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

Memorandum Report

Information Security Program Evaluation

Report Number IT/A-02-06, September 2002

MEMORANDUM REPORT IT-A-02-06

Information Security Program Evaluation

September 2002

In response to the Government Information Security Reform Act (GISRA),[1] the Office of Inspector General (OIG) performed an independent evaluation of the information security program and practices of the Department of State (Department). GISRA provides: (1) a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources; and (2) a mechanism for improved oversight of federal agency information security programs. The objective of the review was to determine whether the Department is effectively implementing key requirements of GISRA, including those areas pertaining to overall information technology (IT) security management and IT security risk management. The purpose, scope, and methodology for this review are discussed in appendix A.

RESULTS IN BRIEF

OIG's evaluation of the effectiveness of the Department's information security program found several key areas of security that still require management attention. Specifically, OIG concluded that the Department has made slow progress in addressing information security weaknesses identified in OIG's September 2001 GISRA report.[2] In response to the report, the Department developed a strategy to address a key deficiency: the lack of certification and accreditation of its information systems. However, the Department has not developed a timetable for certification and accreditation of all systems, and as of August 2002, only four percent of its systems had been certified and accredited. Further, according to OIG's survey questionnaire, although 72 percent of the Department's 358 systems are reported to have security-level determinations, only 15 percent are reported to have security plans.

In addition, in FY 2002, OIG reported on information security vulnerabilities through its reviews of key information management programs. For example, in its

[1] Public Law 106-398, Div. A, Title X, Subtitle G.

[2] *Senior Management Attention Needed to Ensure Effective Implementation of the Government Information Security Reform Act* (Report Number 01-IT-M-082, September 2001).

February 2002 report[3] on the Classified Connectivity Program (CCP), a project to implement classified processing capability at overseas missions, OIG reported that the Department has not developed a definitive strategy for managing the security risks of its CCP deployments. Specifically, OIG reported that the Department had not completed the steps needed to certify and accredit the classified Windows NT LAN in accordance with federal requirements.

Finally, at overseas missions, OIG found significant weaknesses in information security management. Specifically, OIG determined that the information systems security officers (ISSO) generally were not performing all the requisite duties of the position. In addition, none of the 11 missions that OIG visited had developed information systems security plans. Further, OIG found deficiencies in management, technical and operational controls, thus increasing the risk to mission operations.

This report presents the results of OIG's audit work in assessing the security over the Department's information technology resources. Recommendations OIG made to correct the deficiencies identified in this evaluation either were made in prior reports or will be made in reviews currently underway. Therefore, no recommendations are made in this report.

BACKGROUND

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

Computer-supported government operations, including those at the Department, are also at risk. Previous General Accounting Office (GAO), OIG, and Bureau of Diplomatic Security (DS) reports have identified persistent computer

[3] *Classified Connectivity Program: Progress and Challenges* (Report Number IT-A-02-01, February 2002).

security weaknesses that place a variety of critical and mission-essential Department operations at risk of disruption, fraud, and unauthorized disclosure. The Department recognizes that much more must be done to develop fully and ensure continuity of its systems security program.

Faced with growing concerns about information security risks to the federal government, the Congress passed and the President signed GISRA into law in late 2000. GISRA provides: (1) a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations and assets; and (2) a mechanism for improved oversight of federal agency information security programs. Specifically, GISRA requires agencies to:

- identify, use, and share best security practices;
- develop an agency-wide information security plan;
- incorporate information security principles and practices throughout the life cycles of the agency's information systems; and
- ensure that the information security plan is practiced throughout all life cycles of the agency's information systems.

In addition, GISRA assigns the agency's Chief Information Officer (CIO) the authority and responsibility to administer key functions under the statute, including:

- designating a senior agency information security official who reports to the CIO;
- developing and maintaining an agency-wide information security program;
- ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques; and
- training and overseeing personnel with significant responsibilities for information security.

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

OVERVIEW OF THE DEPARTMENT'S MANAGEMENT APPROACH TO INFORMATION SECURITY

The Department provided an overview of its management approach to information security in its FY 2001 Systems Security Program Plan (SSPP) issued in May 2001. The SSPP, which was first developed by the CIO and then issued to the Department, has not been revised to address the GISRA requirements and the more recent changes and delegations of authority within the Department. However, the SSPP does establish a baseline for the Department to build upon in organizing its information security program. It identifies the authorities and fundamental principles guiding IT security in the Department, outlines the IT roles and responsibilities of the Department's bureaus, and briefly addresses the strategies for achieving and maintaining a desirable IT security posture for the Department. The SSPP applies to all classified, unclassified, and sensitive but unclassified systems throughout the Department, its domestic bureaus, offices, annexes, and missions worldwide.

REVIEW FINDINGS

Slow Progress in Addressing FY 2001 GISRA Report Findings

The Department has made slow progress in addressing the information security deficiencies identified in OIG's September 2001 GISRA report.[4] OIG reported that, according to its system survey, nearly 70 percent of the Department's systems were reported to have security level determinations, while only ten percent were reported to have security plans, and only five percent were reported to have been certified and accredited. OIG recommended that the Department develop a strategy and timetable for ensuring that all of the Department's systems and applications address each of the key GISRA system security elements.

In response, DS and the Bureau of Information Resource Management (IRM) developed a strategy aimed at implementing the National Information Assurance Certification and Accreditation Process (NIACAP) across the Department, including quick and efficient certification and accreditation of all Department systems, networks, applications, domains, and sites. The strategy identifies five major areas (education, documentation, applications, sites, and remediation) that need to be

[4] *Senior Management Attention Needed* (Report Number 01-IT-M-082, September 2001).

addressed in order to implement NIACAP. However, the Department has not developed a timetable for certification and accreditation of all systems, and as of August 2002, only four percent of its systems had been certified and accredited. To its credit, as part of OpenNet Plus[5] implementation, the Department has made progress in assessing information security at missions and bureaus through its Connection Approval Process (CAP). So far, 23 bureaus and about 141 missions have had independent verification and validation (IV&V) of their respective IT infrastructures, which measures the extent to which each site complies with the Department's IT security configuration. Missions must show that they comply with existing security standards prior to receiving internet web services from OpenNet Plus. As of September 3, 2002, 20 bureaus and 84 missions have cleared IV&V requirements, and are connected to OpenNet Plus. According to DS and IRM, IV&V will provide a baseline for future efforts aimed at full certification and accreditation.

In addition, OIG reported that the Department has not developed information security performance measures to support strategic goals. Performance measures are key requirements of both the Government Performance and Results Act (Public Law 103-62) and GISRA. OIG recommended that the CIO ensure that program managers develop and use performance measures in support of the Department's information systems security program. In August 2002, the CIO issued the Department's FY 2003 Information Assurance Performance Measures Plan, and requested that all bureaus and missions implement procedures for collecting and submitting data in accordance with the plan. The CIO directed that collection of data should begin no later than October 1, 2002.

Department Information Security Weaknesses Identified in OIG Evaluations

In FY 2002, OIG reported on information security vulnerabilities through its audits of key information management programs. Specifically, OIG identified weaknesses in the management of information security in several information management programs. Also, in May 2002, OIG notified DS and IRM of a security vulnerability involving the fielding of OpenNet Plus. Finally, OIG noted that the Department has not addressed weaknesses in its critical infrastructure protection program.

[5] OpenNet Plus is the Department's program to provide worldwide desktop Internet access to its employees.

Information Security Issues in OIG Audit Reports

OIG identified additional weaknesses in the Department's management of information security in its reports on three different information management programs: Munitions Controls Systems, Classified Connectivity Program (CCP); and Central Financial Management System (CFMS). In March 2002,[6] OIG reported that the Office of Defense Trade Controls (DTC) had not obtained an up-to-date determination of the level of security required to protect its export licensing system and the proprietary munitions license data that it supports. In addition, OIG reported that the DTC's information assurance strategy has been one of risk avoidance; that is, remaining isolated to eliminate the potential for unauthorized access or malicious intrusion, rather than prioritization and risk management. OIG recommended that DTC assess the security risks of the munitions exports licensing process and develop and implement an information security strategy to manage those risks effectively.

Further, in its February 2002 report[7] on the CCP, a project to implement classified processing capability at overseas missions, OIG reported that the Department has not developed a definitive strategy for managing the security risks of its CCP deployment. Specifically, OIG reported that the Department had not completed the steps needed to certify and accredit the classified Windows NT LAN in accordance with federal requirements. Lacking certification, there is no central oversight or in-depth assessments to identify technical or environmental security risks for the CCP program. And, lacking accreditation, there is also no formal acceptance or accountability for managing those risks by site managers or chiefs of mission. OIG also reported that the Department's IT contingency planning efforts have not been adequate to help safeguard classified information systems and the critical business functions they support should unexpected disruptions occur at overseas missions. The report estimated that as many as 85 to 90 percent of the missions lack such plans.

Finally, in a May 2002 assessment[8] of CFMS, OIG reported that while the application functioned in a reasonably secure manner, weaknesses[9] in the Department's supporting IT infrastructure increased the risk that unauthorized users could gain access to the system. OIG made a number of recommendations to improve IT infrastructure security.

[6] *Streamlined Processes and Better Automation Can Improve Munitions License Reviews* (Report Number IT-A-02-02, March 2002).

[7] *Classified Connectivity Program* (Report Number IT-A-02-01, February 2002).

[8] *Information Technology Vulnerability Assessment for the Central Financial Management System* (Report Number AUD/FM-02-15).

OpenNet Plus Security Vulnerability

In May 2002, OIG notified IRM and DS of a security vulnerability concerning the fielding of OpenNet Plus[10] throughout the Department. OIG suggested that the two bureaus determine whether the vulnerability could be fixed or, if not, conduct a risk assessment and make a risk management decision about OpenNet Plus implementation. DS responded in a June 2002 memorandum to OIG, which was not cleared through IRM, suggesting there was no vulnerability, and even if there was, IRM had made a risk management decision to go forward. Subsequently, IRM issued a Department notice reminding employees that they should not download software from the Internet that has not been approved by the IT Change Control Board. As of September 2002, however, IRM had not developed a technical solution to this problem, or decided to accept the risk that this vulnerability presents to OpenNet Plus. Further, IRM had not notified the Department's systems administrators and ISSOs of this vulnerability and the risk it may pose to Department operations.

Critical Infrastructure Program Weaknesses Remain

The Department has not addressed weaknesses in its critical infrastructure protection program, which OIG discussed in a June 2001 report.[11] The report assesses the Department's progress in developing and implementing its cyber-based critical infrastructure protection plan, as mandated by Presidential Decision Directive 63. The OIG report contains a number of recommendations to strengthen the Department's approach to critical infrastructure protection planning, including:

- assessing the vulnerability of the Department's foreign operations to cyber-based disruptions;
- scheduling and conducting security controls evaluations of all minimum-essential cyber infrastructures at least once every three years; and
- ensuring that subsequent critical infrastructure protection plans and vulnerability assessments address minimum-essential interagency infrastructure vulnerabilities.

The Department has not addressed these recommendations, in part because its

[9] The specific details of these security weaknesses are classified.

[10] The specific details of this vulnerability are classified.

[11] *Critical Infrastructure Protection: The Department Can Enhance Its International Leadership and Its Own Cyber Security* (Report Number 01-IT-R-044, June 2001).

critical infrastructure planning has been in a state of flux. Specifically, in February 2002, the Under Secretary for Management established a formal Department-wide critical infrastructure protection program that is to be managed and provided with resources over a multiyear planning period. It is to be aligned with the Department's budget and planning process in order to achieve key objectives for domestic and overseas operations. In addition, the Under Secretary assigned lead responsibility for formulation and execution of the Department-wide critical infrastructure protection program to the Assistant Secretary for Resource Management. Subsequently, in April 2002, the Assistant Secretary for Resource Management established the Tier One Governance Board, which is comprised of senior managers who are responsible for the Department's infrastructure. The board is supposed to facilitate the decision making process on policy and priorities related to critical infrastructure protection objectives.

Mixed Results from OIG's Information Security Management Questionnaire

OIG developed two data collection surveys to determine general information about the Department's information security program. The first questionnaire identified the universe of systems operating throughout the Department. It also obtained information on IT security plans, assessments, and determinations as required by OMB guidance, prior information security laws, and GISRA.

Specifically, the first questionnaire requested information on the following:

- **Risk assessments.** The identification and analysis of possible risks in meeting the agency's objectives, which form a basis for managing the risks identified and implementing deterrents.
- **Security-level determinations.** Assessments that identify the specific security levels that should be maintained for IT systems hardware, software, and the information maintained or processed on systems.
- **System security plan.** A written plan that clearly describes the bureau or mission security program, as well as the policies and procedures that support it. The plan and related policies should include all major systems and facilities and outline the duties of those who are responsible for overseeing security as well as those who own, use, or rely on the entity's computer resources.
- **Certification and accreditation.** Attestations that an information system meets documented security requirements and will continue to maintain the approved security posture throughout its lifecycle.

- **Tests of security controls.** Assessments of controls designed to protect computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access.

According to OIG's survey results, the Department identified 358 systems and applications. Further, the survey indicated that there is significant room for improvement in information security management throughout the Department. As Table 1 shows, bureaus reported that 72 percent of their applications had security-level determinations. However, bureaus also reported that only four percent of their applications are certified and accredited, and only 15 percent of applications have security plans. (See appendix B for detailed survey results.)

Table 1: Department Survey Results on Key Information Systems Security Elements

System Requirement	Number	Percentage
Risk Assessment	201	56
Security-Level Determination	257	72
Security Plan	53	15
Certified and Accredited	16	4
Tested Security Controls	164	46

Note: A total of 358 systems and major applications reported in OIG's department survey.

The second questionnaire highlighted five of the Department's major information systems. OIG selected these systems based on their importance to the Department in the areas of human resources, inventory management, financial management, public diplomacy, and classified information processing. The questions pertained to management and operational controls. More specifically, they focused on security control reviews, personnel security, contingency planning, data integrity, security awareness, training, education, and incident response capabilities.

Overall, the second questionnaire and follow-up results were mixed. As shown in Table 2, bureaus reported that 60 percent of the systems had tested security controls, but only 20 percent of the systems had a documented risk assessment. Also, bureaus reported that only 20 percent of the systems have a security plan in place, and no system in the OIG sample was certified and accredited.

Table 2: Major Information Systems Survey Results

System	Risk Assessment	Security Level Determined	Security Plans	Certified and Accredited	Tested Security Controls
Classified Network	No	No	No	No	No
Global Employment Management System	No	Yes	No	No	Yes
Logistics Management Information System	No	Yes	Yes	No	Yes
Public Diplomacy Network	No	Yes	No	No	No
Regional Financial Management System	Yes	No	No	No	Yes

On a more positive note, Table 3 shows that all five systems have a trained ISSO assigned, and all five systems have automatic virus detection. However, the table also shows that only two of the five systems have contingency plans developed and updated and only one system has a documented IT system security self-assessment.

Table 3: Major Information Systems Survey Results

System	Trained ISSO	Contingency Plans Developed and Updated	Automatic Virus Detection	Security Self-Assessments
Classified Network	Yes	No	Yes	Yes
Global Employee Management System	Yes	Yes	Yes	No
Logistics Management Information System	Yes	Yes	Yes	No
Public Diplomacy Network	Yes	No	Yes	No
Regional Financial Management System	Yes	No	Yes	No

OIG's detailed review of each of these systems revealed the following:

Classified Network (ClassNet)

ClassNet, managed by IRM, is the Department's major classified information processing network. Although the bureau reported that ClassNet is certified and accredited, OIG's evaluation found that the system does not have a documented risk assessment, security plan, or tested security controls. Without these key information security elements in place the system cannot meet the requirements for certification and accreditation under NIACAP. IRM has made progress in strengthening ClassNet information security through the development of a draft document describing its critical operations and a draft backup and recovery plan.

Global Employee Management System (GEMS)

GEMS, managed by the Bureau of Human Resources (HR), is the primary Department personnel and human resource management system. Although OIG found considerable information security documentation in place for GEMS, including a contingency plan and administrator manuals, the documentation does not meet the systems security plan requirements cited in OMB Circular A-130. Further, OIG determined that neither a formal risk assessment nor a self-assessment of the system in accordance with NIST guidelines had been completed. Although HR completed the risk assessment section of its OMB Capital Asset Plan for the Department's FY 2003 budget submission, the information was not supported by an information security assessment.

Logistics Management Information System (LMIS)

LMIS, managed by the Bureau of Administration, is a comprehensive logistics management system. OIG's detailed review of LMIS showed that although an informal risk assessment for LMIS had been conducted, it did not satisfy either the NIST or OMB Circular A-130 guidance. Also, OIG found that no self-assessment had been completed for the system and that although there was a security plan in place, it had not been updated since 1998. Security plans should be updated when any major change is made to the system or at least once every three years during its usable life.

Public Diplomacy Network (PDNet)

PDNet, jointly managed by the Bureau of Educational and Cultural Affairs and the Office of International Information Programs, is the Department's primary network for public diplomacy activities. PDNet also provides users with Internet access. This system had been off-line for several months during FY 2001 following a successful hacker attack. OIG found minimal information security documentation in place and determined that no risk assessment or self-assessment had been conducted. In addition, bureau officials reported in a draft business continuity plan that the ability to recover fully and instantaneously, while desirable, is not possible because of funding constraints. Further, the plan states that disaster recovery would use off-site tape backups that would have to be recovered on another network, which does not exist at this time.

Regional Financial Management System (RFMS)

RFMS, managed by the Bureau of Resource Management, is a major financial management system currently under development. OIG selected this system for further review because GISRA requires that the agency information security plan be practiced throughout the system development life cycle, including initial development. OIG found that the bureau developed and submitted draft certification and accreditation documentation for precertification review. Also, the bureau has developed appropriately the required information security items, such as business case and mission statements, system specifications and designs, a configuration management plan, system administrator manuals, and a system security authorization agreement.

INFORMATION SECURITY MANAGEMENT DEFICIENCIES AT OVERSEAS MISSIONS

OIG evaluated information security management at 11 missions during FY 2002. OIG found that the Department's ISSO program was not meeting its objectives and that no mission visited had developed a mission-wide information systems security plan. In addition, OIG's technical evaluation identified significant weaknesses in mission information security management, technical and operational controls.

ISSO Program Weaknesses

At sites visited, OIG found that ISSOs generally are not performing all the requisite duties of the position. The Department's increasing dependence on information systems has created the need to ensure that IT system assets, including hardware, software, and the information they process, are protected from actions that could jeopardize the ability of employees to perform official duties. Although much of the responsibility for securing information and IT system assets has been placed with the ISSO, in most instances, these duties are assigned on a collateral basis and are not the primary duties of the individual designated as the ISSO. Instead, under the Department's 12 FAM 600 guidance, administrative officers at missions have assigned the responsibilities and associated duties to Foreign Service personnel whose primary positions are found in the information management, regional security, engineering security, and other offices. The collateral nature of these assignments reduces the time available to perform ISSO duties because the incumbents view them as secondary. Also, designating information management and information systems staff as ISSOs may hinder the ability to have independent monitoring and checking of both systems management and operations.

At nine of the eleven missions visited, OIG found that ISSOs were not fulfilling adequately their administrative, physical, personnel, system, and technical responsibilities. At one mission, for example, the designated ISSO had permanently departed, the alternate ISSO was performing none of the ISSO duties and no records existed to show what the previous ISSO had done. At another mission, the ISSO had run the Department's preferred analysis program once in a 12-month period, creating a six-inch stack of paper that was never completely analyzed. These analyses should be performed as frequently as determined appropriate for the specific mission, but not less than quarterly. In all instances, the incumbent ISSOs made the point that their designation and the associated collateral duties were secondary to their primary assignment. In one instance, an ISSO identified a serious problem at the mission concerning the processing of classified information on unclassified systems and was subsequently counseled about the time taken away from the ISSO's usual duties supporting IT operations.

Lack of Information Security Plans at Missions

OIG found that none of the missions visited had developed a mission-wide information systems security plan. DS recommends that ISSOs develop individualized security plans to carry out 12 FAM 600 policies and procedures overseas. At a minimum, these plans should describe:

- the mission's systems, including their names, purpose, location, who will be using them, and type of equipment, including peripherals and network connections;
- the type of information to be processed and stored, including the sensitivity level;
- the system staff and designated security responsibilities;
- vulnerabilities and threats to the mission's IT systems;
- the security incident reporting chain; and
- specific measures to reduce IT system risks.

The lack of security planning at the missions is, in part, the result of insufficient guidance from the Department and a general belief at missions that IT information security is less important than other elements of security. Officials told OIG that developing a mission-wide security plan was unlikely because information management staff were overburdened with the mission's immediate technical and operational concerns. In addition, information management staff told OIG that the mission's culture tended to prioritize physical security, customer service and other business issues before IT information security.

To address this problem, DS has developed draft site Systems Security Authorization Agreement templates for both the sensitive-but-unclassified and classified processing environments. This template, once completed by a mission, will be the single source for all information pertaining to the certification and accreditation process of a mission or bureau. DS plans to implement this template in October 2002.

Results Of Mission Information Security Technical Evaluations

OIG found significant weaknesses in the Department's management, technical and operational controls at missions visited during FY 2002. These weaknesses resulted from improperly configured systems, inadequate testing of controls, and, in some instances, inadequate understanding of the interrelationships of controls and the corresponding system. Thus, at 11 missions visited, IT information systems could be compromised through a variety of means that exploited the existing controls.

Controls improve the security of a particular system or group of systems. They often require technical or specialized expertise as well as rely upon management activities. Management controls include techniques and measures that focus on the oversight of the IT security systems and the management of risk for a specific system. Technical controls are controls that are automated and rely on technical expertise to implement. These controls can provide automated protection against unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The focus of operational controls is those controls implemented and executed by people.

Table 4 below highlights weaknesses identified during OIG's technical evaluations and associates the weaknesses with three key issue areas that are the foundation of the Department's approach to IT risk management, and are necessary to protect mission operations from disruption. Weaknesses in system security proce-

Table 4: Technical Evaluation Summary: Weaknesses in Mission Information Security

	CONTROL AREAS		
ISSUE AREAS	**Management Controls**	**Technical Controls**	**Operational Controls**
Password and Account Management	Inadequate training Inadequate enforcement of standardized requirements Inadequate separation of duties in account establishment	Lack of password and account management plan Inadequate control for system security account manager	Inadequate process for review of password development Inadequate compliance with FAM guidance on password development
Configuration and Change Control Management	IT configuration management process, including change control not implemented	Servers and workstations not in compliance with Department standards	Centralized asset management insufficient
Documentation	No entity-wide security plans No documented risk assessments and other key documentation	No standard approach for implementing and managing systems	No Department guidance that establishes minimum security requirements

dures, if exploited, can cause damage to hardware components, software applications and the information on the system. For example, as a result of inadequate password management, the system could be exploited through penetration or impersonation, and IT information resources could be used for unauthorized purposes or to launch attacks.

DEPARTMENT COMMENTS

OIG discussed the contents of this report with Department officials on August 28, 2002. Generally, these officials agreed with the issues presented, and noted that there is mutual agreement that additional efforts must be made to implement a comprehensive information security program.

PURPOSE, SCOPE, AND METHODOLOGY

Section 3535 of GISRA directs each agency to conduct an annual independent evaluation of its information security program and practices beginning in FY 2001. The objective of the review was to determine whether the Department is effectively implementing key requirements of GISRA, including those areas pertaining to overall IT security and risk management.

To fulfill OIG review objectives, OIG developed two data collection surveys, which OIG used to obtain general information about the Department's information security program. OIG's first survey determined the Department's universe of systems. OIG sent a questionnaire to all identified system managers at the Department asking general information security questions. The managers were also asked to update the Department's list of information systems to the best of their knowledge. The second survey highlighted five of the Department's major information systems. OIG selected these systems based on their importance to the Department in the areas of human resources, inventory management, financial management, public diplomacy, and classified information processing. OIG's questions pertained to management and operational controls. More specifically, the questions focused on security control reviews, personnel security, contingency planning, data integrity, security awareness, training, education, and incident response capabilities. The questions in the surveys came directly from the National Institute of Standards and Technology's *Self-Assessment Guide for Information Technology Systems*, which OIG edited to cover risk/vulnerability assessments, security controls, life cycle, certification and accreditation, information system security plans, personnel security, contingency plans, data integrity, documentation, and incident response capability. OIG did not independently verify the information collected from its first survey, but did selectively verify key information from responses to its second survey.

OIG discussed the contents of this report with Department officials on August 28, 2002, and made revisions to the report where appropriate. Staff from OIG's Information Technology Office performed this evaluation from February 2002 through July 2002. Contributors to this report were Frank Deffer, James Davies, Tim Fitzgerald, Robert Taylor, Chris Watson, Matthew Worner and Heather Rogers. Comments or questions about the report can be directed to Mr. Deffer at defferf@state.gov or at (703) 284-2715 or to Mr. Davies at daviesj@state.gov or at (703) 284-2673.

FY 2002 GISRA Evaluation-Questionnaire Statistics Summary

Department Entity	Total Number of Systems Reported by Bureau	Systems with Risk Assessments		Systems with Security Level Determinations		Systems with Security Plans		Systems Certified and Accredited		Systems with Tested Security Controls	
		Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Bureau of Administration	28	7	25	8	29	6	21	5	18	3	11
Bureau of Consular Affairs	36	25	69	17	47	15	42	4	11	17	47
Bureau of Diplomatic Security	46	46	100	46	100	0	0	0	0	46	100
Bureau of Diplomatic Security, Office of Foreign Missions	4	0	0	1	25	1	25	0	0	0	0
Bureau of East Asian and Pacific Affairs	1	0	0	1	100	0	0	0	0	1	100
Bureau of Educational and Cultural Affairs[12]	38	23	61	38	100	11	29	0	0	0	0
Bureau of European Affairs	5	0	0	0	0	0	0	0	0	0	0
Foreign Service Institute	2	1	50	2	100	1	50	0	0	0	0
Bureau of Human Resources	20	3	15	18	90	6	30	2	10	19	95
Bureau of Information Resource Management	29	11	38	11	38	8	28	2	7	3	10
Office of Inspector General	8	5	63	6	75	0	0	0	0	6	75
Bureau of Intelligence and Research	3	2	67	3	100	2	67	1	33	1	33
Bureau of International Narcotics and Law Enforcement Affairs	1	1	100	1	100	1	100	0	0	1	100
Bureau of International Organizational Affairs	2	2	100	2	100	0	0	0	0	0	0
Office of the Legal Adviser	5	0	0	0	0	0	0	0	0	0	0
Office of Medical Services	3	2	67	3	100	0	0	0	0	2	67
Bureau of Nonproliferation	2	0	0	2	100	0	0	0	0	0	0
Bureau of Oceans and International Environmental and Scientific Affairs	5	5	100	5	100	0	0	0	0	0	0
Overseas Building Operations	29	1	3	29	100	0	0	0	0	0	0
Bureau of Population, Refugees, and Migration	2	0	0	0	0	0	0	0	0	0	0
Bureau of Public Affairs	5	1	20	1	20	0	0	0	0	0	0
Bureau of Resource Management	23	5	22	2	9	2	9	2	9	5	22
Office of the Secretary	61	61	100	61	100	0	0	0	0	60	98
Totals	**358**	**201**	**56**	**257**	**72**	**53**	**15**	**16**	**4**	**164**	**46**

[12] The Bureau of Educational and Cultural Affairs response also includes the Coordinator of International Information Programs office.