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-05-09, September 2005

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[2] 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 plan 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 and practices. 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's information security program and practices continue to evolve under the leadership of the Chief Information Officer (CIO). Also, the Department has taken several actions to improve the effectiveness of the Department's information security program since last year's independent evaluation. The Department is in the process of upgrading the information technology application baseline to strengthen the connections between enterprise architecture, e-Authentication, privacy, systems authorization, the POA&M process, and the capital planning process. All system owners and information system security officers (ISSO) will be required to use the Department's automated web-based tool to standardize management of self-assessments, POA&Ms, and performance measures for all data calls. The Department also ensures that all deficiencies are included in the POA&Ms. The Department's web-based training tool is used to ensure that all employees receive an annual information security awareness briefing.

Additionally, 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 has initiated a project to be completed within the next three years. The Department has taken a proactive approach to improve patch management operations and customer service. The Department continues to operate a successful and robust cyber incident response program.

---

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

[2] FISMA defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

However, OIG found several key areas that require senior management attention. The Department still does not have a complete inventory of systems that includes major applications, minor applications, and general support systems.[3] Also, IT security weaknesses found within a local area network are not included in the POA&M process because the Department does not consistently define a system throughout documentation and guidelines. OIG found several deficiencies in the patch management, configuration management, and the information systems security programs as well.

The Department's certification and accreditation process has not been fully implemented. All general support systems and major applications were certified and accredited during the 18-month special project. The next phase was to include the post operations, which most Department officials believe are the weakest link in the layered security approach that the Department has implemented. All aspects of this project have not been incorporated into the current evaluation and verification process, and the chief information security officer (CISO) has not provided formal guidance.

The separation of the cyber security roles and responsibilities continues to affect the Department's information security program. The August 2004 Cyber Security Roles and Responsibilities Matrix assigns to the Bureau of Diplomatic Security (DS) many operational responsibilities including the systems-related site evaluation and verification function. OIG found that the meetings between DS and the Bureau of Information Resource Management (IRM) do not result in clear statements of work, assignment of responsibilities, and establishment of milestones. As reported last year, the Department has no effective coordinating or monitoring mechanism to ensure that assigned responsibilities are accomplished. Furthermore, OIG noted areas for improvement in the Department's Privacy Act implementation.

Additionally, implementation of information security at overseas posts and domestic bureaus continues to require Department attention. OIG observed problems with ISSO duties, patch management, contingency planning, and inappropriate use at many of the 36 sites visited.

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

[3] The Department defines a general support system as an interconnected information resource under the same direct management control that shares common functionality.

systems. Furthermore, 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 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 the life cycles of the agency's information systems.

FISMA also assigns the agency's CIO the authority and responsibility to administer key functions under the statute, including designating a senior agency information security officer 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. 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.

Department's Progress in Addressing Information Security

Effective Information Security Management Procedures

To assess the Department's information management security practices, OIG used a subjective sample and selected four major application systems[4] (American Citizens Services (ACS), Baseline Tool Kit Back End (BTKBE), Passport Lookout Tracking System (PLOTS), and Telegram Web Portal (Webgram)) and two general support systems--Classified Network (ClassNet) and the Public Affairs Communicating Electronically (PACE) Network. The Bureau of Consular Affairs (CA) manages ACS and PLOTS; DS manages BTKBE; IRM manages Webgram and ClassNet; and the

[4] The Department defines a major application as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Bureau of Public Affairs (PA) manages PACE. OIG's assessment pertained to management and operational controls and focused on security control reviews, contingency planning, data integrity, security awareness, training, and education.

As shown in Table 1, all six systems have completed the certification and accreditation process and have documented risk assessments and security plans in place. Systems undergo security control testing during the system, testing, and evaluation phase of the certification and accreditation process, which is generally once every three years. The Department has implemented annual contingency plan testing. One-third of the systems (two of six) have had the impact levels determined. Two-thirds (four of six) systems have not complied with the FISMA requirement to test and evaluate security controls annually. Department officials plan to improve these areas in FY 06.

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

System	Risk Assessment	Security Level Determined	Security Plans	Certified and Accredited	Tested Security Controls (within the past year)	Impact Level Determined
ACS	Yes	Yes	Yes	Yes	No	No
BTKBE	Yes	Yes	Yes	Yes	No	No
ClassNet	Yes	Yes	Yes	Yes	No	Yes
PACE	Yes	Yes	Yes	Yes	Yes	Yes
PLOTS	Yes	Yes	Yes	Yes	No	No
Webgram	Yes	Yes	Yes	Yes	Yes	No

Table 2 shows that ACS, PLOTS, Webgram, PACE and ClassNet have trained ISSOs, but the BTKBE ISSO has not been trained. All of the reviewed systems have documented IT security self-assessments, which were performed using the National Institute of Standards and Technology (NIST) Special Publications 800-26 as criteria, and 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 Tested or Updated (within the past year)	Security Self Assessments
ACS	Yes	No	Yes
BTKBE	No	No	Yes
ClassNet	Yes	No	Yes
PACE	Yes	Yes	Yes
PLOTS	Yes	No	Yes
Webgram	Yes	Yes	Yes

OIG's review of these systems found the following.

American Citizens Services

CA manages ACS, an automated system designed to provide services to American citizens living and traveling abroad. The system received full accreditation to operate in July 2004. As part of the certification process, CA completed the system security plan and the contingency plan. Also, CA completed the NIST self-assessment, and security controls for the system and contingency plans were tested as the system went through certification and accreditation. The bureau has not tested and evaluated security controls and the contingency plan within the past year.

Baseline Tool Kit Back End

DS manages BTKBE, a web-based system that provides trend analysis and automated report generation of security assessments data. DS conducted and documented a risk assessment, and developed and tested a systems security plan and contingency plan as part of the certification and accreditation process. The BTKBE also went through security control testing. BTKBE received full accreditation to operate in August 2003.

BTKBE's primary ISSO has not attended the Department's Basic ISSO Training class. Also, DS has not tested and evaluated security controls and the contingency plan within the past year.

Classified Network

ClassNet, managed by IRM, is the global enterprise network that provides secure transportation of classified information at domestic and foreign sites. ClassNet transports information classified up to the Secret level in addition to classified and unclassified e-mail and cable traffic for about 220 posts and 17 domestic bureaus and offices.

IRM 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. ClassNet underwent system, test, and evaluation in accordance with the Department's System Authorization Process Guide. Because of the length of time since completion of the verification and penetration testing and in special consideration of the unquantified risk, ClassNet received full accreditation to operate for 18 months in August 2004.

Public Affairs Communicating Electronically Network

PA manages PACE, an unclassified, Internet access network that supports 325 users and seven remote locations. PACE, which is not connected to the Department's unclassified network (OpenNet), was created to meet the need for Internet access when this capability was absent at the departmental level. PA conducted and documented a risk assessment, and developed and tested security controls and contingency plan as part of the certification and accreditation process. PACE received full accreditation in January 2005.

Passport Lookout Tracking System

CA uses PLOTS to track passport fraud and issue a "lookout" case for questionable passport applications. A "lookout" case identifies that the application requires investigation. The system security and contingency plans for PLOTS were developed, updated, and tested as part of the certification and accreditation process. The system received full accreditation in March 2004. The bureau completed a self-assessment on the system using NIST guidance but has not tested and evaluated security controls and the contingency plan within the past year.

Telegram Web Portal

IRM manages Webgram, a web-enabled system developed for displaying unclassified and nonrestricted telegrams on the Department's Intranet. The system allows authorized users to retrieve their telegrams. OIG found that IRM completed the NIST self-assessment as the system went through the certification and accreditation process. In addition, IRM has developed, updated, and tested security and contingency plans. Webgram received full accreditation to operate in January 2005.

Compliance and Identification of Contractor Facilities and Services

The CIO and Department program officials have made progress in identifying and ensuring contractor facilities that support Department programs and services are adequately secure and meet FISMA, OMB policy, and NIST guidance. The Department is implementing a policy requiring all new contracts to adhere to FISMA guidelines. Contracts already awarded will be reviewed, inventoried, and evaluated to verify FISMA compliance. The Department estimates three years to develop the full universe of contractor facilities and services, and to determine the compliance with established information security requirements.

Plan of Action and Milestones Process

The Department made significant improvements in its POA&M process by developing an automated tool, State Automated FISMA Reporting Environment (SAFIRE), to ensure accurate submissions of POA&Ms, create computer-based training

on how to use the automated tool, and establish a formal domestic training program for system managers and other stakeholders.

The Office of Information Assurance (IRM/IA) is the central point for collecting, analyzing, managing, and reporting POA&Ms information to OMB and is responsible for certifying and accrediting all systems. Last year OIG recommended the Department develop procedures to ensure that the POA&M process addresses IT security findings and recommendations from external and internal reviews, and to inform regional bureaus and overseas posts on the responsibilities for remediating identified IT security vulnerabilities and submitting information to the Department. The Department developed SAFIRE, which serves as the central repository for POA&Ms data. IRM/IA has asked system owners to use the automated tool to report their POA&Ms. System owners[5] create POA&Ms when IT vulnerabilities are identified during the certification and accreditation process, annual self assessments, external and internal audits, evaluations, and inspections. OIG findings are also used to create a POA&M in SAFIRE.

In addition to the computer-based training on how to use SAFIRE, the Department increased awareness of stakeholders through workshops, individual bureau consultations, monthly bureau meetings, as well as information contained on the IRM/IA web-site and the POA&M process guide.

Patch Management

The Department's patch management program has taken several steps to improve operations and customer service. An independent consultant reviewed the patch management program and suggested improvements regarding deploying, automating test and evaluation, and upgrading the patch distribution tool. In addition, the Department's Office of Enterprise Network Management has made the patch management process more transparent by finalizing patch management standard operating procedures and a Microsoft Systems Management Server guide. Finally, to promote awareness of the program, the Office of Enterprise Network Management has provided several patch management briefings this year and ensured system administrator classes include patch management training.

Configuration Management

OIG's comparison of the Department configuration guides to the NIST configuration guidance found the Department guidelines meet or exceed NIST requirements. The Department's security configuration setting validation tool scans workstations and servers to compare the operating system settings to the security

[5] 5 Foreign Affairs Manual (FAM) 825 defines the system owner as the bureau designated senior executive who is responsible for the system. Abroad, the system owner is the chargé, deputy chief of mission, consul general, or principal officer or equivalent.

requirements and produces a report on the configuration status of each workstation and server.

Cyber Security Incident Response

The Department's cyber security incident response program is robust and efficient. There are basic policies and procedures in place and general awareness department-wide of how and to whom to report cyber incidents. The Department's Cyber Incident Response Team is the central reporting point for computer security events and incidents on the Department's information systems. The Cyber Incident Response Team effectively coordinates with appropriate parties to ensure all security-related incidents are detected, loss of data and/or resources is minimal, and all issues are resolved.

Awareness and Training

The Department's IT security awareness and role-based training program continues to improve. The Department added file sharing policies to the current curriculum in response to last year's OIG report. The Department also deployed and implemented an on-line computer-based training application for all computer users to conduct their annual computer security awareness briefing.

The Department's information assurance classes provide basic IT security training for eight roles. The classes are tailored for ISSOs, system administrators, managers, senior-level managers, executives, regional security officers, and security engineering officers.

Previously Identified Weaknesses Continue

Inadequate Inventory of IT Systems

The Department does not have a complete systems inventory that includes major applications, minor applications, and general support systems. Although 5 FAM 864 requires that all posts and bureaus enter custom-built applications into the Department's applications inventory system, not all bureaus and posts are aware of the applications inventory system and its purpose. For example, OIG identified over 20 applications created by three posts that should have been entered into the Department's applications inventory system. The Department cannot know the full universe of systems and applications until it ensures that all posts and bureaus enter their information into the applications inventory system.

The Department believed the full universe of applications and systems would be identified as part of its site inspections overseas. During FY 2005, the regional computer security officers visited 13 posts to perform an evaluation and verification review. The evaluation and verification process searches the posts' networks for unauthorized software, but does not include providing guidance on entering locally approved software applications into Department's applications inventory system.

The Information Technology Change Control Board standard operating procedures require that all applications be entered into the Department's applications inventory system prior to being added to the Department's baseline. The Department has not included this requirement in the local change control board procedures to ensure that all applications installed on the Department's infrastructure are reported.

> **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.

Department Response: "The CIO agrees with the recommendation. The Information Technology Asset Baseline (ITAB) partners will facilitate implementation. In the process, we will consider adding additional IT assets, including the overseas applications, contractor systems, and sites into ITAB. The ITAB changes underway must be completed before any other inventory types may be added. Because the asset inventory will expand significantly, the Department will follow a phased implementation process. The CIO is committed to resolving this recommendation and will provide a schedule with milestones by October 15."

OIG Comments: OIG considers the recommendation resolved.

Last year's FISMA report recognized a large discrepancy between the number of applications and systems reported in the Department's applications inventory system and the number reported in the Department's systems authorization process. OIG recommended that the Department review the applications and systems reported in the Department's applications inventory system and determine those to be included in the Department's inventory. The Department agreed with the recommendation, which will remain open until OIG receives the Department's inventory after a final comparison with the Department's applications inventory system.

Inadequate Identification of Contractor Facilities and Services

In last year's FISMA evaluation, OIG reported that the CIO should ensure that all contractor services and facilities are identified and in accordance with established information security requirements. The Department has a plan to address this deficiency within three years, and OIG believes that the Department should incorporate this requirement into the current corrective action plan for information systems security.

> **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.

Department Response: "The CIO agrees with the recommendation and will implement an inventory process in line with still-evolving NIST standards. Because of

unsettled policy and the overlapping and interwoven nature of contractor systems containing government information (e.g., contractors that deal with multiple government agencies), the Department's response and actions must be coordinated with other agencies and OMB. As noted in the OIG's recommendation, the Department's plan for addressing inventory, contract modifications and oversight is already being implemented. Language to address this issue from a contractual perspective is under development by representatives from across the Department. Upon completion of the new version of ITAB, central registration of contractor systems will be possible. *See also* response to recommendation # 1. The CIO is committed to resolving this recommendation and will add the requirement to the Federal Managers' Financial Integrity Act, Corrective Action Plan."

OIG Comments: OIG considers the recommendation resolved.

Plan of Action and Milestones Process Needs Improvement

All IT weaknesses are not included in the Department's POA&M process because the definition of a system remains unclear. The term "system" is used to describe major applications and general support systems in some Department processes; in other situations, a local area network is considered a system. IRM/IA's website states that system owners are responsible for developing and maintaining POA&Ms for their systems, recommending milestones and resource requirements, but because of these conflicting definitions, system owners are unsure of their responsibilities to report their POA&Ms. Some system owners included their networks in SAFIRE and many did not. Without consistent reporting of vulnerabilities, the Department cannot determine the magnitude of the risk and the extent of the remediation activities necessary.

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

Department Response: "The CIO agrees with the recommendation. The official Department definition of the term 'System' is found in 5 FAM 614: **System. A combination of hardware, software, facilities, personnel, data, and services to perform a designated function with specified results to user(s).** The 5 FAM will be rewritten to contain a separate section that consolidates all terms and definitions."

OIG Comments: OIG considers the recommendation resolved.

Data received from SAFIRE is incomplete because system owners are not reporting all the required information. OIG was told that some system owners are reluctant to enter in needed data because the tool has not been accredited. OIG inspections overseas have found that system owners have limited knowledge about SAFIRE.

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

Department Response: "The CIO agrees with the recommendation. The office that performs systems authorization is the owner of the application. Therefore, to avoid the potential conflict of interest, the Department hired an independent certification agent. The State Automated FISMA Reporting Environment (SAFIRE) application is in the Accreditation phase of the Systems Authorization Process. Remediation of the findings is complete and barring unforeseen circumstances, the CIO expects to authorize the system by the end of the fiscal year."

OIG Comments: OIG considers the recommendation resolved.

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.

Department Response: "The CIO agrees with the recommendation. This activity was not adequately funded in FY2005 due to budget constraints. The Department will add more resources to the SAFIRE project to increase SAFIRE visibility and strengthen the message that is already in place through additional training and advocacy. Furthermore, the SAFIRE team will continue to hold monthly meetings with the bureaus and continue to offer bureau assistance. In addition, presentations will be provided both domestically and overseas at conferences."

OIG Comments: OIG considers the recommendation resolved.

Patch Management Needs Improvement

The Department needs to correct deficiencies in patch reporting, enforce compliance with patch management,[6] and increase awareness of patch management and its responsibilities for nontechnical managers such as chiefs of mission, deputy chiefs of mission, management officers, and executive directors. The Department adheres to the NIST guidelines concerning patch management, with the exception of training administrators on vulnerability resources.

Last year, OIG found that patch management procedures were not being followed in six inspections and recommended that the CIO establish written guidance and procedures on what actions will be taken if overseas posts do not install the patches the

[6] Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches to a computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required.

Department releases. Despite these recommendations, patch management problems appear to have proliferated throughout the Department's posts. Twenty-one of 36 sites inspected were found to have patch management problems. For example, at 11 sites visited, OIG found that automated systems failed to accurately report the status of software security patch management thus providing an erroneous view of network vulnerabilities. OIG also found that not all required patches were installed in seven posts.

The monthly patch status report is an inaccurate representation of the Department's patch management status because the report does not include the ClassNet and the majority of domestic sites, as well as Microsoft Systems Management Server (SMS) inaccuracies that skew the results. Inaccurate reporting of workstations and incomplete distribution of patches remain a problem. SMS identifies the workstations and servers connected to the network and distributes the patches accordingly. Hardware, software, or configuration errors can prevent SMS from recognizing all workstations on the network. Local administrators must manually install patches on the workstations that SMS does not recognize. Last year OIG identified 11 posts where SMS inaccurately reported the patch management status to the Department. The Office of Enterprise Network Management plans to install SMS 2003 to eliminate this problem.

The Department does not verify or enforce patch management on ClassNet. ClassNet has no patch distribution tool, so local administrators must manually install patches on each workstation. The Office of Enterprise Network Management tracks compliance by e-mail. If local administrators fail to send the confirmation e-mail, the patch management group does not follow up to verify that the patches have been installed. This method leaves many workstations and servers potentially vulnerable to software security flaws. The Office of Enterprise Network Management plans to automate the patch installation and validation process this year.

Inadequate patch management continues to plague the Department and will continue to do so until patch management compliance is enforced. According to 5 FAM 866, the Designated Approval Authority may disconnect any network that does not meet the Department's patch management directives. OIG has no evidence of any post/bureau being disconnected from the Department's network because of patch noncompliance. Without enforcement, posts that are not in compliance can continue operating which leaves the unclassified and classified networks open to operational problems and malicious attacks.

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

Department Response: "The CIO agrees with the recommendation. This is supported by existing policy in 5 FAM 866.d that provides, "the Designated Approval Authority (DAA) may disconnect any system, LAN, or domain that does not comply with the Department's Enterprise Patch Management Program's directives." Furthermore, the Department must continue to balance acceptable risk against operational requirements for information and information systems services."

OIG Comments: OIG considers the recommendation resolved.

Nontechnical managers are not aware of the criticality of patch management. Because 5 FAM 825 states the system owner is responsible for the system, nontechnical managers should have a basic awareness of patch management. The Department needs to ensure that nontechnical managers understand their responsibilities as a system owner and how critical patch management is to the confidentiality, integrity, and availability of their network. Nontechnical managers should have a clear understanding of the patch management report.

The Department does not provide guidance to local administrators on how and where they can obtain data to identify vulnerabilities and corrective measures including patches for software outside the core baseline. NIST special publication 800-40 states that local administrators should be trained on identifying vulnerabilities and applicable patches. Providing local administrators with this information creates another line of defense in the patch management process.

> **Recommendation 7**: The Chief Information Officer should develop and implement a process for local administrators on identifying vulnerabilities and applicable patches for software not included in the core baseline as well as identifying additional government resources.

Department Response: "The CIO generally agrees with the recommendation, but notes the even greater potential to reduce vulnerabilities by remotely monitoring networks and administering patches from off-site locations, thereby reducing the burden on local administrators and improving overall network management. IRM senior management will coordinate and develop a process for oversight and compliance for other hardware / software applications or systems. The Local Change Control Boards (CCBs) report local post patch management activity and approval of IT items to their IT CCB Voting Representatives and the IT CCB Change Manager. This reporting mechanism provides information to the Patch Management Team for tracking."

OIG Comments: OIG considers the recommendation resolved.

Improvements Needed in Addressing Information Security

Certification and Accreditation Process – A Process in Flux

As the certification and accreditation process matures, needed improvements are identified: acceptable risk, penetration testing, and the accuracy of certification and accreditation data. The evaluation and verification process can provide valuable information to the Department by determining the vulnerability specific posts present, remediating the risks identified, and developing mandatory documentation.

The certification and accreditation process does not fully identify the risk that individual subcomponents or local area networks pose to the Department's infrastructure. The Department certified and accredited two general support systems, OpenNet and ClassNet, without determining all of the risks. OpenNet and ClassNet are distributed networks that make up a significant part of the Department's critical infrastructure. These systems are used by approximately 70,000 personnel worldwide and support numerous major and minor systems. The certification and accreditation packages for these general support systems state that a large portion of risk remains unquantified because of lack of resources, immaturity of the certification and accreditation process, and time constraints. Both systems received approval for 18 months and will be recertified in 2006.

> **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.

Department Response: "The CIO agrees with the recommendation. The Department performed risk assessments on the major components of OpenNet and ClassNet. For example, the Department performed a risk assessment of the software image of workstations deployed overseas through the type accreditation of GITM-U and GITM-C. The systems are currently undergoing the initial phases of re-accreditation and will undergo more rigorous testing and scrutiny than on the first pass."

OIG Comments: OIG considers the recommendation resolved.

The current evaluation and verification process does not meet the intent of the system authorization process. Major deliverables that were to result from the site certification process are not being produced such as security plans, contingency plans, and risk assessments. In accordance with the 2004 Cyber Security Roles and Responsibilities Matrix, DS conducts site verifications, which have replaced site authorizations. In last year's report, OIG expressed concerns with the division of responsibilities in the certification process between DS and IRM. OIG also believed that the proposed division of responsibilities did not allow the CIO oversight of information system functions performed by DS personnel. In its response, the Department stated that the shared CIO and DS approach would meet the Department's needs. OIG has found no evidence of the CIO setting performance requirements for the DS office that conducts system site evaluations and verifications.

> **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.

Department Response: "The CIO agrees with the recommendation. As a matter of clarification, the report's text should reflect the fact that the 2004 Roles and Responsibilities Matrix – developed jointly by the CIO and Assistant Secretary for DS - established the Evaluation and Verification (E&V) program, and assigned responsibility

for this program to DS. The E&V program will help the Department maintain a continuous monitoring capability in accordance with NIST guidance and in keeping with the Department's resource priorities as well as help support the Systems Authorization programs under CIO oversight.

With regard to E&V oversight, it is also important to note that DS and IRM/IA staffs are continuing to work closely to develop reporting procedures that will support the CIO in meeting FISMA responsibilities. Furthermore, DS and IRM/IA present joint quarterly briefings to the CIO and Assistant Secretary for DS detailing the progress of the E&V program.

Due to limited staff and funding availability to support the E&V process, the CISO's office was limited to setting direction and collaborating with DS to provide high-level guidance and a framework for the E&V process. The CIO, through the CISO, is acting on this recommendation by instituting a formal oversight role using performance measurements and metrics."

OIG Comments: OIG considers the recommendation resolved.

The Department has not performed penetration testing on all systems with high security levels. The Department has certified 42 systems that require such testing; 37 have not had penetration testing. The Department's System Authorization Plan states that all major systems and general support systems with a high security certification level must receive penetration testing. The CIO has delegated penetration testing to DS. In a memorandum dated January 5, 2004, DS stated that it was not feasible to perform penetration testing for all systems going through the certification and accreditation process. DS further asserted that penetration testing is labor-intensive, time-consuming, expensive, and potentially dangerous to an organization's network. DS recommended that the Department limit penetration testing to general support systems that support the major and minor applications and a small number of critical systems. In August 2005, the CIO provided DS a list of applications that must have penetration testing. The Department's overseas financial management feeder system has been certified for only 18 months rather than three years, because of no penetration testing.

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

Department Response: "The CIO agrees with the recommendation. Recently, NIST informed the Department that it intends to provide clarification on how to more effectively integrate penetration-test results of General Support Systems into the authorization of Major Applications. The formal outcome of NIST's guidance will provide the Department with critical information necessary to determine the mechanics, periodicity and linkage of penetration testing results into system authorization activities. Further, Department draft policy will be modified upon receipt of NIST's clarification.

The expected NIST clarification does not change the penetration testing requirements that the CIO identified and provided to the Bureau of Diplomatic Security. The testing and the periodicity specified in the CIO's directive is considered essential to the continued security health of the Department's networks and critical applications. The results of DS penetration testing will be reviewed as part of future systems authorization activities."

OIG Comments: OIG considers the recommendation resolved.

The certification and accreditation data in the Department's applications inventory system, and POA&Ms database, SAFIRE, is inaccurate. As of August 11, 2005, the Department had certified and accredited 32 applications and general support systems this fiscal year. In the Department's applications inventory system, there were 10 records with no contingency plan data, 17 records with no system security plan data, and six records were not entered. Of the 19 records in SAFIRE, OIG identified 15 with no certification and accreditation data, 15 with no contingency plan data, and 14 with no system security plan data. All certification and accreditation data in these databases should be consistent.

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.

Department Response: "The CIO agrees with the recommendation. The solution is the development and implementation of the data bridge between the Information Technology Asset Baseline (ITAB) and the State Automated FISMA Reporting Environment (SAFIRE). This bridge will align the data within the two tools and allow for easier and more accurate validation and verification, as well as offer a complete inventory of systems for the Department including C&A information associated with them. SAFIRE and ITAB will be feeding information to each other by 2nd quarter 2006."

OIG Comments: OIG considers the recommendation resolved. During this evaluation, the consistency of the data in the applications has improved significantly. As of September 21, 2005, in the Department's applications inventory system, there were four records with no certification and accreditation data, seven records with no contingency plan data, seven records with no system security plan data, and five records were not entered. Of the 22 records in SAFIRE, OIG identified two with no certification and accreditation data, two with no contingency plan data, and two with no system security plan data.

As discussed above, other weaknesses have surfaced in the Department's certification and accreditation process. The Department has not determined the security impact level of two-thirds of the systems in OIG's sample. The Department also has not established a process to ensure that security controls and contingency plans are tested

annually. Finally, the primary ISSO for a major application had not received the required information systems security training.

Configuration Management Needs To Be Worldwide

The Department does not require all administrators to comply with configuration management procedures. Nor does the Department have a process in place to ensure that the procedures are being followed. There is no reporting requirement for domestic networks so the Department does not know if all local administrators are following the required security configuration procedures. In May 2004, the Department required overseas local administrators to upload quarterly the verification tool results for DS analysis. OIG found that some posts did not conduct quarterly uploads or did not include a full scan of their unclassified networks. OIG believes that the Department needs to require all local administrators to provide quarterly scan results to DS. Furthermore, OIG found that the Department does not have processes in place to ensure that Oracle database and Cisco Internet Operating System security configuration procedures are being implemented.

Not following department configuration procedures puts the Department at an unnecessary risk. The Cyber Incident Response Team reports from November 2004 to June 2005 showed 22 instances of users on OpenNet connecting to remote workstations outside of the Department, such as their home or school computer. As the current Microsoft Windows XP configuration guidelines require that the remote services be disabled, these 22 events show that local administrators have not followed the required configuration security guidelines. A connection to a remote machine can bypass perimeter security processes and puts the Department at risk.

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

Department Response: "The CIO agrees with the recommendation, however, it should be noted except that the process may be done remotely or on-site. The Department is developing a process to improve compliance with security configuration guidelines. Improved reports include cumulative metrics used to facilitate CISO E&V process oversight and input into site visit selection. The ISSO program is supporting E&V by encouraging configuration scans and scheduling scanning tool training in the ISSO course."

OIG Comments: OIG considers the recommendation resolved.

Roles and Responsibilities for Information Security Need To Be Made Clearer

The integration of the cyber security roles and responsibilities between DS and IRM has not always been as effective as possible. Friction exists because the current

guidance does not clearly define functions, leaves room for misinterpretation of responsibilities, and causes omissions or duplications in several key information security activities.

In an April 2005 memorandum, the CIO assigned to the CISO, who is the director of IRM/IA, the following responsibilities:

- developing and maintaining an agency-wide information security program;
- coordinating the design and implementation of processes and practices that assess and quantify risks;
- developing and maintaining information security policies, procedures, and control techniques to address all applicable information security requirements;
- training and overseeing personnel with significant responsibilities and providing liaison with ISSOs domestically and overseas;
- advising and assisting Department senior management with their information security responsibilities; and
- reporting Department compliance with federal mandates to Department leadership, OMB, and Congress.

IRM/IA has not been fully integrated into many of the Department's ongoing IT initiatives – especially those that are operational such as standing up the embassy in Baghdad. IRM/IA was excluded from the decision process where risks were assessed and waiver decisions made to facilitate IT processing in Baghdad. Also, during a recent virus outbreak, the August 26, 2005 daily cyber security briefing report stated that mitigation and remediation actions continue between DS and its IRM security partners, which did not include IRM/IA. These actions by DS and its IRM security partners bypassed the coordinating and advising responsibilities of the CISO.

> **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.

Department Response: "The CIO agrees with the recommendation. To address the issues cited the CIO relies on the CISO in ensuring the security of the Department's information and information systems. During FY 2005, DS and IRM/IA staff in partnership with IRM/OPS shared information to resolve operational issues and address emerging policy challenges. The CIO will formally task all operational elements and all Department-wide security elements to include the CISO in all operational and policy decisions that may significantly impact the risk to the Department's information security posture.

We note that DS has continued to carry out its operational security duties in accordance with the Omnibus Diplomatic Security Act. These separate, but complementary, security responsibilities were documented and approved by the Under Secretary for Management in 2003 and subsequently updated in 2004."

OIG Comments: OIG considers this recommendation resolved.

The conflicting information in the FAM and the foreign affairs handbook (FAH) regarding each office and individual's role in cyber security further exacerbates a difficult situation. In last year's FISMA evaluation, OIG found that the Department had not provided clear guidance to posts including roles and responsibilities for meeting information security management requirements. OIG recommended that the CIO provide guidance and direct the appropriate bureaus to revise the relevant FAM and FAH chapters or sections annually, or sooner if significant changes occur. The cyber security roles and responsibilities matrix, which the Under Secretary for Management approved in August 2004, does not address any of the overseas or functional bureau participants in this process. The CIO has included updating the FAM and FAH to reflect the Department's information security policies and standards in the IRM corrective action plan with a milestone date of August 31, 2006, to complete this action.

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

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b)[(b) (2)] (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(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 14: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

[(b) (2)] (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Department Response: "The CIO agrees with the recommendation. The CISO's staff is working with the Bureau of Human Resources to professionalize the ISSO program. The initiative includes establishing mandatory minimum requirements for ISSOs by end of the calendar year."

OIG Comments: OIG considers this recommendation resolved.

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 four sites OIG inspected, the ISSOs or alternate ISSOs performed other responsibilities in conjunction with their primary duties and were overwhelmed by both responsibilities.

At nine sites visited by OIG, there was inadequate segregation between information management and information security duties and responsibilities. This lack of separation of duties led to several weaknesses in the implementation of the Department's information systems security program. These weaknesses included compromised access to classified and sensitive but unclassified information and inadequate reviews of user directories, system audit logs, and network reviews for inappropriate or excessive personal use of government equipment. Furthermore, some ISSOs did not review systems operations and systems maintenance logs and conduct quarterly network scans. At another site, OIG observed difficulties in revoking access privileges for personnel leaving the mission and a high number of staff with administrative rights to unclassified information systems.

Awareness and Training Programs Need Additional Work

Although all Department network users are required to complete annual security awareness training to ensure the confidentiality, integrity, and availability of information, there are no procedures in place to ensure a user completes the awareness training annually. The role-based IT security training program needs to include the increasing responsibilities of employees with significant IT security responsibilities.

All Department employees have not completed the annual awareness training because there is no enforcement method such as requiring training prior to receiving or keeping logon access. The Department has over 70,000[8] employees, which includes full-time employees, Foreign Service nationals, and domestic contractors. OIG found that 46,430 computer users have valid certificates, 647 have incomplete certificates, and 23,567 have expired certificates as of August 16, 2005. Incomplete and expired

[8] The number of employees is based on the Bureau of Human Resources number of 57,062 employees overseas and domestic as of June 30, 2005, and 13,871 active contractor badges reported by DS as of August 23, 2005. This number includes an estimated number of domestic contractors and thus is different from the number reported in last year's FISMA report.

certificates may be for users who have left the Department or have not completed the on-line test to satisfy the training requirement. Regardless, only 46,430 users have up-to-date awareness training, which is less than 70 percent of the approximate number of Department employees.

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

Department Response: "The CIO agrees with the recommendation. In FY2005, the Department implemented procedures that both encourage system users to take the annual computer security awareness training and provides for enforcement. All parties desiring access to the Department's primary network, OpenNet, must first complete an online training session and test. An annual training session and test is required for continued system access. Enforcement of this policy is delegated to local ISSOs and effectiveness will be monitored by the CISO's office. Should enforcement prove insufficient, the CISO will develop mitigating controls to improve performance."

OIG Comment: OIG considers this recommendation resolved.

The Department has not fully identified which employees have significant IT security responsibilities. NIST 800-16 identifies 26 functions to be considered when developing an IT security training program including software developers, project managers, and contracting officers. The Department was planning to create a course for software developers by FY 2005. This information assurance course and curriculum for software developers is still in the preliminary approval stage.

> **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.

Department Response: "The CIO agrees with the recommendation with comment. Since 2001, the Department has taken steps to identify employees with significant IT security responsibilities. These efforts are now documented in the Information Assurance Training Plan. This plan identifies required security training for specific information assurance roles relevant to the Department. It is a living document and is reviewed each year to evaluate resources, priorities, and timelines. As additional roles are added, additional resources will be required to design and deliver additional role-based training.

Also, the report should note that the Department has, in accordance with NIST SP 800-16, identified 13 specific roles, the target audience for those roles, and the training courses available to meet the IA training requirements. This information is documented in the "FY05 Information Assurance Training Plan." Moreover, many of the 26 roles in SP 800-16 have been incorporated into the Department's set of 13 specific roles. As a result, resources are focused on meeting the largest percentage of significant employees

with IT security responsibilities, specifically the Information Systems Security Officers (ISSOs), Technical Security Personnel at three levels, IT Managers, Senior-level Managers, Executives, Special Agents, Security Engineers, and OIG Auditors."

OIG Comment: OIG reviewed the "FY 05 Information Assurance Training Plan" and considers this recommendation closed upon issuance of this report.

Privacy Act Requirements Are Not Addressed

Additional opportunities exist to improve the Department's information privacy activities. Specifically, OIG found weaknesses in the Privacy Act implementation in the certification and accreditation of systems, inadequate communication on privacy act training for new employees, and lack of information privacy act awareness throughout the Department.

The Department is not consistently capturing information system privacy act requirements in the Department's information technology applications baseline, the central database of all Department systems. Section 208 of the E-Government Act (Public Law 107-347, 44 U.S.C. Ch 36) requires that systems that collect, maintain, or disseminate information in identifiable form have privacy impact assessments when developing or procuring IT systems or projects. These assessments determine whether an IT system has adequate built-in protections to ensure the privacy and handling of personal information. Furthermore, the privacy impact assessment evaluates the risks and effects of collecting, maintaining, and disseminating electronic personal information. Privacy impact assessments are updated as necessary when a system change creates new privacy risks or when new uses of an existing IT system significantly change how information in identifiable form is managed in the system. Privacy impact assessment information is not mandatory in the Department's applications inventory system. OIG found many web-based applications that request and capture users' social security numbers, which have not been entered into the Department's applications inventory system. Therefore, the Department does not have an accurate representation of all applications that contain Privacy Act information and the resultant controls that must be implemented.

> **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.

Department Response: "The CIO agrees with the recommendation. The Department's new registration process for Information Technology Asset Baseline (ITAB) will incorporate mandatory privacy reporting into the Department's application registration process. Specifically, system owners will be required to file all appropriate documentation with the Bureau of Administration's Senior Agency Official for Privacy for any information category that falls within the scope of a privacy impact assessment. The system authorization process serves as an additional verification that the applicable

documentation is both complete and accurate and the commensurate security controls are tested."

OIG Comment: OIG considers this recommendation resolved.

The Department does not provide standard Privacy Act training nor does it have a Privacy Act awareness campaign for the Department workforce. OMB M-05-08 states the senior agency official shall ensure the agency's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures that govern the agency's handling of personal information.

The Department's privacy office assumed a Privacy Act overview is conducted during the orientation session; however, OIG found such information is not provided during the DS review of the protection of classified information. The Department conducts weekly information management officer training that covers the Privacy Act but there is little to no information privacy awareness training for the remainder of the Department.

The Department has not developed guidance on Privacy Act information issues nor on how or where to obtain Departmental Privacy Act assistance. The Department Notice on employee roles and responsibilities when dealing with privacy information is dated September 1993.

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

Department Response: "The Assistant Secretary for Administration (Senior Agency Official for Privacy) agrees (and the CIO concurs) with the recommendation, which should be redirected to the Assistant Secretary for Administration. Numerous efforts are underway that address the need to raise employee awareness of protecting privacy information. A Department-wide training program for employees and contractors is under development. Recently, the Office of Information Programs and Services delivered a three-day course to those employees responsible for processing Freedom of Information Act and Privacy Act requests from the public.

A Department notice informing employees of their roles and responsibilities with regard to the Privacy Act and handling of personal information is in clearance.

The Department set-up an e-mail address, Privacy-DL@state.gov **mailto:Privacy-DL@state.gov**>, for employees to ask privacy-related questions.

The Department has trained IT systems managers on completing Privacy Impact Assessments required by Section 208, Privacy Provisions of the E-Government of 2002.

Part of that training included detailed guidance on their responsibilities under the Privacy Act and the handling of personal information."

OIG Comment: OIG considers this recommendation resolved.

Additional Information Security Management Deficiencies Identified by OIG Inspections

OIG conducted information security inspections at 36 sites during FY 2005. OIG found numerous issues that should be addressed by the Department to ensure effective implementation of information security at sites. Besides patch management and ISSO program deficiencies described earlier, several sites lacked required contingency plans and documentation, inappropriate material was downloaded to post servers and users' computers, and the Department policy regarding inappropriate use of government equipment was not being followed. The details of these deficiencies and recommendations have been addressed in individual inspection reports.

Patch Management

Flaws are identified in software in use that leaves it vulnerable to outside sources of disruption. Patches are released to fix these flaws, protecting software from such vulnerabilities, and are an integral part of information systems security. Patches are necessary to protect software from intrusion or attack. A lack of up-to-date patches places not only embassies but also the entire Department's network at risk.

Contingency Planning

OIG found that several overseas posts do not have the required contingency plans for their respective embassies. To assist Department compliance with these documents, IRM has comprehensive automated templates for developing system specific contingency plans for classified and unclassified information technology systems.

Inappropriate Material on Networks

OIG found several instances of inappropriate material on embassy networks. For example, nine sites had inappropriate material on the servers that included nonwork related video and audio files, prohibited software. As a result, systems could be vulnerable to viruses, which would greatly reduce the productivity and compromise system security.

Recommendations

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.

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 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 ensure 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: The Chief Information Officer should develop and implement a process for local administrators on identifying vulnerabilities and applicable patches for software not included in the core baseline as well as identifying additional government resources.

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 ensures all local administrators comply with the Department's security configuration guidelines, which includes requiring domestic system administrators to provide quarterly security configuration scan results.

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 14: (b) (2)(b) (2)(b) (2)(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 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 CIO and the Office of the Legal Adviser, should update guidance on employee Privacy Act responsibilities.

Abbreviations

ACS	American Citizens Services
BTKBE	Baseline Tool Kit Back End
CA	Bureau of Consular Affairs
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ClassNet	Classified network
Department	Department of State
DS	Bureau of Diplomatic Security
FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IRM	Bureau of Information Resource Management
IRM/IA	Office of Information Assurance
ISSO	Information systems security officer
IT	Information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OpenNet	Unclassified network
PA	Bureau of Public Affairs
PACE	Public Affairs Communicating Electronically
PLOTS	Passport Lookout Tracking System
POA&M	Plan of action and milestones
SAFIRE	State Automated FISMA Reporting Environment
SMS	System Management Server
Webgram	Telegram Web Portal

Appendix A

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 evaluating the Department's information security roles and responsibilities, configuration management, cyber security incident reporting policies, information security awareness and training, certification and accreditation, and system inventory. Further, the review included how the agency implements patch management, the role of the Privacy Act official in IT security, and contractor systems oversight.

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 previous reports that evaluate the Department's information security program to identify previous issues and follow up on past recommendations. OIG also reviewed documents provided by Department officials, including but not limited to, corrective action plans, standard operating procedures, and process guides.

OIG met with officials from DS and IRM to discuss the Department's procedures for granting approval and providing oversight to contractor services, inventory, and facilities; and implementing and managing information security awareness and training. 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. OIG also selected a subjective sample 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 June 2005 through September 2005. Contributors to this report were Mary Heard, Jennifer Noisette, Michelle Wood, Olukemi Adebiyi, and Jonathan Tull. Comments or questions about the report can be directed to Ms. Mary Heard at Heardm@state.gov on 703-284-2656 or Jennifer Noisette at Noisettejm @state.gov on 703-284-2641.

Appendix B

Department Response

United States Department of State

Washington, D.C. 20520

September 22, 2005

UNCLASSIFIED

INFORMATION MEMO FOR INSPECTOR GENERAL KRONGARD – OIG

FROM: IRM – Jay N. Anania, Acting

SUBJECT: Department of State Response to the OIG Report entitled *Review of Information Security Program at the Department of State.*

I appreciate the opportunity to review and comment on the memorandum report, *Review of the Information Security Program at the Department of State*, IT-I-0509. Please find attached the Department's response to the recommendations provided in the memorandum report.

Attachment:
As stated.

Appendix B

Department Response

Drafted by: IRM/IA: E Caffrey
09/22/2005 ext. 2-2424
Clearances:
A/RPS – L. Lohman
DS/SI - D. Reid
IRM/BPC - C. Liu
IRM/EX - T. Williamson
IRM/OPS – S. Musser
IRM/IA – J.S. Norris

Appendix B

Department Response

Department of State Response
to the
OIG Memorandum Report IT-I-0509
Review of the Information Security Program at the Department of State

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.

The CIO agrees with the recommendation. The Information Technology Asset Baseline (ITAB) partners will facilitate implementation. In the process, we will consider adding additional IT assets, including the overseas applications, contractor systems, and sites into ITAB. The ITAB changes underway must be completed before any other inventory types may be added. Because the asset inventory will expand significantly, the Department will follow a phased implementation process. The CIO is committed to resolving this recommendation and will provide a schedule with milestones by October 15.

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 systems security.

The CIO agrees with the recommendation and will implement an inventory process in line with still-evolving NIST standards. Because of unsettled policy and the overlapping and interwoven nature of contractor systems containing government information (e.g., contractors that deal with multiple government agencies), the Department's response and actions must be coordinated with other agencies and OMB. As noted in the OIG's recommendation, the Department's plan for addressing inventory, contract modifications and oversight is already being implemented. Language to address this issue from a contractual perspective is under development by representatives from across the Department. Upon completion of the new version of ITAB, central registration of contractor systems will be possible. *See also* response to recommendation # 1. The CIO is committed to resolving this recommendation and will add the requirement to the Federal Managers' Financial Integrity Act, Corrective Action Plan.

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

The CIO agrees with the recommendation. The official Department definition of the term "System" is found in 5 FAM 614: **System. A combination of hardware, software, facilities, personnel, data, and services to perform a designated function with specified results to user(s).** The 5 FAM will be rewritten to contain a separate section that consolidates all terms and definitions.

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

Appendix B

Department Response

The CIO agrees with the recommendation. The office that performs systems authorization is the owner of the application. Therefore, to avoid the potential conflict of interest, the Department hired an independent certification agent. The State Automated FISMA Reporting Environment (SAFIRE) application is in the Accreditation phase of the Systems Authorization Process. Remediation of the findings is complete and barring unforeseen circumstances, the CIO expects to authorize the system by the end of the fiscal year.

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.

The CIO agrees with the recommendation. This activity was not adequately funded in FY2005 due to budget constraints. The Department will add more resources to the SAFIRE project to increase SAFIRE visibility and strengthen the message that is already in place through additional training and advocacy. Furthermore, the SAFIRE team will continue to hold monthly meetings with the bureaus and continue to offer bureau assistance. In addition, presentations will be provided both domestically and overseas at conferences.

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

The CIO agrees with the recommendation. This is supported by existing policy in 5 FAM 866.d that provides, "the Designated Approval Authority (DAA) may disconnect any system, LAN, or domain that does not comply with the Department's Enterprise Patch Management Program's directives." Furthermore, the Department must continue to balance acceptable risk against operational requirements for information and information systems services.

Recommendation 7: The Chief Information Officer should develop and implement a process for local administrators on identifying vulnerabilities and applicable patches as well as identifying additional government resources.

The CIO generally agrees with the recommendation, but notes the even greater potential to reduce vulnerabilities by remotely monitoring networks and administering patches from off-site locations, thereby reducing the burden on local administrators and improving overall network management. IRM senior management will coordinate and develop a process for oversight and compliance for other hardware / software applications or systems. The Local Change Control Boards (CCBs) report local post patch management activity and approval of IT items to their IT CCB Voting Representatives and the IT CCB Change Manager. This reporting mechanism provides information to the Patch Management Team for tracking.

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.

The CIO agrees with the recommendation. The Department performed risk assessments on the major components of OpenNet and ClassNet. For example, the Department performed a risk

Department Response

assessment of the software image of workstations deployed overseas through the type accreditation of GITM-U and GITM-C. The systems are currently undergoing the initial phases of re-accreditation and will undergo more rigorous testing and scrutiny than on the first pass.

Recommendation 9: The Chief Information Officer should provide information security requirements for the regional computer security officers' enhanced evaluation and verification visits.

The CIO agrees with the recommendation. As a matter of clarification, the report's text should reflect the fact that the 2004 Roles and Responsibilities Matrix – developed jointly by the CIO and Assistant Secretary for DS - established the Evaluation and Verification (E&V) program, and assigned responsibility for this program to DS. The E&V program will help the Department maintain a continuous monitoring capability in accordance with NIST guidance and in keeping with the Department's resource priorities as well as help support the Systems Authorization programs under CIO oversight.

With regard to E&V oversight, it is also important to note that DS and IRM/IA staffs are continuing to work closely to develop reporting procedures that will support the CIO in meeting FISMA responsibilities. Furthermore, DS and IRM/IA present joint quarterly briefings to the CIO and Assistant Secretary for DS detailing the progress of the E&V program.

Due to limited staff and funding availability to support the E&V process, the CISO's office was limited to setting direction and collaborating with DS to provide high-level guidance and a framework for the E&V process. The CIO, through the CISO, is acting on this recommendation by instituting a formal oversight role using performance measurements and metrics.

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

The CIO agrees with the recommendation. Recently, NIST informed the Department that it intends to provide clarification on how to more effectively integrate penetration-test results of General Support Systems into the authorization of Major Applications. The formal outcome of NIST's guidance will provide the Department with critical information necessary to determine the mechanics, periodicity and linkage of penetration testing results into system authorization activities. Further, Department draft policy will be modified upon receipt of NIST's clarification.

The expected NIST clarification does not change the penetration testing requirements that the CIO identified and provided to the Bureau of Diplomatic Security. The testing and the periodicity specified in the CIO's directive is considered essential to the continued security health of the Department's networks and critical applications. The results of DS penetration testing will be reviewed as part of future systems authorization activities.

Recommendation 11: The Chief Information Officer should verify the accuracy of certification and accreditation information that is input into the information technology application baseline

Department Response

and the State Automated Federal Information Security Management Act Reporting Environment databases.

The CIO agrees with the recommendation. The solution is the development and implementation of the data bridge between the Information Technology Asset Baseline (ITAB) and the State Automated FISMA Reporting Environment (SAFIRE). This bridge will align the data within the two tools and allow for easier and more accurate validation and verification, as well as offer a complete inventory of systems for the Department including C&A information associated with them. SAFIRE and ITAB will be feeding information to each other by 2nd quarter 2006.

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

The CIO agrees with the recommendation, however, it should be noted except that the process may be done remotely or on-site. The Department is developing a process to improve compliance with security configuration guidelines. Improved reports include cumulative metrics used to facilitate CISO E&V process oversight and input into site visit selection. The ISSO program is supporting E&V by encouraging configuration scans and scheduling scanning tool training in the ISSO course.

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

The CIO agrees with the recommendation. To address the issues cited the CIO relies on the CISO in ensuring the security of the Department's information and information systems. During FY 2005, DS and IRM/IA staff in partnership with IRM/OPS shared information to resolve operational issues and address emerging policy challenges. The CIO will formally task all operational elements and all Department-wide security elements to include the CISO in all operational and policy decisions that may significantly impact the risk to the Department's information security posture.

We note that DS has continued to carry out its operational security duties in accordance with the Omnibus Diplomatic Security Act. These separate, but complementary, security responsibilities were documented and approved by the Under Secretary for Management in 2003 and subsequently updated in 2004.

Recommendation 14: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

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

Appendix B

Department Response

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

The CIO agrees with the recommendation. In FY2005, the Department implemented procedures that both encourage system users to take the annual computer security awareness training and provides for enforcement. All parties desiring access to the Department's primary network, OpenNet, must first complete an online training session and test. An annual training session and test is required for continued system access. Enforcement of this policy is delegated to local ISSOs and effectiveness will be monitored by the CISO's office. Should enforcement prove insufficient, the CISO will develop mitigating controls to improve performance.

Also, the report should note that the Department has, in accordance with NIST SP 800-16, identified 13 specific roles, the target audience for those roles, and the training courses available to meet the IA training requirements. This information is documented in the "FY05 Information Assurance Training Plan." Moreover, many of the 26 roles in SP 800-16 have been incorporated into the Department's set of 13 specific roles. As a result, resources are focused on meeting the largest percentage of significant employees with IT security responsibilities, specifically the Information Systems Security Officers (ISSOs), Technical Security Personnel at three levels, IT Managers, Senior-level Managers, Executives, Special Agents, Security Engineers, and OIG Auditors.

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.

The CIO agrees with the recommendation with comment. Since 2001, the Department has taken steps to identify employees with significant IT security responsibilities. These efforts are now documented in the Information Assurance Training Plan. This plan identifies required security training for specific information assurance roles relevant to the Department. It is a living document and is reviewed each year to evaluate resources, priorities, and timelines. As additional roles are added, additional resources will be required to design and deliver additional 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.

The CIO agrees with the recommendation. The Department's new registration process for Information Technology Asset Baseline (ITAB) will incorporate mandatory privacy reporting into the Department's application registration process. Specifically, system owners will be required to file all appropriate documentation with the Bureau of Administration's Senior Agency Official for Privacy for any information category that falls within the scope of a privacy impact assessment. The system authorization process serves as an additional verification that the applicable documentation is both complete and accurate and the commensurate security controls are tested.

Department Response

Recommendation 18: The Chief Information Officer should update guidance on employee privacy act responsibilities.

The Assistant Secretary for Administration (Senior Agency Official for Privacy) agrees (and the CIO concurs) with the recommendation, which should be redirected to the Assistant Secretary for Administration. Numerous efforts are underway that address the need to raise employee awareness of protecting privacy information. A Department-wide training program for employees and contractors is under development. Recently, the Office of Information Programs and Services delivered a three-day course to those employees responsible for processing Freedom of Information Act and Privacy Act requests from the public.

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

The Department set-up an e-mail address, Privacy-DL@state.gov mailto:Privacy-DL@state.gov>, for employees to ask privacy-related questions.

The Department has trained IT systems managers on completing Privacy Impact Assessments required by Section 208, Privacy Provisions of the E-Government of 2002. Part of that training included detailed guidance on their responsibilities under the Privacy Act and the handling of personal information.