United States Department of State
Office of Inspector General

Executive Summary

Government Information Security Reform Act
FY 2002 Submission

September 16, 2002

EXECUTIVE SUMMARY

PURPOSE

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). This executive summary provides the results of OIG's evaluation in two parts. Part I summarizes the results of OIG's review of the Department's information security program. Part II contains OIG's assessment of the Department's information security program using performance measures provided by the Office of Management and Budget (OMB).

PART I

Results of OIG's Information Security Program Evaluation (Report IT-A-02-06)

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 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.

[1] Public Law No. 106-398, Div. A, Title X, Subtitle G., 114 Stat. 1654A (2000), 44 U.S.C. 3531 et seq.
[2] *Senior Management Attention Needed to Ensure Effective Implementation of the Government Information Security Reform Act* (Report Number 01-IT-M-082, September 2001).
[3] *Classified Connectivity Program: Progress and Challenges* (Report Number IT-A-02-01, February 2002).

Part II

OIG Assessment of the Department's Information Security Program Based on OMB Performance Measures

A. General Overview

1. Not Applicable

2. Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or IGs in both last year's report (FY01) and this year's report (FY02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.

TABLE A.1: DEPARTMENT OF STATE PROGRAMS AND SYSTEMS

		FY 2001	FY 2002
2a	Total number of agency programs.	NA	211
2b	Total number of agency systems reported to OIG in its Department survey.	370	358
2c	Total number of programs reviewed by OIG.	0	12
2d	Total number of systems reviewed by OIG.	16	9

Note: Line 2a is the sum of those missions with MPP reporting requirements [181] + Bureaus [27] + Financial Service Centers [3].

OIG developed two data collection surveys to obtain general information about the Department's information security program. The first survey determined the Department's universe of systems. The second survey highlighted five of the Department's major information systems. OIG selected these systems according to 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, 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 (NIST) self-assessment guide, which OIG edited to cover risk and 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 the first survey, but did selectively verify key information from responses to the second survey. Additionally, OIG conducted independent audit and inspection work on 12 Department programs and four other systems, again relying on the NIST self-assessment guide.

3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act.) Identify the number of reported material weaknesses for FY 01 and FY 02, and the number of repeat weaknesses in FY02.

TABLE A.2: DEPARTMENT OF STATE MATERIAL WEAKNESSES

		FY 2001	FY 2002
3a	Number of material weaknesses reported.	4	3
3b	Number of material weaknesses repeated in FY 2002.	NA	3

In FY 2001, the Department had four material weaknesses on its books. Three of these were reported under the Federal Managers Financial Integrity Act (FMFIA),[4] as follows:

- inadequate administrative staffing overseas;
- integration of grants tracking system; and
- exchange visitor information system.

The Department's fourth material weakness for FY 2001 was: *"information systems security for networks in domestic operations."* This weakness was brought to the Department's attention in a U.S. General Accounting Office (GAO) review, and it was cited in OIG's audit of the Department's financial statements under the Federal Financial Management Improvement Act of 1996.[5] Although the weakness was closed for FMFIA purposes as GAO closed out the recommendations pertaining to it, it is still considered a material weakness for financial statement purposes and is reported in the Department's FY 2001 Accountability Report.

On June 27, 2002, the Department's Management Control Steering Committee voted to close the material weakness concerning "inadequate administrative staffing overseas," and it will not be reported in the FMFIA report for FY 2002. The Committee added the other two material weaknesses from last year to the agenda for consideration on closing at the next Management Control Steering Committee meeting, scheduled for September 2002.

B. Responsibilities of Agency Head

1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

In August 2001, the Department took the following key steps:

- The Deputy Secretary issued a Delegation of Authority to the CIO, empowering him to administer the Department's information security program.

[4] Public Law No. 97-255, 96 Stat. 814 (1982).
[5] Public Law No. 104-208, Div. A, Title I, 110 Stat. 3009-389 (1996).

- The CIO designated the deputy assistant secretary for countermeasures and information security as the senior agency information security officer. This officer reports directly to the CIO regarding the implementation and maintenance of the Department's information security program and security policies.
- The Under Secretary for Management designated the CIO as the designated approving authority (DAA), responsible for making risk acceptance determinations for information technology on behalf of the Department. Based on mission criticality, the DAA may accept risk and grant either an approval to operate or an interim approval to operate if the system does not meet requirements.
- The Under Secretary for Management also agreed to several changes in the respective roles and responsibilities of the Bureaus of Diplomatic Security (DS) and Information Resource Management (IRM) over information security. For example, DS is responsible for developing and recommending computer security policies, while the CIO, who is under IRM, has final review and approval authority for such policies.

Concerning the enforcement of GISRA responsibilities and authorities, 5 FAM 619 requires that Department systems undergo certification and accreditation evaluation by DS before implementation. Further, the directive states that project managers should estimate the cost of incorporating each safeguard or countermeasure into a system.

The Department has established information technology (IT) review boards to evaluate and approve certain projects. According to the Foreign Affairs Handbook (5 FAH-5 H-116), boards determine if projects will benefit the mission of the Department as outlined in the Department's Strategic Plan. Specifically, the Information Technology Program Board reviews projects with a life cycle cost of $30 million or more, or those determined by the Under Secretary for Management to be of critical importance to the mission. Further, the Management Review Advisory Group and the Technical Review Advisory Group evaluate projects with life cycle values of less than $30 million. Generally, department bureaus and overseas missions can make routine IT investment decisions (less than $100,000) without review by and concurrence of the CIO.

As part of its IT Capital Planning Process, the Department requires bureaus to submit budget information on all IT projects, regardless of funding source, into the IT Investment Portfolio System (I-TIPS). For FY 2004, bureaus were required to submit project information by June 7, 2002, in order to be considered for inclusion in the Department's budget request.

2. How does the head of the agency ensure that the agency's information security program is practiced throughout the life cycle of each agency system? During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the life cycle of each system?

In December 2001, OMB notified the Department that it had disapproved its security program, largely on the basis of the Department's GISRA report and the serious issues found, and its own reviews of security integration in the capital planning process.

In response, in March 2002, the Under Secretary for Management directed DS and IRM to develop a plan to address incomplete planning and certification and accreditation of individual systems. Specifically, the Under Secretary directed DS and IRM to develop plans to:

- implement fully the National Information Assurance Certification and Accreditation Process (NIACAP) in the Department. The plan must include performance-based, competitive sourcing options, and budget impact statements for all options presented.
- eliminate quickly and efficiently the current systems certification and accreditation backlog. This plan must also include performance-based, competitive sourcing options, and budget impact statements for all options presented.

In July 2002, the Under Secretary for Management approved a proposal by DS and IRM to implement NIACAP across the Department, including quick and efficient certification and accreditation of all Department systems, networks, applications, domains, and sites. The plan identifies five major issue areas (education, documentation, applications, sites, and remediation) that need to be addressed in order to implement NIACAP.

3. How has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.) Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?

Generally, the Department has not integrated its information technology security program with its critical infrastructure protection (CIP) responsibilities and other security programs. It has, however, taken a number of steps to strengthen its approach to CIP. Specifically, in February 2002, the Under Secretary for Management decided to:

- establish a formal Department-wide CIP program that will be managed and resource-loaded over a multiyear planning period that is aligned with the Department's budget and planning process to achieve CIP objectives for domestic and overseas operations; and
- assign lead responsibility for formulation and execution of the Department-wide CIP program to the Assistant Secretary for Resource Management.

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 CIP objectives.

Finally, the Department has a wide variety of security programs at its bureaus and overseas missions operating under the authority of different agency officials. Thus far, there have been no specific efforts taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complementary across the various programs and disciplines.

4. Has the agency undergone a Project Matrix review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets.

The Department has not undergone a Project Matrix review. In December 2001, the Department's Critical Infrastructure Protection Governance Board agreed to participate in Project Matrix. Because of limitations on the collection, processing, and controlling of classified and highly sensitive information, the Department's participation has been limited to that of providing unclassified materials. At this time, the Department is developing its approach to identifying its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets.

5. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

<table>
<tr><th colspan="4">TABLE B.1: RESPONSIBILITIES OF AGENCY HEAD</th></tr>
<tr><td>5a</td><td colspan="2">Total number of agency components including bureaus, field activities (functional areas and worldwide transmitting sites).</td><td>344</td></tr>
<tr><td>5b</td><td colspan="2">Number of agency components with incident handling and response capability.</td><td>344</td></tr>
<tr><td>5c</td><td colspan="2">Number of agency components that report to FedCIRC.</td><td>1 (DS CIRT)</td></tr>
<tr><td>5d</td><td colspan="2">Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?</td><td>Yes</td></tr>
<tr><td>5e</td><td colspan="2">What is the required average time to report to the agency and FedCIRC following an incident?</td><td>Varies case-by-case</td></tr>
<tr><td>5f</td><td colspan="2">How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?</td><td>Engineering a comprehensive process</td></tr>
<tr><td colspan="2"></td><td><b>FY 2001</b></td><td><b>FY 2002</b></td></tr>
<tr><td>5g</td><td>By agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported by each component.</td><td>1,441 CIRT
239,272 VIRT</td><td>As of July 1: 1,085
As of July 30: 181,180</td></tr>
<tr><td>5h</td><td>By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.</td><td>118</td><td>As of July 1: 70</td></tr>
</table>

Note 1: CIRT is Computer Incident Response Team
Note 2: VIRT is Virus Incident Response Team
Note 3: FedCIRC is Federal Computer Incident Response Capability

OIG did not evaluate the Department's incident handling policy and procedures. This area of interest will be included in OIG's work for FY 2003 under the proposed Federal Information Security Management Act. The information shown in Table B.1 was provided by the CIO and has not been verified.

C. Responsibilities of Agency Program Officials

1. Have agency program officials: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? (Section 3534(a)(2) of the Security Act.)

According to OIG's survey results, the Department identified 358 systems and applications in FY 2002 (compared with 370 in FY 2001). Generally, OIG's survey indicates that there is significant room for improvement. As Table C.1 shows, bureaus reported in FY 2002 that 72 percent of their systems had security-level determinations. However, bureaus also reported in FY 2002 that only four percent of their systems are certified and accredited, and only 15 percent of systems have security plans. The tables below provide the survey results for the Department as a whole, and for each bureau.

TABLE C.1: DEPARTMENT OF STATE – AGENCY TOTALS

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	370		358	
1a	Systems that have been assessed for risk	219	59	201	56
1b	Systems that have been assigned a security level determination	256	69	257	72
1c	Systems that have an up-to-date security plan	38	10	53	15
1d	Systems that have been authorized for processing following certification and accreditation	18	5	16	4
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	352	95	342	96
1g	Systems for which security controls have been tested and evaluated in the last year	162	44	164	46

Note: Section C, questions 1f (cost of security controls), 1h (contingency plan), and 1i (contingency plan tested in last year) were not addressed in the OIG survey.

TABLE C.2: BUREAU OF ADMINISTRATION

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	55		28	
1a	Systems that have been assessed for risk	8	15	7	25
1b	Systems that have been assigned a security level determination	39	71	8	29
1c	Systems that have an up-to-date security plan	5	9	6	21
1d	Systems that have been authorized for processing following certification and accreditation	4	7	5	18
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	51	93	23	82
1g	Systems for which security controls have been tested and evaluated in the last year	4	7	3	11

Note: The 55 systems shown for the Bureau of Administration are the total reported before May 15, 2001, when the Office of Foreign Buildings Operations (FBO) was still part of the bureau. After that date, FBO became a separate Bureau of Overseas Buildings Operations, reporting directly to the Under Secretary for Management.

TABLE C.3: BUREAU OF CONSULAR AFFAIRS

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	36		36	
1a	Systems that have been assessed for risk	23	64	25	69
1b	Systems that have been assigned a security level determination	8	22	17	47
1c	Systems that have an up-to-date security plan	0	0	15	42
1d	Systems that have been authorized for processing following certification and accreditation	2	6	4	11
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	34	94	32	89
1g	Systems for which security controls have been tested and evaluated in the last year	1	3	17	47

TABLE C.4: BUREAU OF DIPLOMATIC SECURITY

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	51		46	
1a	Systems that have been assessed for risk	46	90	46	100
1b	Systems that have been assigned a security level determination	47	92	46	100
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	1	2	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	50	98	46	100
1g	Systems for which security controls have been tested and evaluated in the last year	46	90	46	100

TABLE C.5: BUREAU OF DIPLOMATIC SECURITY, OFFICE OF FOREIGN MISSIONS

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	See Note		4	
1a	Systems that have been assessed for risk			0	0
1b	Systems that have been assigned a security level determination			1	25
1c	Systems that have an up-to-date security plan			1	25
1d	Systems that have been authorized for processing following certification and accreditation			0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)			4	100
1g	Systems for which security controls have been tested and evaluated in the last year			0	0

Note: In FY 2001, the Office of Foreign Missions' data were rolled into the Bureau of Diplomatic Security data.

TABLE C.6: BUREAU OF EAST ASIAN AND PACIFIC AFFAIRS

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	1		1	
1a	Systems that have been assessed for risk	0	0	0	0
1b	Systems that have been assigned a security level determination	0	0	1	100
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	1	100	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	0	0	1	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	1	100

TABLE C.7: BUREAU OF EDUCATIONAL AND CULTURAL AFFAIRS

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	40		38	
1a	Systems that have been assessed for risk	30	75	23	61
1b	Systems that have been assigned a security level determination	32	80	38	100
1c	Systems that have an up-to-date security plan	12	30	11	29
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	40	100	38	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

Note: The Bureau of Educational and Cultural Affairs response also includes the Coordinator of International Information Programs office.

TABLE C.8: BUREAU OF EUROPEAN AFFAIRS

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	5		5	
1a	Systems that have been assessed for risk	0	0	0	0
1b	Systems that have been assigned a security level determination	0	0	0	0
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	5	100	5	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

TABLE C.9: FOREIGN SERVICE INSTITUTE

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	2		2	
1a	Systems that have been assessed for risk	0	0	1	50
1b	Systems that have been assigned a security level determination	2	100	2	100
1c	Systems that have an up-to-date security plan	0	0	1	50
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	2	100	2	100
1g	Systems for which security controls have been tested and evaluated in the last year	2	100	0	0

TABLE C.10: BUREAU OF HUMAN RESOURCES

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	20		20	
1a	Systems that have been assessed for risk	4	20	3	15
1b	Systems that have been assigned a security level determination	18	90	18	90
1c	Systems that have an up-to-date security plan	6	30	6	30
1d	Systems that have been authorized for processing following certification and accreditation	1	5	2	10
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	19	95	18	90
1g	Systems for which security controls have been tested and evaluated in the last year	19	95	19	95

TABLE C.11: BUREAU OF INFORMATION RESOURCE MANAGEMENT

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	29		29	
1a	Systems that have been assessed for risk	12	41	11	38
1b	Systems that have been assigned a security level determination	11	38	11	38
1c	Systems that have an up-to-date security plan	7	24	8	28
1d	Systems that have been authorized for processing following certification and accreditation	3	10	2	7
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	26	90	27	93
1g	Systems for which security controls have been tested and evaluated in the last year	2	7	3	10

TABLE C.12: OFFICE OF INSPECTOR GENERAL

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	6		8	
1a	Systems that have been assessed for risk	5	83	5	63
1b	Systems that have been assigned a security level determination	6	100	6	75
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	6	100	8	100
1g	Systems for which security controls have been tested and evaluated in the last year	6	100	6	75

TABLE C.13: BUREAU OF INTELLIGENCE AND RESEARCH

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	3		3	
1a	Systems that have been assessed for risk	2	67	2	67
1b	Systems that have been assigned a security level determination	3	100	3	100
1c	Systems that have an up-to-date security plan	2	67	2	67
1d	Systems that have been authorized for processing following certification and accreditation	1	33	1	33
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	2	67	2	67
1g	Systems for which security controls have been tested and evaluated in the last year	1	33	1	33

TABLE C.14: BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	1		1	
1a	Systems that have been assessed for risk	1	100	1	100
1b	Systems that have been assigned a security level determination	1	100	1	100
1c	Systems that have an up-to-date security plan	1	100	1	100
1d	Systems that have been authorized for processing following certification and accreditation	1	100	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	0	0	1	100
1g	Systems for which security controls have been tested and evaluated in the last year	1	100	1	100

Table C.15: Bureau of International Organizational Affairs

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	2		2	
1a	Systems that have been assessed for risk	2	100	2	100
1b	Systems that have been assigned a security level determination	2	100	2	100
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	2	100	2	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

Table C.16: Office of the Legal Adviser

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	5		5	
1a	Systems that have been assessed for risk	0	0	0	0
1b	Systems that have been assigned a security level determination	0	0	0	0
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	5	100	5	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

Table C.17: Office of Medical Services

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	3		3	
1a	Systems that have been assessed for risk	3	100	2	67
1b	Systems that have been assigned a security level determination	3	100	3	100
1c	Systems that have an up-to-date security plan	3	100	0	0
1d	Systems that have been authorized for processing following certification and accreditation	3	100	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	0	0	3	100
1g	Systems for which security controls have been tested and evaluated in the last year	3	100	2	67

Table C.18: Bureau of Nonproliferation

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	2		2	
1a	Systems that have been assessed for risk	0	0	0	0
1b	Systems that have been assigned a security level determination	2	100	2	100
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	2	100	2	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

Table C.19: Bureau of Oceans and International Environmental and Scientific Affairs

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	5		5	
1a	Systems that have been assessed for risk	5	100	5	100
1b	Systems that have been assigned a security level determination	5	100	5	100
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	5	100	5	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

TABLE C.20: OVERSEAS BUILDINGS OPERATIONS

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	See Note		29	
1a	Systems that have been assessed for risk			1	3
1b	Systems that have been assigned a security level determination			29	100
1c	Systems that have an up-to-date security plan			0	0
1d	Systems that have been authorized for processing following certification and accreditation			0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)			29	100
1g	Systems for which security controls have been tested and evaluated in the last year			0	0

Note: The 55 systems shown for the Bureau of Administration are the total reported before May 15, 2001, when the Office of Foreign Buildings Operations (FBO) was still part of the bureau. After that date, FBO became a separate Overseas Buildings Operations, reporting directly to the Under Secretary for Management.

TABLE C.21: BUREAU OF POPULATION, REFUGEES, AND MIGRATION

		FY 2001		FY 2002	
		Number	Percent	Number	Percent
	Total systems and major applications reported to OIG in its Department survey	2		2	
1a	Systems that have been assessed for risk	0	0	0	0
1b	Systems that have been assigned a security level determination	0	0	0	0
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	2	100	2	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

TABLE C.22: BUREAU OF PUBLIC AFFAIRS

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	5		5	
1a	Systems that have been assessed for risk	1	20	1	20
1b	Systems that have been assigned a security level determination	1	20	1	20
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	5	100	5	100
1g	Systems for which security controls have been tested and evaluated in the last year	0	0	0	0

TABLE C.23: BUREAU OF RESOURCE MANAGEMENT

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	22		23	
1a	Systems that have been assessed for risk	2	9	5	22
1b	Systems that have been assigned a security level determination	1	5	2	9
1c	Systems that have an up-to-date security plan	2	9	2	9
1d	Systems that have been authorized for processing following certification and accreditation	1	5	2	9
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	21	95	21	91
1g	Systems for which security controls have been tested and evaluated in the last year	3	14	5	22

TABLE C.24: OFFICE OF THE SECRETARY

		FY 2001		FY 2002	
		Number	**Percent**	**Number**	**Percent**
	Total systems and major applications reported to OIG in its Department survey	75		61	
1a	Systems that have been assessed for risk	75	100	61	100
1b	Systems that have been assigned a security level determination	75	100	61	100
1c	Systems that have an up-to-date security plan	0	0	0	0
1d	Systems that have been authorized for processing following certification and accreditation	0	0	0	0
1e	Systems that are operating without written authorization (including the absence of certification and accreditation)	75	100	61	100
1g	Systems for which security controls have been tested and evaluated in the last year	74	99	60	98

2. For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

OIG did not evaluate the Department or program officials' handling of contractor or other agency information services provided to the Department. This area of interest will be included in the OIG's work for FY 2003 under the proposed Federal Information Security Management Act.

D. Responsibilities of Agency Chief Information Officers

1. Has the agency CIO: 1) adequately maintained an agency-wide security program; 2) ensured the effective implementation of the program and evaluated the performance of major agency components; and 3) ensured the training of agency employees with significant security responsibilities? Identify actual performance according to the measures and in the format provided below. (Section 3534(a)(3)-(5)) and (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

TABLE D.1: RESPONSIBILITIES OF AGENCY CHIEF INFORMATION OFFICERS

		FY 2001	FY 2002
1a	Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews?	N/A	161 IV&V
1b	What percentage of components and field activities have had such reviews?	N/A	unknown
1c	Number of agency employees including contractors.	25,604	31,975
1d	Number and percentage of agency employees including contractors that received security training. (1-hour security training for OpenNet Plus users)	N/A	16,365 51%
1e	Number of employees with significant security responsibilities	N/A	unknown
1f	Number of employees with significant security responsibilities that received specialized training.	325	2,800
1g	Briefly describe what types of security training were available.	narrative	narrative
1i	Do agency POA&Ms account for all known agency security weaknesses including of all components and field activities? If no, why not?	N/A	No - narrative
1j	Has the CIO appointed a senior agency information security official?	Yes	Yes

Note 1: POA&Ms are plans of action and milestones reports

1) Adequately maintained an agency-wide security program.

The CIO has not adequately maintained an agency-wide security program, in part because all the elements of such a program are not in place, or have not been implemented. First, as OIG states in its evaluation report, the Systems Security Program Plan (SSPP), which provides an overview of the Department's management approach to information security, was not revised to address the requirements resulting from GISRA's enactment and does not reflect changes and delegations of authority made within the Department to meet GISRA requirements.

The Department is currently revising the SSPP so that it is consistent with GISRA.

Second, a critical element of the SSPP, certification and accreditation, has not been implemented across the Department. According to the SSPP, the certification and accreditation process is the primary vehicle for the implementation of IT risk management for the Department. Further, the SSPP states that this process is designed to ensure that IT security requirements established by law and by Department policy are met and followed to ensure that the Department's information security posture is not adversely impacted. Toward that end, in July 2002, the Under Secretary for Management approved a strategy developed by DS and IRM to implement NIACAP, 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 addressed. However, as OIG reported in its FY 2002 GISRA evaluation, 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.

Third, for FY 2002, the Department had not developed and implemented information security performance measures to support strategic goals. Without meaningful and measurable performance measures, the Department was not able to implement a results-based information security management program. To resolve this problem, 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.

To address weaknesses in the Department's security program, the CIO has approved the establishment of the Office of Information Assurance (IA). The new directorate reports to the deputy assistant secretary (deputy chief information officer) and has had a significant number of resources, both financial and staff, assigned commensurate with its new and increased responsibilities. The purpose of this office is to plan, manage, and track the Department's IT security program in accordance with government mandates. The IA Office supports the DAA and CIO in accrediting systems and applications that have undergone the certification process. The IA Office is also responsible for developing the Departmental Information Assurance Program Plan that acts as an implementation guide for IT security throughout the Department.

2) *Ensured the effective implementation of the program and evaluated the performance of major agency components.*

The CIO has not ensured effective implementation of the security program. As OIG reported in its evaluation of the Department's information security program, the CIO is making slow progress in addressing the information security weaknesses identified in OIG's September 2001 GISRA report.[6] Specifically, OIG reported that there is significant room for improvement in information security management throughout the Department. For example, although 72 percent of the Department's 358 systems were reported to have security level determinations, only 15 percent were reported to have security plans. In addition, OIG reported that information security deficiencies at overseas missions increase the risk that mission operations could be disrupted.

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

For example, OIG noted that none of the missions visited had developed a mission-wide information systems security plan. Further, OIG found that because of weaknesses in the Department's management, technical, and operational controls, IT systems could be compromised through a variety of means.

Finally, the CIO has made progress in evaluating the performance of major components. As part of OpenNet Plus[7] implementation, the CIO is assessing information security at missions and bureaus through the connection approval process. 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.

3) Ensured the training of agency employees with significant security responsibilities.

The Department has made progress in addressing the information security training needs of its employees. The SSPP identifies 13 roles or functions that have significant security responsibilities. Each function impacts the design, execution, or evaluation of automated information systems (AIS) security procedures and practices. Specialized AIS security training has been developed or is planned for eight of the functions. The eight functions include Ambassadors and Chiefs of Mission, system owners, information management officers (IMO), system administrators, information system security officers (ISSO), security engineering officers, regional security officers (RSO), and regional computer security officers (RCSO).

Under the Automated Information Systems Security Training Program (AISSTP), courses of instruction vary according to a group's responsibility, as established by the Department, and last up to five days. With the exception of RCSOs, for whom the AISSTP office arranges specialized outside instruction, all classes are developed and presented by DS. Classes are presented worldwide throughout the year. In FY 2002, a total of 44 classes will have been presented.

Until FY 2002, the ISSO basic course was the only training presented by AISSTP. About 1,100 people have attended this course in the four years it has been presented. Everyone was provided with the same content regardless of his or her role. The AISSTP recognized that this did not conform to federal requirements and started the development and delivery of new courses. Two of them, AIS Security for System Administrators and AIS Security for RSOs, were started in FY 2002. Another course, AIS Security for IMOs, is expected to debut within three months. AISSTP expects to develop instruction for all of the groups mentioned above. It is anticipated that 700 people will receive AIS security training in FY 2003.

The Department also conducts computer security awareness training to ensure the confidentiality, integrity, and availability of its information. Pursuant to this duty, DS's customer support branch is responsible for the Computer Security Awareness Program. Computer security "awareness" is required for all employees because IT security is part of every employee's job, and awareness supports individual accountability. Thus, the program is designed to increase the awareness of all those in the Department who are permitted access to the systems.

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

4) Do plans of action and milestones reports account for all known security weaknesses*.*

Not all known security weaknesses are addressed by the Department's plans of action and milestones reports. For example, the Department's July 2002 update does not reflect security weaknesses identified by OIG in its February 2002 report on the Classified Connectivity Program. Nor does it address reported weaknesses in the Department's critical infrastructure protection program, among others. The Department uses a number of reporting vehicles to document and provide status of security vulnerabilities including project plans, working group reports, corrective action reports, corrective action plans, remediation reports, as well as plans of action and milestones reports. However, corrective action plans and plans of action and milestones are not currently integrated as a complete and comprehensive, single source for eliminating known and documented vulnerabilities for programs and systems within the Department.

2. For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

TABLE D.2: DEPARTMENT OF STATE CONTRACTOR OPERATIONS FACILITIES

		FY 2001	FY 2002
2a	Number of contractor operations.	16	23
2b	Number of contractor operations or facilities reviewed.	9	16

OIG did not evaluate the Department or CIO's handling of contractor or other agency information services provided to the Department. This area of interest will be included in the OIG's work for FY 2003 under the proposed Federal Information Security Management Act. The information shown in Table D.2 was provided by the CIO and has not been verified.

3. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If no, why not? Identify actual performance according to the measures and in the format provided below. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

TABLE D.3: RESPONSIBILITIES OF AGENCY CHIEF INFORMATION OFFICER

		FY 2003 Budget Materials	**FY 2004 Budget Materials**
3a	Number of capital asset plans and justifications submitted to OMB	22	In process
3b	Number of capital asset plans and justifications submitted to OMB without requisite security information and costs?	0	In process
3c	Were security costs reported for all agency systems on the agency's exhibit 53?	Yes	In process
3d	Have all discrepancies been corrected?	Unknown	Unknown
3e	How many have the CIO/other appropriate official independently validated prior to submittal to OMB?	22	In process

Note: 3a - Capital asset plan is under development.

OIG did not evaluate the extent to which the CIO has integrated security fully into the Department's capital planning and investment control process. However, as indicated in Table D.3, for FY 2003, the Department reports that all of its 22 capital asset plans and justifications were submitted to OMB with the requisite security information and cost. In this process, the CIO relies on the IT Investment Portfolio System, which provides a detailed breakdown of new and ongoing projects and initiatives. Starting in FY 2002, a new mandatory section includes planned and current security and privacy spending.