MEMORANDUM REPORT 01-IT-M-082 - REDACTED
Senior Management Attention Needed to Ensure Effective Implementation of the Government Information Security Reform Act
September 2001

In response to the Government Information Security Reform Act (GISRA), Public Law 106-398, the Office of Inspector General (OIG) performed an independent evaluation of the information security program and practices of the Department of State (Department). The Government Information Security Reform Act 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 our review was to determine whether the Department is effectively implementing key requirements of GISRA, including those pertaining to security planning and risk management, information security roles and responsibilities, training, and performance measures.

RESULTS IN BRIEF

OIG's evaluation of the effectiveness of the Department's information security program found mixed results. Specifically, OIG concluded that information security weaknesses continue to threaten Department operations, both here and abroad. Both OIG and Bureau of Diplomatic Security (DS) evaluation reports over the past 2 years identified weak information security management practices at dozens of overseas posts. For example, only 10 of the 35 posts in one geographic region reviewed by OIG security teams in 1999 and 2000 were reported to have adequate information security procedures in place. Further, according to OIG's survey questionnaire, although 59 percent of the Department's 371 systems are reported to have risk assessments, only 10 percent are reported to have security plans, as required by GISRA.

On the other hand, the Department has made progress in implementing a key GISRA provision—establishing the agency's Chief Information Officer (CIO) as the central management focal point for information security activities. In mid-August 2001, OIG provided the Department a draft of this report, which discussed our concern at that time that the Department's senior leadership had not agreed on what functional and organizational changes needed to be made to comply with the law. In response to the draft report, the Under Secretary for Management promptly reassessed the relative senior management roles and responsibilities of the Bureau of Information Resource Management (IRM) and DS in managing information security and directed actions consistent with GISRA requirements. Specifically, on August 20, 2001, on the recommendation of the Under Secretary for Management, the Deputy Secretary issued a Delegation of Authority to the CIO to administer the Department's information security program. The CIO's new role as the administrator of this program establishes the central management focus on information security that is required by the law and puts the Department in a better posture to protect its information technology assets from security risks. In its response to OIG's draft report, the Department stated that it believes that its actions will resolve the issues raised in the report, while recognizing that a number of details implementing the changes remain to be worked out over a 30-day period.

Although the Department has not developed performance measures for its information security program, which are required by both GISRA and the Government Performance and Results Act (Public Law 103-62), in response to a draft of this report, the Under Secretary for Management's office said that by October 15, 2001, IRM, working with DS, will develop measurable and meaningful performance measures for the Department's information security program. This is important because without useable performance measures, the Department is unable to assess the adequacy and effectiveness of information security policies and procedures. Further, it is hindered in its efforts to implement a results-based information security management program.

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 our government, the 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. The rash of cyber attacks launched in February 2000 against major U.S. firms and the global disruption caused by the "ILOVEYOU" virus in May 2000 illustrate the risks associated with this new electronic age.

Computer-supported government operations, including those at the Department, are also at risk. Previous OIG and DS reports have identified persistent computer security weaknesses that place a variety of critical and mission-essential Department operations at risk of disruption, fraud, and unauthorized disclosure. The Department has been able to close four material weaknesses previously reported under the Federal Manager's Financial Integrity Act of 1982 (Public Law 97-255), and it has been able to close all recommended actions resulting from a 1998 General Accounting Office (GAO) audit of information security (GAO 98-145). However, 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 the information security plan is practiced throughout all life cycles of the agency's information systems.

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

- designating a senior agency information security official who shall report 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 Inspector General or the independent evaluator performing a review may use any audit, evaluation, or report relating to 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 provides an overview of its management approach to information security in its FY 2001 Systems Security Program Plan (the Plan) issued in May 2001. The Plan—the first developed by the CIO and issued to the Department—was not revised to address requirements resulting from GISRA's enactment in late 2000 and does not reflect more recent changes and delegations of authority within the Department to meet GISRA requirements. However, the Plan establishes a baseline for the Department to build on in organizing its information security program. It identifies the authorities and fundamental principles guiding Information Technology (IT) security in the Department, outlines the roles and responsibilities of the Department's bureaus in the realm of IT, and briefly addresses the strategies for achieving and maintaining a desirable IT security posture for the Department. The Plan applies to all classified, unclassified, and sensitive but unclassified systems throughout the Department, its domestic bureaus, offices, annexes, and posts worldwide.

According to the Plan, three senior management officials have key roles in the implementation and governance of security policy. Specifically:

- The **Under Secretary for Management** is responsible for the control of all management resources, organizational structure, and assignment of functions within the Department.

- The **CIO** is the senior accountable official for IT security. The establishment of the CIO as the focal point for IT security in the Department is intended to facilitate the life cycle management of the Department's IT security program. This official is also the **Designated**

Approving Authority responsible for making risk acceptance determinations for information technology on behalf of the Department.[1] Based on mission criticality, the Designated Approving Authority may accept risk and grant either an approval to operate or an interim approval to operate if the system does not meet requirements. Also, the CIO promulgates IT security policy in concert with DS and oversees its implementation throughout the Department.

- The **Assistant Secretary for Diplomatic Security** serves as the principal adviser to the Secretary of State and the Under Secretary for Management on all security matters. DS is responsible for defining threat levels relevant to IT assets and for developing IT security policy and standards consistent with threat level, national policy, and the National Institute for Standards and Technology's guidelines in conjunction with the CIO. Also, the DS Deputy Assistant Secretary for Countermeasures and Information Security reports to the CIO on all matters regarding information security.[2]

According to the Plan, the CIO and DS need to work together to ensure that IT security is adequately developed and implemented throughout the Department.

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. In response to GISRA, OIG conducted a review with the specific objectives of: (1) identifying the Department's policies and procedures for securing information on its information systems; and (2) determining if the Department is in compliance with GISRA with regard to establishing and ensuring the effectiveness of controls over information resources.

To fulfill our review objectives, we developed two data collection surveys, which we used to obtain general information about the Department's information security program. Our first survey determined the Department's universe of systems. We sent a questionnaire to all identified system owners at the Department asking general information security questions. The owners were also asked to update the Department's list of information systems to the best of their knowledge. The second survey narrowed in on 16 major applications, facilities, and nodes[3] to the Department's infrastructure. Criteria for selection included: (1) mission criticality; (2) Presidential Decision Directive 63 identification;[4] and, (3) documentation availability. The

[1] On August 20, 2001, the Deputy Secretary of State delegated the Designated Approving Authority responsibilities to the CIO.

[2] On August 20, 2001, the CIO designated the DS Deputy Assistant Secretary for Countermeasures and Information Security as the Senior Agency Information Security Official. The Senior Agency Information Security Official reports directly to the CIO regarding the implementation and maintenance of the Department's information security program and security policies.

[3] Node—A system connected to a network.

[4] Presidential Decision Directive 63 established a national effort to ensure the security of the critical infrastructure of the United States. Under this Directive, the Department of State is responsible for protecting those of its facilities, people, and systems that it deems essential to the national critical infrastructure, and for being the Foreign Affairs Lead Agency.

questions in the questionnaire 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. We interviewed the owners of the 16 systems to collect documentation regarding their information systems security program. We did not independently verify the information collected from the two surveys.

To learn more about information system security at the Department, we reviewed OIG and DS inspection reports, the OIG Presidential Decision Directive 63 audit, and General Accounting Office reports on the Department. Our analysis grouped the recommendations in the OIG and DS inspections into five major categories to report on areas that need more attention at posts.

In the Department, we also interviewed officials in DS, the Foreign Service Institute, and the Bureaus of Financial Management and Policy, Information Resource Management, Consular Affairs, and International Narcotics and Law Enforcement Affairs regarding their efforts for securing their information systems.

We did not test the Department's information security controls during this evaluation, but instead relied on the results of previous OIG reviews, General Accounting Office reports, and DS inspections. Except as noted above regarding our use of data collection surveys, we followed generally accepted government auditing standards and conducted such tests and procedures as were considered necessary for the assignment. We obtained written comments on a draft of this report from the Department and revised the report where appropriate. The Department's comments are included in Appendix A. Staff from our Information Technology Division performed this evaluation from February 2001 through July 2001. Contributors to this report were Frank Deffer, James Davies, Tim Fitzgerald, Robert Taylor, Anthony Carbone, Sharon Hunter, Chris Watson, and Matthew Worner. 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.

AUDIT FINDINGS

DEPARTMENT INFORMATION SECURITY WEAKNESSES IDENTIFIED IN OIG AND DS EVALUATION REPORTS

OIG and DS evaluation reports in 1999 and 2000 identified information security weaknesses at the Department's overseas posts, as well as at headquarters in Washington, DC. Specifically, OIG reported on information security readiness at 35 overseas posts and on the Department's progress in implementing its Critical Infrastructure Protection Plan under Presidential Decision Directive 63. DS conducted 54 evaluations on information security at overseas posts between January 1999 and November 2000.

OIG Information Security Reports

In FYs 1999 and 2000, as part of its comprehensive security inspection efforts, OIG evaluated the information security programs and practices at 35 posts under the supervision of one geographic bureau. OIG consolidated the results of these reviews in its classified May 2001 capping report (01-SEC-R-005). The results of the OIG inspections, as indicated in the capping report, were mixed. OIG determined that 26 of the 35 posts inspected were adequately training their U.S. systems users. However, in terms of effective information security procedures, most of the posts fell short of Department standards. Specifically, only 10 posts had adequate (or better) information security procedures in place, 24 had minimal security procedures, and 1 was inadequate. OIG is currently following up on this report to determine the extent to which the problems identified have been resolved.

OIG identified additional weaknesses in the Department's management of information security in its June 2001 report[5] on critical infrastructure protection. 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. Specifically, OIG reported that the Department's:

- international outreach strategy is unnecessarily constrained, and, thus, does little to encourage the development of preventative measures needed to enhance global critical infrastructure protection;[6]
- critical infrastructure protection plan provided a suitable framework for addressing minimum-essential infrastructure. However, the plan falls short because it does not address potential cyber vulnerabilities in its foreign operations or in its interagency connections (i.e., such as between the Foreign Service National Payroll System and the Treasury Department); and
- policies and programs concerning information security training awareness were not sufficient to ensure that employees are properly trained to secure the agency's information systems.

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

[6] The Bureau of International Narcotics and Law Enforcement had responsibility for the critical infrastructure protection outreach strategy at the time of OIG's June 2001 report.

The OIG report contains a number of recommendations to strengthen the Department's approach to critical infrastructure protection planning. The recommendations include:

- 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 3 years;
- strengthening information security training policies and procedures through changes to appropriate sections of the *Foreign Affairs Manual*; and
- expanding the Department's international outreach approach to include a wide range of friendly countries requesting such assistance.

DS Information Security Reports

The Office of Information Security Technology in DS conducted 54 readiness evaluations on information security at overseas posts in 1999 and 2000. DS assessed the extent to which posts were complying with Department information security requirements in a number of key areas, including: (1) Security Program Planning and Management; (2) Access Controls Effectiveness; (3) Application Software: Installation, Development, and Storage; (4) Security of Operating System Software; and (5) Service Continuity Planning. The number of recommendations in each category is shown in Table 1 below.

Table 1
Summary of DS Computer Security Report Recommendations

Recommendation Category	Number of Recommendations		
	Unclassified	Classified	Combined
1. Security Program Planning and Management	149	16	165
2. Access Controls Effectiveness	580	153	733
3. Application Software: Installation, Development, and Storage	12	11	23
4. Security of Operating System Software	92	13	105
5. Service Continuity Planning	104	29	133
TOTALS	937	222	1159

Generally, DS reports on post information security readiness provide a mixed picture. DS made the fewest number of recommendations (23) in the area of Application Software:

Installation, Development, and Storage, which suggests that posts were managing this area with relatively few problems. DS made the largest number of recommendations in the area of Access Controls, namely 733, or more than 63 percent of all the recommendations it developed in the 2-year period. The specific problems DS found at posts in this evaluation area include:

- (REDACTED) ----------
- ----------

- ----------

- emergency power-off controls related to air conditioning in the computer rooms are inaccessible or not installed; and
- access privileges of each application user are not being reviewed by post supervisors annually to verify that the privileges originally granted are still appropriate.

According to DS, periodic compliance reviews of its reports have consistently shown that many of the reported issues are systemic in nature and require a change in culture of the Department's systems management and users to be resolved. Further, the Assistant Secretary for DS reported to OIG that in order to bring about this change, and add a strong element of accountability across all levels of users, DS is developing strategies to allow senior management to interject accountability into the information systems operations and management.

MIXED RESULTS FROM OIG'S INFORMATION SECURITY MANAGEMENT QUESTIONNAIRE

OIG developed two data collection surveys that were used to determine general information about the Department's information security program. The purpose of the first questionnaire was to identify the universe of systems operating throughout the Department and to obtain information on IT security plans, assessments, and determinations that are required by the OMB guidance, prior information security laws, and also by GISRA. Specifically, our first questionnaire included requests for information on the following:

- **Risk assessments—**The identification and analysis of possible risks in meeting the agency's objectives, which forms 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 entity's security program and policies and procedures that support it. The plan and related policies should cover 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—**Attests that an information system meets documented security requirements and will continue to maintain the approved security posture throughout its life-cycle.

- **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 our survey, the Department has 371 systems. Further, the survey indicates there is significant room for improvement in information security management throughout the Department. As Table 2 below indicates, nearly 70 percent of systems were reported to have security level determinations, only 10 percent were reported to have security plans, and just 5 percent were reported to have been certified and accredited. See Appendix B for detailed survey results.

Table 2
Department Survey Results:
Key Information Systems Security Elements

Department of State—OIG GISRA Questionnaire Results Summary Totals (Total Systems 371)		
	Number	**Percentage**
Systems with Risk Assessments	219	59%
Systems with Security Level Determinations	256	69%
Systems with Security Plans	38	10%
Systems Certified and Accredited	18	5%
Systems with Tested Security Controls	162	44%

Our second questionnaire focused on 15 of the Department's 83 mission-critical systems and 1 mission-critical asset (the Beltsville Information Management Center, SA-26).[7] We selected these systems based on the guidance from the Critical Infrastructure Assurance Office and related assessments. Specifically, our questions covered risk/vulnerability assessments, security level determinations, system security plans, certification and accreditation, and system

[7] Responses to OIG's first questionnaire reported 83 mission-critical systems out of the total of 371 systems identified.

security controls. Also, in our second questionnaire, we asked about personnel security, contingency plans, virus detection practices, hardware and software documentation, and incident response capability.

Overall, OIG's second survey questionnaire results were mixed. As shown in Table 3 below, while 75 percent of the systems reported having done a risk assessment, only 13 percent reported having a security plan in place, 44 percent reported that they had tested security controls, and only 31 percent reported that they had been certified and accredited.

Table 3
Mission-Critical System Survey Results

	Risk Assessment	Security Level Determined	Security Plans	Certified and Accredited	Tested Security Controls
American Citizen Services	Yes	Yes	No	No	No
CableXpress	Yes	Yes	No	No	No
Classified Network	No	No	No	No	No
Consular Lookout and Support System - Enhanced	Yes	No	No	No	No
Electronic Certification System	Yes	Yes	Yes	Yes	Yes
Foreign Service National Payroll System	No	No	No	No	No
Guard	Yes	Yes	No	Yes	Yes
INS Allocation Management System	Yes	No	No	No	No
Intelligence Research Information System	Yes	Yes	No	Yes	Yes
International Narcotics and Law Enforcement System	Yes	Yes	Yes	Yes	Yes
Open Sensitive but Unclassified Intra-Network	Yes	No	No	No	No
Overseas Financial Management System	No	No	No	No	No
Overseas Security Advisory Council Electronic Database	Yes	Yes	No	No	Yes
Principal Officers Executive Management System	Yes	Yes	No	No	Yes
State Annex 26	Yes	Yes	No	Yes	Yes
State Transportation and Tracking System	No	No	No	No	No
TOTAL YES (PERCENTAGE)	**75%**	**56%**	**13%**	**31%**	**44%**

On a more positive note, Table 4 below shows that 100 percent of the systems reported having an incident response capability, 94 percent reported an active virus detection program, 88 percent reported having necessary hardware and software documentation, and 69 percent were reported to have accurate position security reviews.

Table 4
Mission-Critical System Survey Results

	Accurate Security Position Description	Contingency Plans Tested and Updated	Automatic Virus Detection	Hardware and Software Documentation	Incident Response Capability
American Citizen Services	Yes	No	Yes	Yes	Yes
CableXpress	No	No	Yes	Yes	Yes
Classified Network	Yes	No	Yes	Yes	Yes
Consular Lookout and Support System - Enhanced	Yes	Yes	Yes	Yes	Yes
Electronic Certification System	Yes	No	Yes	Yes	Yes
Foreign Service National Payroll System	Yes	No	Yes	Yes	Yes
Guard	Yes	No	No	Yes	Yes
INS Allocation Management System	Yes	No	Yes	Yes	Yes
Intelligence Research Information System	No	No	Yes	Yes	Yes
International Narcotics and Law Enforcement System	Yes	Yes	Yes	Yes	Yes
Open Sensitive but Unclassified Intra-Network	Yes	No	Yes	No	Yes
Overseas Financial Management System	Yes	No	Yes	Yes	Yes
Overseas Security Advisory Council Electronic Database	No	Yes	Yes	Yes	Yes
Principal Officers Executive Management System	No	Yes	Yes	Yes	Yes
State Annex 26	Yes	No	Yes	Yes	Yes
State Transportation and Tracking System	No	No	Yes	No	Yes
TOTAL YES (PERCENTAGE)	**69%**	**25%**	**94%**	**88%**	**100%**

Recommendation 1: We recommend that the Chief Information Officer in coordination with the Bureau of Diplomatic Security develop a strategy and timetable for ensuring that all of the Department's systems/applications address each of the key system security elements identified in

the tables above. This strategy and timetable should be completed by October 15, 2001, in order for it to be included in the Department's information security remediation plan, which is due to the Office of Management and Budget by October 31, 2001.

PROGRESS MADE IN THE DEPARTMENT'S REASSESSMENT OF INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Managing the increased risks associated with a highly interconnected computing environment demands increased central coordination to ensure that weaknesses in one part of the organization do not place the entire organization's information assets at undue risk. Further, centralized information security management can help ensure that: (1) information security risks are considered in both planned and ongoing operations; and (2) senior management is fully informed about security-related issues and activities affecting the organization. Toward that end, GISRA establishes the agency's CIO as the central management focal point for information security activities. In addition to modifying existing requirements, GISRA adds new requirements to the Department's information security programs—all of which require a reappraisal of information security management throughout the agency. The Department has made progress in assessing information security roles and responsibilities, and has taken action to meet GISRA requirements; however, a number of details remain to be worked out to ensure full and effective implementation of the law.

In mid-August 2001, OIG provided the Department a draft of this report, which discussed its concern that the Department's senior leadership had not agreed on what functional and organizational changes need to be made to comply with the law. OIG recommended that the Under Secretary for Management assess the Department's organizational structure for managing information security and identify the changes needed to comply with GISRA. In response to the issues raised in the draft report, the Under Secretary for Management promptly reassessed the relative senior management roles and responsibilities of IRM and DS in managing information security and directed actions consistent with GISRA requirements. Subsequently, on August 20, 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;
- The CIO designated the Deputy Assistant Secretary for Countermeasures and Information Security as Senior Agency Information Security Official. This official will report directly to the CIO regarding the implementation and maintenance of the Department's information security program and security policies; and
- The Under Secretary for Management designated the CIO as the designated approving authority, responsible for making risk acceptance determinations for information technology on behalf of the Department.

The Department believes that these actions will resolve the issues raised in OIG's draft report regarding the agency's information security program. The Department also recognizes that further details implementing the new organizational arrangement remain to be worked out.

The Department's current operating approach to information security roles and responsibilities grew out of its response to a May 1998 General Accounting Office report[8] that outlined major information security weaknesses in the Department. The General Accounting Office recommended that the Department establish a central information security unit to facilitate, coordinate, and oversee information security in the Department. In January 2000, the Under Secretary for Management issued a memorandum that: (1) named IRM as the authority for the Department's information security program; and (2) designated DS as responsible for developing information security policy, with promulgating authority held jointly by DS and IRM. Further, the memorandum laid out agreed-upon roles and responsibilities for DS and IRM in four areas: IT security policy and implementation; information security awareness; monitoring and evaluation; and risk assessments. This memorandum was superseded on August 20, 2001, by the Deputy Secretary of State's delegation to the CIO of the authority to administer all functions under GISRA.

Under GISRA, many of the existing roles and responsibilities regarding information security management remain unchanged. For example, DS will continue to: provide worldwide computer security support; provide computer security training for security officers and systems staff; and act in an advisory capacity to the CIO on IT security issues. IRM will continue its virus protection role and operational monitoring of Department networks. However, the law and the recent delegation of authority to the CIO significantly expand the role of the CIO in managing the Department's information security program. With the reporting relationship now established between the DS Deputy Assistant Secretary for Countermeasures and Information Security and the CIO, relative roles and responsibilities are being institutionalized. Specifically in line with GISRA requirements, the CIO now has the delegated authority to administer all information security functions, including:

- designating a senior agency information security official who shall report 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;
- training and overseeing personnel with significant responsibilities for information security; and
- assisting senior agency officials concerning information security aspects of their respective program areas.

The CIO's new role establishes the central management focus on information security that is required by the law and puts the Department in a better posture to protect its information technology assets from security risks.

These new CIO responsibilities may necessitate additional organizational changes within the Department as demonstrated by the CIO's designation of the DS Deputy Assistant Secretary for Countermeasures and Information Security to be the Department's Senior Agency Information Security Official. This designation requires the incumbent DS Deputy Assistant

[8] *Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations*, GAO/AIMD-98-145, May 1998.

Secretary to report directly to the CIO regarding the implementation and maintenance of the Department's information security program and security policies. These newly-created, cross-bureau responsibilities may require a reallocation of information security resources to support the CIO. For example, the requirement that the CIO have responsibility for developing and maintaining the Department's information security program may require the transfer of specific policy and planning resources from DS to IRM.

Recommendation 2: We recommend that the Under Secretary for Management ensure that the Bureaus of Information Resource Management and Diplomatic Security resolve any remaining issues regarding the establishment of the Chief Information Officer as the Department's central management focal point for information security and the appointment of a Senior Agency Information Security Official. This effort should include an assessment of both the resources and the reporting structure needed to support the newly-delegated Chief Information Officer authorities and responsibilities. This completed effort should be included in the Department's information security remediation plan, which is due to the Office of Management and Budget by October 31, 2001.

Department Response

In commenting on a draft of this report (see Appendix A), the Department states that it has assessed its organization and made determinations that will resolve the issues raised in the report regarding the Department's information security program. The Department cites its recent actions (discussed above) as evidence that the Department is now complying with GISRA. Further, the Department states in its comments that it does not agree that Recommendation 2 should remain in the report.

OIG Comment

We agree that the Department's recent actions to assign roles and responsibilities over its information security program represent significant progress toward GISRA compliance, and we have revised our draft report accordingly. We also agree that Recommendation 2 should not remain as it was originally drafted; however, there are a number of significant details that need to be addressed in order fully to implement the recommended changes to the agency's information security program. For example, the Department needs to determine the extent to which organizational resources may need to be transferred between DS and IRM, as a result of GISRA requirements. Further, the Department needs to assess how the specific DS and IRM roles and responsibilities established by the January 2000 memorandum need to be revised in order to comply with GISRA. In its response to our draft report, the Department acknowledges that further details need to be worked out and it pledges to complete that work within 30 days. Because of these outstanding issues related to the Department's efforts to implement GISRA, we have revised Recommendation 2 to reflect the need for the Under Secretary for Management to continue his oversight of DS and IRM efforts to resolve these issues by October 31, 2001.

INFORMATION SECURITY TRAINING

Training is a key element in reducing risk and enhancing the Department's risk-based management approach for IT security. The Department of State's FY 2001 Systems Security Program Plan recognizes the importance of training and notes that the most comprehensive and logical IT security program will prove ineffective in the absence of adequate and regularly scheduled education and awareness efforts. It goes on to state that education and awareness efforts ensure that users, IT professionals, managers, and senior executives understand and appreciate both the complexity of this discipline and also its unique contribution to the success of overall IT security efforts. We found that the Department conducts information security training at all user levels, carries out an aggressive awareness program, and supports a complete range of computer-based training tools. As shown in Table 5 below, DS has provided training to more than 13,000 employees in the past 3 years to support information assurance and security.

Table 5
EMPLOYEES TRAINED BY DS:
IN SUPPORT OF INFORMATION ASSURANCE AND SECURITY

	Domestic End Users	Overseas End Users	Executive Management	Totals
FY1999	**2232**	**1638**	**778**	**4648**
FY2000	**2481**	**1820**	**865**	**5166**
FY2001	**1861**	**1315**	**649**	**3825**
Total number of personnel trained in FY 1999-2001				**13,639**

However, the results of our evaluation show that adjustments in training curriculum could further improve the Department's training program and thereby reduce additional risk through better understanding and awareness. For example, we were informed that inclusion of IT security in the Department's Managing State Projects curriculum would require minor revision that would improve the Department's management of information systems security projects. All Department project managers are encouraged to take this 5-day intensive workshop, which, according to the Foreign Service Institute course guide, provides a solid entry into the field of project management.

CIO NEEDS TO DEVELOP INFORMATION SECURITY PERFORMANCE MEASURES

OIG found that the Department has not developed information security performance measures to support strategic goals—key requirements of both the Government Performance and Results Act and GISRA. Two important Government Performance and Results Act factors in establishing measures are that each performance measure should be an indicator mainly used by managers as they direct and oversee how a program is carried out, and should help managers respond when problems arise. Without meaningful and measurable performance measures, the

Department will be unable to assess the adequacy and effectiveness of information security policies and procedures effectively; further, it will be hindered in its efforts to implement a results-based information security management program.

In response to a draft of this report, the Under Secretary for Management's office has directed that IRM and DS incorporate Government Performance and Results Act requirements into their GISRA compliance efforts. According to the executive assistant to the Under Secretary for Management, information security performance measures are to be established prior to October 15, 2001.

Recommendation 3: We recommend that the Chief Information Officer ensure that program managers develop and use Government Performance and Results Act and Government Information Security Reform Act performance measures in support of the Department's information systems security program.

Bureau of Populations, Refugees, and Migrations	2	0	0%	0	0%	0	0%	0	0%	0	0%
Office of the Secretary	75	75	100%	75	100%	0	0%	0	0%	74	99%
Totals	**370**	**219**	**59%**	**256**	**69%**	**38**	**10%**	**18**	**5%**	**162**	**44%**

DEPARTMENT COMMENTS

S/S 200118364

United States Department of State

Washington, D.C. 20520

August 20, 2001

MEMORANDUM

TO: OIG - Clark Kent Ervin

FROM: M - Grant S. Green

SUBJECT: Comments concerning OIG draft report 01-IT-M-082 - *Senior Management Attention Needed to Ensure Effective Implementation of the Government Information Security Reform Act*

Thank you for the opportunity to comment on the subject OIG report. I have reviewed the report along with my staff and I do not agree that Recommendation 2 should remain in the report. I have assessed the Department's organization and have made determinations which I believe will resolve the issues raised in your report regarding the Department's information security program.

Attached you will find a Delegation of Authority from the Deputy Secretary of State to the Chief Information Officer. The Delegation of Authority, written by the Office of the Legal Adviser, brings State into compliance with GISRA. As discussed in the accompanying Action Memorandum, DS and IRM have also resolved how best to allocate and perform their respective responsibilities within the context of this new delegation. This includes identifying the CIO as the Designated Approving Authority vice the Under Secretary for Management. In addition, the CIO has designated the DS Deputy Assistant Secretary for Countermeasures and Information Security as the Senior Agency Information Security Official, who will report directly to the CIO regarding the implementation and maintenance of the Department's information security program and security policies.

Any further details of implementing this new organizational arrangement will be fleshed out within the next thirty days between the Bureaus of Information Resources Management and Diplomatic Security under my direction and we will advise your Office of Information Technology Issues accordingly.

DEPARTMENT COMMENTS

Once again, thank you for the opportunity to react to this draft OIG report. I have also asked my staff to make suggested changes (attached) on the sections of your draft report pertaining to the Delegation of Responsibilities which has now been accomplished.

Attachment:
Memorandum of Delegation to the CIO.
Suggested Revisions to 01-IT-M-082.

Office of Inspector General – 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[9]	55	8	15%	39	71%	5	9%	4	7%	4	7%
Bureau of Consular Affairs	36	23	64%	8	22%	0	0%	2	6%	1	3%
Bureau of Diplomatic Security	51	46	90%	47	92%	0	0%	1	2%	46	90%
Bureau of East Asian and Pacific Affairs	1	0	0%	0	0%	0	0%	1	100%	0	0%
Bureau of Educational and Cultural Affairs	40	30	75%	32	80%	12	30%	0	0%	0	0%
Bureau of European Affairs	5	0	0%	0	0%	0	0%	0	0%	0	0%
Bureau of Financial Management and Policy	22	2	9%	1	5%	2	9%	1	5%	3	14%
Foreign Service Institute	2	0	0%	2	100%	0	0%	0	0%	2	100%
Bureau of Human Resources	20	4	20%	18	90%	6	30%	1	5%	19	95%
Bureau of International Narcotics and Law Enforcement Affairs	1	1	100%	1	100%	1	100%	1	100%	1	100%
Bureau of Intelligence and Research	3	2	67%	3	100%	2	67%	1	33%	1	33%
Bureau of International Organization Affairs	2	2	100%	2	100%	0	0%	0	0%	0	0%
Bureau of Information Resource Management	29	12	41%	11	38%	7	24%	3	10%	2	7%
Office of the Legal Adviser	5	0	0%	0	0%	0	0%	0	0%	0	0%
Office of Medical Services	3	3	100%	3	100%	3	100%	3	100%	3	100%
Bureau of Nonproliferation	2	0	0%	2	100%	0	0%	0	0%	0	0%
Bureau of Oceans and International Scientific Affairs	5	5	100%	5	100%	0	0%	0	0%	0	0%
Office of Inspector General	6	5	83%	6	100%	0	0%	0	0%	6	100%
Bureau of Public Affairs	5	1	20%	1	20%	0	0%	0	0%	0	0%
Bureau of Populations, Refugees, and Migrations	2	0	0%	0	0%	0	0%	0	0%	0	0%
Office of the Secretary	75	75	100%	75	100%	0	0%	0	0%	74	99%
Totals	**370**	**219**	**59%**	**256**	**69%**	**38**	**10%**	**18**	**5%**	**162**	**44%**

[9] The 56 systems shown for the Bureau of Administration is 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 office, titled Overseas Building Operations, reporting directly to the Under Secretary for Management.