

OIG sent a questionnaire to bureau executive directors requesting information on creating POA&Ms based on external and internal audits, evaluations, and inspections. Results from the questionnaire and analysis of information provided by CIP indicate that no POA&Ms were created as a result of an IT security vulnerability identified by CIP officials during its last Vulnerability Assessment Report.

The Department needs to develop procedures to ensure that IT security findings and recommendations from external and internal reviews are being addressed in the POA&Ms process. Bureau representatives OIG spoke with were not aware of IT security vulnerabilities identified for their respective posts during OIG and Regional Computer Security Office inspections in FY 2004. Also, several bureau representatives responded that they were unaware of the type of information to be provided and the responsibilities of the bureaus and IRM officials in ensuring that POA&Ms, if needed, are being done.

> **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.

**Department Response:** The Department concurs with the recommendation. The Department's Cyber Security Program Management Plan will establish and implement an information governance structure that contains cross-bureau working-level teams called Information Security Integrated Teams composed of experts and supervisors in each of the main information security areas, including CIP.

**OIG Comments:** OIG accepts the Department's response and considers this recommendation resolved.

> **Recommendation 2:** The Office of Information Assurance should develop procedures 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.

**Department Response:** The Department concurs with the recommendation. The Department's Information Security Steering Committee will be charged with providing a comprehensive, collaborative information security management structure. In FY 2004, the Department focused primarily on the identification and remediation of security findings at the system level. Subsequently, the Department is developing a communication plan to inform program officials about what should be addressed in their respective POA&Ms. The scope would include any recommendations and guidance from recognized federal oversight entities, including OIG, GAO and OMB.

**OIG Comments:** OIG accepts the Department's response and considers this recommendation resolved. However, OIG reiterates that the communication plan to inform program officials of items to be addressed in their respective POA&Ms must include recommendations and guidance from GAO, OMB, OIG and other Department entities.

**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.

**Department Response:** The Department concurs with the recommendation. The Department's cyber security communication efforts are ongoing and will continue to include meetings, notices, memoranda, telegrams, and workshops.

**OIG Comments:** OIG accepts the Department's approach to address the recommendation, and considers this recommendation resolved.

## Inadequate Inventory of IT Systems

The Department has not adequately ensured that all IT systems have been identified and included in its inventory. FISMA requires that the CIO identify information systems that support the operations and assets of the Department. Using definitions provided by OMB, the Department identifies each system either as a major application, general support system, other application, or retired system. The Department has made progress in updating its inventory of applications and systems domestically. For example, the Department obtains information via funding or connection requests, during the certification and accreditation process, and from Information Technology Change Control Board requests. The Department has initiated site inspections overseas to update its inventory of applications and systems. At the time of this report, the Department had visited 59 overseas locations as part of its site authorization process. However, the Department has more than 290 overseas locations, all of which will not be covered during a single annual reporting period. As a result, the Department does not know the extent of its applications and systems. The Department is currently reviewing the site authorization process responsibility, which is explained later.

The Department needs to address the number of applications and systems reported in the IT Application Baseline (ITAB). ITAB officials are reporting almost 500 applications and systems in the Department, while IRM/IA in its systems authorization process reports over 170 applications and systems. The Department recognizes that the two reports of applications and systems need to be closer, and have begun to address this issue by conducting working group meetings. With representatives of IRM/IA and ITAB, the working group meetings are conducted to ensure that all applications and systems are being reported to the Department and being vetted through the certification and accreditation 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.

**Department Response:** The Department concurs with the recommendation. The ITAB partnership is led by IRM, and IRM offices make up the majority voting membership. The current information contained in ITAB is being scrubbed and validated by the data owners.

**OIG Comments:** OIG accepts the Department's response and considers this recommendation resolved. The recommendation will be closed when OIG receives the Department's inventory after its review of the applications and systems reported in the information technology application baseline.

## Inadequate Compliance and Identification of Contractor Facilities and Services

The CIO and Department program officials have not ensured that contractor-provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy, and NIST guidance. Although DS has approved 26 contractor services and facilities for connection to OpenNet Plus, the Department has not identified the full universe of contractor facilities and services and, thus, is not in compliance with FISMA requirements. OIG found that adequate processes and procedures have not been defined and implemented to verify whether those contractor facilities and services are being carried out securely. While the Department identified contractor organizations that are connected to the Department, further analysis needs to be done for those contractor facilities and services that use their own systems to perform work for the Department. The universe of contractor facilities and services is unknown and potentially significant in number. The CIO has the responsibility to identify information systems used or operated by a contractor for the Department, in accordance with FISMA, and therefore, this issue must be addressed.

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

**Department Response:** The Department concurs with the recommendation. The OIG, like IRM/IA and DS/SI are grappling with defining the implementation of this FISMA requirement. The three offices have agreed to continue meetings to determine an agreed course of action. In the interim, the Department has identified the number of contractor facilities and those facilities that exchange data with Department systems. Furthermore, the CISO has polled other agencies for their practices in this area.

**OIG Comments:** OIG accepts the Department’s response and considers this recommendation resolved. The OIG has an advisory role in assisting the Department in defining the implementation of this FISMA requirement, and the Department has the sole responsibility for ensuring that contractor services and facilities are properly being identified.

## Patch Management Needs Improvement

The Department’s patch management program needs improvement. Specifically, the Department’s delegation of patch management roles and responsibilities is unclear. Responsible officials within the Department are not certain who has the responsibility to enforce the installation of patches. Further, bureaus and overseas posts are not certain of the timeframe and importance for installing patches with different levels of criticality.

During inspections in FY 2004, OIG identified six locations where patch management was not performed adequately. Two inspections showed the posts did not document patch installations, and another post was not receiving notification from the Department of recently issued patches and was unaware of where to go within the Department to locate information. Another post was unaware of its responsibilities for patch management as outlined in the Enterprise Network Management (ENM) Patch Management Standard Operating Procedures, while another post was completely failing in implementing patch management procedures.

A review of helpdesk inquiries sent to the IRM Info Center illustrated inadequate patch management implementation. Of the recorded events that took place from May 2003 through May 2004, there were 18 requests to be added to the patch management notification list, eight incidents of incorrect installation of patches, and four requests for determining the location of recent patches. In 2004, in a selective sampling of the Regional Computer Security Officer reports on overseas posts, OIG found several cases in which necessary system patches were not installed. In each of these reports, DS officials recommended corrective action to prevent possible disruptions in post operations.

The Department's delegation of patch management roles and responsibilities are unclear. Specifically, it is unclear within the Department who has the responsibility to enforce installation of patches. OIG had discussions with Department officials and found confusion about which office was responsible for the enforcement of patch installations. ENM officials said that IRM/IA is responsible for enforcing the installation of patches, while IRM/IA disagreed and said ENM is responsible. Not installing patches appropriately places the Department at significant risk when hackers take advantage of known vulnerabilities. The Department must ensure that the relevant parties are performing their duties to prevent possible network vulnerabilities. Further, the Department needs to provide and communicate information on the importance of installing patches to overseas sites.

The Department needs to emphasize clearly the importance of each patch. Although the ENM web site does a relatively good job of defining the different risk levels associated with each patch as well as stating that each patch is mandatory, it does not state the timeframe within which sites must install each patch. During the FY 2004 inspection cycle, OIG found that information management staff or regional security officers who were performing ISSO duties were not installing those patches classified as low risk, but only installing high and critical patches. OIG also found that the number of patches being applied during calendar year 2004 was extremely low. Information contained in the daily Department Computer Incident Response Team briefing showed a low percentage of high- and medium-risk patches being applied. The percentage of affected machines that have had the patch applied ranged from as low as 19.05% and only as high as 45.55%. These statistics raise concern for several reasons. First, the due date for installation had passed for all eight patches that were classified as primarily high- and medium-level patches. Also, numerous machines were left vulnerable to threats that those patches would have addressed.

The Department has created a Statement of Procedures, which outlines a five-phase life-cycle process, including Discovery, Test, Delivery, Validation, and Compliance for the Patch Management Program as required by NIST 800-40 and 5 FAM 800. In the Discovery phase, the vendor announces update patches. The patch management office, in conjunction with the United States Computer Emergency Readiness Team (US-CERT) officials, analyzes the patch and determines the level of vulnerability and critical threat based on the Department's baseline. During the Test phase, ENM officials assign each patch a level of risk (i.e., critical, medium, low, or none) based on the level of impact it could have on the network and likelihood of occurrence. As part of the Delivery phase, officials post patches onto the Patch Management web site and send notifications to the IRM Info Center for action. The IRM Info Center distributes bulletins to the Department. Patches are then sent to bureaus and posts via the Systems Management Server (SMS) or compact disks. In the Validation phase, IRM uses SMS to identify successful and unsuccessful patch installations. Unsuccessful installations are reviewed by IRM officials to determine the cause. Finally, IRM/IA receives a copy of the validation report during the Compliance phase. However, no action is taken against posts that do not comply with Department procedures.

**Recommendation 6:** The Chief Information Officer should ensure that patch management roles and responsibilities are shared with relevant parties within the Department. The information should include responsibilities for installation and enforcement as well as the mandatory timeframe for the installation of patches.

**Department Response:** The Department concurs with the recommendation. The CIO has established ownership for the Patch Management Program through the ENM Office. This program directly addresses and should satisfy this recommendation with respect to a mandatory timeframe for the installation of patches. Under the direction of the CIO, the ENM Office will provide IRM/IA with patch installation reports on a continuous basis. IRM/IA will use these reports, together with other relevant information, to assess risk and monitor compliance. The CIO will continue to coordinate the definition and enforcement of roles and responsibilities for patch management between IRM/IA and ENM by updating 5 FAM and 12 FAM to delineate patch management roles and responsibilities and provide a methodology to address patch management noncompliance. In addition, ENM executed a service level agreement with Info Center to assist posts and bureaus with patch management responsibilities.

**OIG Comments:** OIG accepts the Department's response and considers this recommendation resolved. OIG believes that the Department must ensure clear dissemination of timeframes for the installation of patches because overseas posts are inconsistent in implementation even though the Patch Management Program has existed for some time.

## Roles and Responsibilities for Information Security Need Close Examination

The Department's management of information systems security contributes to its inability to meet all FISMA requirements because information system security roles and responsibilities are not sufficiently defined overseas and do not provide the necessary structure to meet information security responsibilities either domestically or overseas. Responding to identified management weaknesses in October 2003, the Department issued a memorandum outlining its revised information security roles and responsibilities and as of the beginning of September 2004, is again revising the matrix, assigning responsibilities to both IRM and DS. Specifically, IRM under the direction of the CIO, is assigned the responsibility to manage the Department's cyber security program, while DS is to handle physical security responsibilities. Under the proposed revision, IRM will remain the accrediting authority. DS will have the responsibility for addressing site certification of IT assets at all overseas sites, while IRM will address site certification of IT assets at domestic locations.

FISMA directs that the agency CIO has the responsibility to ensure compliance with information systems security requirements for the agency, including:

- designating a senior agency information security officer to carry out CIO responsibilities;
- developing and maintaining an agency-wide information security program;
- developing and maintaining information security policies, procedures, and controls to address all applicable requirements;
- training and overseeing personnel with significant responsibilities for information security; and
- assisting senior agency officials in their responsibilities as outlined in the act.

In April 2003, the Department undertook an 18-month project to certify and accredit its major applications and general support systems. The 18-month project managed by IRM/IA and augmented with staff resources from DS is scheduled for completion in September 2004, at which time it is to be rolled into an ongoing program to address systems authorization for all the Department's systems on a 3-year cyclical basis or upon significant change. As of the first week in September, the Department had processed and approved 164 of 179, or 92 percent of the general support systems and major applications included in the project. Before the project, when DS was responsible for certification and IRM was responsible for accreditation, as reported in FY 2002, the Department had processed and approved only 4 percent of its major applications and general support systems.[2] The 18-month project has been coordinated with OMB, and has moved the Department constructively forward to begin meeting FISMA requirements in a key area where it previously had been failing.

In a memorandum dated June 24, 2004, OIG informed DS and the CIO of our concerns with the division of responsibilities in the certification process as the Department moved forward with its system authorization program after the project. OIG strongly encouraged the Department to maintain its forward progress and momentum by reconsidering the decision to split the certification responsibility between DS and IRM. The Department's proposed revision of the roles and responsibilities splits the certification process: DS is responsible for site certification of IT assets and IRM/IA is responsible for systems certification and major processing center facilities. Based on the revised proposal, IRM/IA will retain the responsibility for accreditation and the overall authorization process; however, since the roles and responsibilities are being revised, the impact on the process remains to be determined.

The proposed division of responsibilities currently does not allow the CIO oversight of information system functions performed by DS personnel. For example, the October 2003 memorandum states that DS personnel are responsible for recommending and developing cyber security policy, creating and delivering cyber security training, and carrying out operational and tactical components of the Department's cyber security program. In response to the memorandum, DS established the Office of Security Integrity (DS/SI) to focus on cyber security issues. Currently the CIO cannot ensure that the information security responsibilities performed by DS are being conducted in an effective and efficient manner because although CIO coordinates with DS, neither CIO nor IRM activities have a mechanism to direct or measure what DS does to ensure information security. Similarly, under the newly proposed DS responsibilities, the CIO has no mechanism for ensuring that certification of IT assets at more than 200 foreign sites will be carried out in a manner to satisfy IRM/IA criteria.

OIG questions this reassignment and believes that the success of the 18-month project demonstrates it would be better for IRM/IA to be responsible for managing the certification and accreditation program for systems, applications, and sites. As noted earlier in this report, IRM/IA conducted 59 site visits in FY 2004 as part of a 3-year program to visit all sites and to establish a Department baseline for site certifications of IT assets to begin in 2007. This program was curtailed in August 2004 with the intent to pass the responsibility to DS. At the time of this report, no site certification visits for inspection of IT assets were occurring, and DS had not yet finalized a program plan for their conduct. Additionally, DS certification program managers reported that their direction was to develop the program so it relied on remote testing and collection of information as opposed to physically visiting the sites. Also, the DS program management was told that no additional funds were to be provided for conducting site certification visits.

[2] *Information Security Program Evaluation* ( IT/A-02-06, Sept. 2002).

OIG is concerned with this direction, and questions whether it will allow the Department to meet the objectives in its coordinated efforts with OMB to have in place a viable, forward-looking program ensuring that the necessary information security requirements are met. OIG believes the 18-month project and the temporary reassignment of resources to IRM for addressing the certification and accreditation backlog has proven to be effective. However, recent decisions by the CIO and DS call for a fragmentation of the process by returning overseas site certification of IT assets to DS. To split certification between two bureaus could very easily lead to ineffective performance and an inability to assign accountability and, as was the case 2 years ago, jeopardizes the Department's ability to meet FISMA requirements. The Department senior management in its decision on this issue has recognized the absence of performance requirements and the need for performance measures.

Further, the Department has not provided clear guidance to overseas posts nor ensured that the Foreign Affairs Manual (FAM) and Foreign Affairs Handbook (FAH) are up-to-date on posts' roles and responsibilities for meeting information security management requirements. For example, operations officers at the Regional Information Management Centers and the Regional Computer Security Office appear to perform similar functions in many instances. OIG inspections have shown numerous examples of the problems in differentiating the information systems security responsibilities of regional security officers and the information management officers, and in some instances, functions are not being performed at all.

IRM's proposed funding for its information assurance activities in FYs 2005 and 2006 does not fully support IRM/IA's proposed certification and accreditation program requirements. In accordance with FISMA and its implementing guidance, a viable program must include all systems and applications, not just those that are identified as general support systems and major applications. In order to meet the program requirements, the Department must include all of its systems and applications. As of the end of August 2004, the Department's universe of systems, major applications, and minor applications totaled almost 500. Although the Department showed significant progress with its 18-month project by authorizing processing for 163 general support systems and major applications, a viable program within the Department must address about three times that number for certification and accreditation.

At the beginning of September 2004, OIG found that the preliminary FY 2005 budget for IRM/IA did not include sufficient money to meet projected costs for operating the certification and accreditation program. While not yet finalized in early September for use in this report, the IRM funding proposal for all of IRM/IA's activities was approximately $12 million to cover both FYs 2005 and 2006. OIG anticipates this proposed funding level will not support the required certification and accreditation program as envisioned by IRM/IA or FISMA guidance. The proposed funding, when compared to IRM/IA's submitted budget request, is short by about $6 million in FY 2005 and $12 million in FY 2006. Also, the Department, under newly revised draft roles and responsibilities, has reassigned the responsibility for site certification of IT assets to DS, but as of the end of August 2004, the FY 2005 budget did not include enough money to fund site visits to certify IT assets.

In its response to a final draft of this report, the Department said the following:

> "We believe the structure and accountability systems are in place to meet FISMA certification and accreditation responsibilities through a shared CIO and DS approach. The CIO will articulate his certification and accreditation requirements and IRM and DS

> will execute their respective responsibilities... The Department agrees that the CIO is responsible for all certification and accreditation. DS has transferred to IRM complete functional responsibility and the associated resources for certification and accreditation of all major applications and general support systems. The CIO has requested and DS has agreed to perform site activities. Where appropriate, site visits will be conducted as part of a joint IRM and DS team. Although performed by DS, the site activities will fit into the overall authorization program run by IRM. The CIO will continue to have oversight authority over the DS contribution to certification and accreditation."

In the final draft report responded to by the Department, OIG included two recommendations directing that all functional activities and associated appropriations relating to the certification and accreditation process should remain permanently with the CIO. On the basis of the Department responses to the draft, we have chosen to withdraw those recommendations. OIG remains concerned as stated above, and we will continue to monitor as the Department moves forward on this initiative. OIG requests that the CIO keep us informed on its progress in developing certification performance requirements and criteria and further delineating the roles and responsibilities for information systems security. OIG will have the certification and accreditation process and roles and responsibilities of information systems security as a focal point for FY 2005 inspections and FISMA work that we will conduct.

**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.

**Department Response:** The Department concurs with the recommendation. IRM/IA is developing a detailed budget impact assessment that supports this recommendation. IRM/EX is working to increase proposed funding levels to ensure the IRM/IA program will not become noncompliant with the requisite authorities (FISMA, OMB and congressional scoring).

**OIG Comments:** OIG accepts the Department's response but considers it to be restrictive. If DS is to have responsibility for a portion of the certification program and process, then it must be included in and contribute to the detailed budget plans. This recommendation is unresolved.

**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.

**Department Response:** The Department concurs with the recommendation. Information Security Management is addressed in both the Foreign Affairs Manual (the requirements) and the Foreign Affairs Handbook. The CISO will continue to address and coordinate policy review and development activities with appropriate bureaus, in carrying out CIO-designated FISMA responsibilities. The same process applies to the update and review of information security procedures for the Foreign Affairs Handbook.

**OIG Comments:** OIG accepts the Department's response and considers this recommendation resolved.

## Information Security Management Deficiencies at Overseas Sites

OIG conducted information security inspections at 34 sites during FY 2004. OIG found numerous issues that should be addressed by the Department to ensure effective implementation of information security at overseas sites. Besides Patch Management Program deficiencies as described earlier, the Department's ISSO program was not meeting its objectives; several sites lacked required security documentation; inappropriate material was downloaded to post servers and users' computers; and Department configuration standards were not being met.

### ISSO Program Weaknesses

Designating information management and information systems staff as ISSOs must be managed diligently to maintain independent monitoring and checking of both systems management and operations. Recent efforts by the Department, such as sending cables to overseas posts outlining ISSO responsibilities, have been an improvement in the management of information security roles and responsibilities; however, more must be done. For example, at five sites visited, there was inadequate segregation between information management and information security duties and responsibilities. At one site, the ISSO is also the information systems officer and communications security (COMSEC) custodian. At another site, the information program specialist responsible for the classified system is also the ISSO for that system. In addition, one site's information management and information systems are generally effective, but lack independent oversight. The ISSO at this site oversees the administration of the bureau's unclassified and classified information systems, creating inadequate segregation of duties because the ISSO, who has systems administration responsibilities, also has security oversight authority for those systems.

Further, although much of the responsibility for securing information and IT system assets has been placed with the ISSO, in most instances these duties were assigned on a collateral basis and were not the primary duties of the individual designated as the ISSO. The collateral nature of these assignments reduces the time available to perform ISSO duties because the incumbents view them as secondary. For example, at one site, the ISSO performed responsibilities in conjunction with primary duties as a computer specialist and informed the inspection team that duties are not performed fully because both responsibilities were overwhelming. Further, at two sites, the ISSOs were not adequately performing their duties, such as documenting monthly and annual reviews of randomly selected libraries, reviews of user and system operational practice, and reviews of audit logs. One ISSO reported that there is no time to develop written procedures to instruct users to report incidents because of the multiple responsibilities as system administrator, COMSEC custodian, and ISSO.

In August 2003, the Department presented a recommendation for the CIO to institute a career field for cyber security practitioners. According to the Department, the recommended approach will leverage existing resources to maximum effect and provide a streamlined force to enhance compliance with federal mandates. As stated by the Department, regional security officers and security engineering officers readily acknowledge that ISSO duties do not fall within their core competencies. As a result, the work falls to the information management specialist, whose ISSO responsibilities are collateral to other assigned duties. The recommendation to the CIO included institutionalizing a skill matrix for the cyber security practitioners, developing an outreach program managed by a seasoned ISSO liaison, and establishing a cyber security skill code enabling growth opportunities throughout the information infrastructure.

At the time of this report, the Department issued a cable to posts reiterating the ISSO program responsibilities. The cable stated that posts should ensure that IRM staff are properly assigned ISSO responsibilities before nonregulatory functions are performed. In addition to the cable, the ISSO liaison office was established with responsibility to handle overseas and domestic monitoring issues. The ISSO liaison was in the process of developing a mailing list with all ISSOs to disseminate relevant ISSO information. The ISSO liaison office also ensured that it was included in all communications between the CIO and Computer Incident Response Team to be kept aware of any changes and issues affecting the ISSO program.

### Lack of Documentation

OIG found that overseas posts do not have the necessary systems documentation for their respective embassies. For example, two sites reviewed did not have a documented contingency plan for the automated information systems as required by 12 FAM 622.3 and 12 FAM 632.3. Further, five sites did not have an adequate site IT strategic plan that covers the embassy's operational, technical, and staffing needs as required by 5 FAM 121.1. Also, two sites did not have a life cycle plan for all IT equipment, nor did they have a bureau-specific IT budget plan that includes life cycle costs. Finally, six sites did not have a current, documented, and approved information system security program plan for their information systems in compliance with 12 FAM 632.4 and 12 FAM 622.4.

### Inappropriate Material on Networks

OIG found several instances of inappropriate material on embassy networks. For example, one site had several instances of inappropriate material on the servers. This included excessive personal use and storing of digital pictures, and downloading and using prohibited software. Further, at two sites, the inspection team found inappropriate material on individual systems. Information management staff was not ensuring and conducting periodic reviews of unclassified systems, checking for inappropriate material, such as executable files, pictures, and music files. As a result, systems could be vulnerable to viruses, which would greatly reduce the productivity and compromise system security.

### Configuration Issues

OIG found configuration issues at some sites visited during the inspection cycle. For example, one site was using naming conventions for its computers and servers that did not follow IRM's Standard for Network Naming and Addressing guidelines. Another site had incorrect documentation for local configuration control board decisions that did not comply with Department guidance on testing and evaluation reports. There was also no indication at this site that the local control board had reported all locally approved software to the Department. One site was using software that was not approved by the control board for installation and usage. In some instances, the Department software identified false positives.

# Recommendations

**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 2:** The Office of Information Assurance should develop procedures 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.

**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 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 ensure that all contractor services and facilities performing work for the Department are identified and are in accordance with established information security requirements.

**Recommendation 6:** The Chief Information Officer should ensure that patch management roles and responsibilities are shared with relevant parties within the Department. The information should include responsibilities for installation and enforcement as well as the mandatory timeframe for the installation of patches.

**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.

# Abbreviations

| | |
|---|---|
| CIO | Chief Information Officer |
| CIP | Critical Infrastructure Protection |
| CISO | Chief Information Security Officer |
| COMSEC | Communications security |
| Department | Department of State |
| DS | Diplomatic Security |
| EMR | Electronic Medical Record |
| ENM | Enterprise Network Management |
| ESC | Employee Services Center |
| FISMA | Federal Information Security Management Act |
| GEMS | Global Employment Management System |
| IRM/IA | Bureau of Information Resource Management, Office of Information Assurance |
| ISSO | Information Systems Security Officer |
| IT | Information technology |
| ITAB | IT Application Baseline |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PIERS | Passport Information Electronic Records System |
| POA&M | Plans of Action and Milestones |
| RMS | Report Management Subsystem |
| SAFIRE | State Automated FISMA Information Reporting Environment |
| SMS | Systems Management Server |
| US-CERT | United States Computer Emergency Readiness Team |

# Objectives, Scope, and Methodology

The objective of this review was to assess the overall effectiveness of the Department's information security program. Specifically, the review included identifying the total number of programs and systems in the agency; identifying and reporting material weaknesses in policies, procedures, or practices; and describing steps taken by the agency to implement and enforce the FISMA's CIO responsibilities and authorities. Also, the review included evaluating measures of performance; employee training; security incidents response; and development, implementation, and management of the agency-wide plans of action and milestones process. Further, the review included how the agency employs system configuration management and system security settings and maintains the Patch Management Program.

To meet its review objectives, OIG first researched U.S. laws and federal guidance to identify relevant criteria for implementing and managing information security programs. OIG then reviewed its own previous reports that evaluate the Department's information security program to identify previous issues requiring updating. OIG also reviewed documents provided from Department officials, including but not limited to, corrective action plans, standard operating procedures, process guides, and system authorization plans.

OIG met with officials from DS and IRM to discuss the Department's procedures for granting approval to contractor services or facilities, coordination and communication with CIP officials, and their assessment of the Department's implementing information system security roles and responsibilities. OIG also met with CIP and Computer Incident Response Team officials to obtain information about procedures for reporting security incidents and communicating with Department officials. OIG also attended working group meetings regularly with IRM/IA officials to obtain necessary information for completing the OMB FISMA report and OIG independent evaluation report. Meetings were conducted with Foreign Service Institute representatives to obtain information regarding the Department's training program. OIG also selected a subjective sample of the Department's systems to evaluate the certification and accreditation process. Further, OIG selected several reports of inspection conducted during FY 2004 to evaluate the Department's information security implementation, including the POA&Ms process. This included selecting IT security recommendations and speaking with bureau executive officials to determine what was done to address each IT security finding.

OIG's Information Technology Office performed this evaluation from March 2004 through September 2004. Contributors to this report were Lynn Allen, Mary Heard, James Davies, Vandana Patel, Pamela Young, and Brandon Carter. Comments or questions about the report can be directed to Mr. Lynn Allen at allenlx@state.gov or 703-284-2652, or to Mr. James Davies at daviesj@state.gov or (703) 284-2673.

Appendix B

## Department Comments

United States Department of State

*Washington, D.C. 20520*

SEP 2 1 2004

**INFORMATION MEMORANDUM**
UNCLASSIFIED

TO: OIG – Amb. Cameron Hume

FROM: CIO – Bruce Morrison BM
DS – Francis X. Taylor

SUBJECT: Formal Comments to the Office of Inspector General's Review of the Information Security Program at the Department of State

As requested, the Bureaus of Information Resource Management and Diplomatic Security are providing formal comments on the OIG's *Review of the Information Security Program at the Department of State*.

The OIG report provides welcome credit to the Department for its substantial progress in information security over the past year. While we understand that the OIG's role is to highlight areas of deficiency, this report forms the basis not only of the Congressional grading but also of the OMB Director's letter to the Secretary next spring approving or disapproving the Department's information security program. Therefore, a good balance between the accomplishments to date and the required future enhancements serve the Department appropriately.

Although the accomplishments of the Department's information security program, especially that of certifying and accrediting 92% of the general support systems and major applications, have been recognized by numerous outside entities, the opinions and assessments of the IG are highly valued. The praise and constructive tone reflected throughout the report is consistent with OMB's guidance to measure the "quality" of the agency's program.

The Bureaus of Information Resource Management and Diplomatic Security will address each of the issues identified in the report. In an effort to further and foster our working relationship, we second OMB's suggestion made in the 2004 FISMA guidance that "IGs should consider delivering interim reporting to agency officials..."

## Department Comments

### Responses to Recommendations of Office of Inspector General's Review of the Information Security Program at the Department of State

**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.

***Department Concurs with Response:***
*Homeland Security Presidential Directive 7, the primary CIP authority, requires "agency cyber security plans [as required by HSPD-7], be reviewed in a manner consistent with reviews of cyber security reports submitted under FISMA and current guidance."*

*In accordance with the Department's recently published Cyber Security Program Management Plan (CSPMP), the Department will establish and implement an information governance structure (Information Security Steering Committee) that contains cross-bureau working level teams called Information Security Integrated Teams composed of experts and supervisors in each of the main information security areas, including CIP.*

**Recommendation 2:** The Office of Information Assurance should develop procedures to ensure that information technology security findings and recommendations from external and internal reviews are being addressed in the Plan of Action and Milestone process.

***Department Concurs with Response:***
*The 2004 OMB FISMA guidance provides "an agency should develop a separate POA&M for every program and system for which weaknesses were identified in the FISMA reports, as well as those discovered during other reviews including GAO audits, financial system audits, and critical infrastructure vulnerability assessments."*

*In accordance with the Cyber Security Program Management Plan, the Department's Information Security Steering Committee will be charged with providing a comprehensive, collaborative information security management structure. In FY 2004, the Department focused primarily on the identification and remediation of security findings at the system level, in conjunction with the Systems Authorization Project. Subsequently, the Department is developing a communication plan to inform program officials about what should be addressed in their respective POA&Ms. The scope would include any recommendations and guidance from recognized federal oversight entities, including OIG, GAO and OMB.*

## Department Comments

**Recommendation 3:** The Office of Information Assurance 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.

***Department Concurs with Response:***
*FISMA assigns the responsibility of "assisting Department senior management with their information security responsibilities" to the CIO, delegated to the CISO.*

*The Undersecretary for Management in the fall of 2003 announced to all Undersecretaries and Assistant Secretaries the implementation of FISMA. This memo clearly outlines the annual requirements.*

*Throughout FY 2004, telegrams have been sent to the field announcing specific cyber security related actions necessary to promote good security practices. Specifically, three cables to the field address FISMA roles and responsibilities. In addition, during the Systems Authorization Project, the CISO met directly with bureau executive management to emphasize and promote necessary security practices. Cyber security communication efforts are ongoing and will continue to include meetings, notices, memoranda, telegrams, and workshops.*

**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.

***Department Concurs with Response:***
*FISMA requires "periodic testing and evaluation...of which testing shall include testing of management, operational, and technical controls of every information system identified in the inventory..."*

*The ITAB Partnership is led by IRM, and IRM Offices make-up the majority voting membership (IRM/OPS/SIO/API; IRM/BPC/CST; IRM/IA; IRM/EAP/AE). The current information contained in ITAB is being scrubbed and validated by the data owners and that effort directly addresses and should satisfy Recommendation 4 of the OIG Report IT-A-04-08.*

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

***Department Concurs with Response:***
*FISMA requires " information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source, that includes- subordinate plans for providing adequate information security for networks, facilities, and systems..."*

## Department Comments

*The OIG, like IRM/IA and DS/SI, are grappling with defining the implementation of this FISMA requirement. The three offices have agreed to continue meetings to determine an agreed course of action. In the interim, the Department has identified the number of contractor facilities and those facilities that exchange data with Department systems. Furthermore, the CISO has polled other agencies for their practices in this area.*

**Recommendation 6:** The Chief Information Officer should ensure that patch management roles and responsibilities are shared with relevant parties within the Department. The information should include responsibilities for installation and enforcement, as well as the mandatory timeframe for the installation of patches.

***Department Concurs with Response:***
*The Chief Information Officer has established ownership for the Patch Management Program through the Enterprise Network Management Office. The goal of the Patch Management program is to develop processes and procedures that leverage new and existing tools to mitigate vulnerabilities that have the potential to disrupt daily support operations. This program directly addresses and should satisfy this recommendation with respect to a mandatory timeframe for the installation of patches. Under the direction of the CIO, the ENM Office will provide IA with patch installation reports on a continuous basis. IA will use these reports, together with other relevant information, to assess risk and monitor compliance. The CIO will continue to internally coordinate the further definition and enforcement of roles and responsibilities between IA and ENM for Patch Management.*

*During FY 2004, we have endeavored to update the 5 FAM to delineate patch management roles and responsibilities. ENM has communicated this to the field by cable. ENM posts information to Department lists serves specifically for system administrators to facilitate communication regarding patch management issues to security practitioners. 12 FAM cyber security sanctions are currently in the clearance process and provide a methodology to address patch management non-compliance. In addition, ENM executed a Service Level Agreement with InfoCenter to assist posts and bureaus with patch management responsibilities.*

**Recommendation 7:** The Undersecretary for Management should direct that the certification and accreditation process, including all information technology-related site activities, should remain permanently with the CIO for compliance with the Federal Information Security Management Act as well as to ensure continuity of the certification and accreditation process.

**Recommendation 8:** The Undersecretary for Management should direct that in order to achieve greater efficiencies, all functional activities and associated appropriations relating to the certification and accreditation process should be transferred to the CIO.

***The Department non-concurs with Recommendations 7 & 8:***

## Department Comments

*We believe the structure and accountability systems are in place to meet FISMA C&A responsibilities through a shared CIO and DS approach. The CIO will articulate his C&A requirements and IA and SI will execute their respective responsibilities. The SI portion devolves to the CISO and the CIO, in turn. Both the DS A/S and CIO are accountable to the U/S for Management. We simply do not see the need for the changes recommended by the OIG.*

*The Department agrees that the CIO is responsible for all certification and accreditation. DS has transferred to IRM complete functional responsibility and the associated resources for C & A of all major applications and general support systems.*

*The CIO has requested and DS has agreed to perform site activities. Where appropriate, site visits will be conducted as part of a joint IA/SI team. Although performed by DS/SI/CS, the site activities will fit into the overall authorization program run by IA. The CIO will continue to have oversight authority over the DS contribution to C&A. The splitting of the certification responsibilities will satisfy the agency requirement to "centrally manage the development, implementation, and assessment of the security controls".*

*Therefore, we reluctantly non-concur with the above OIG recommendations as not necessary given the high level of collaboration between the Bureau of Information Resource Management and the Bureau of Diplomatic Security. FISMA defines the "what" not the "how."*

*The Under Secretary for Management and Chief Information Officer (CIO) both recognize the significant information security responsibilities the Assistant Secretary for Diplomatic Security (DS) has to the Secretary and the foreign affairs community as codified in the Omnibus Diplomatic Security Act of 1986. We recognize that some OIG's information security concerns have been long-standing and pre-date the current appointments of the CIO and DS A/S. Yet, under the direction of the Under Secretary, the commitment of these two leaders is directly related to the dramatic FISMA compliance reported by the OIG.*

*Much of the OIG rationale for its C&A recommendations is driven by a concern that the CIO does not have oversight and cannot direct DS resources. The CIO has successfully relied on DS for such FISMA mandated requirements as network monitoring and intrusion detection, role-based training, and cyber security awareness. The OIG evaluation is silent in recognizing the DS A/S's considerable responsibility to the foreign affairs community in developing information security standards through his chairmanship of the Overseas Policy Board. Nor, is there acknowledgement that many of DS' security responsibilities intersect with IT security – such as technical security countermeasures and counterintelligence. In other words, the CIO is already very reliant on DS to be able to fulfill his full information security mandate.*

## Department Comments

*There are other examples outside FISMA that reinforce how well IRM and DS collaborate in serving the Secretary and the Department. The CIO and DS A/S have committed resources toward a Global Situational Assurance Fusion Environment (G-SAFE). This is a DS and CIO shared vision to create continuous information security assurance than the current tri-annual C&A process offers. DS and IRM are collaborating on the development of remote evaluation tools to assess configuration, security integrity, patch management compliance and more. Respectfully, we believe a "fix" has been proposed where a problem doesn't exist.*

**Recommendation 9:** The Undersecretary for Management should direct that annual funding be established to meet the Department's full information technology certification and accreditation program requirements.

***Department Concurs with Response:***
*IRM/IA is developing a detailed budget impact assessment that supports this recommendation. IRM/EX is working to increase proposed funding levels to ensure the IA program will be not become non-compliant with the requisite authorities (FISMA, OMB and Congressional scoring).*

**Recommendation 10:** The Department's 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.

***Department Concurs with Response:***
*Information Security Management is addressed in both the Foreign Affairs Manual (the requirements) and the Foreign Affairs Handbook. The CISO will continue to address and coordinate policy review and development activities with appropriate bureaus, in carrying out CIO-designated FISMA responsibilities. The same process applies to the update and review of information security procedures for the Foreign Affairs Handbook.*

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

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

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

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