

Statement by  
Bruce F. Morrison  
Chief Information Officer, Acting  
United States Department of State

Before the  
House Government Reform Committee  
Subcommittee on  
Technology, Information Policy, Intergovernmental  
Relations  
and the Census

Hearing on  
*Cyber Security: The Status of Information Security  
and the Effects of the Federal Information System  
Management Act (FISMA) at Federal Agencies*

June 24, 2003

Good Morning Mr. Chairman and Members of the Committee. I am honored to be here and appreciate the opportunity to discuss with you the solid performance, recognized progress and renewed vigor during the past year in the area of information security at the Department of State. We take seriously the oversight role your Subcommittee provides in ensuring the integrity of cyber security in these challenging times.

### **Summary**

While we are not yet where we would like to be in relation to cyber security, we are pleased to come before you to report on the initial stages of improving our program. Today we will highlight the measurable progress we have made so far.

Traditionally, the world of diplomacy is slow and deliberative by nature. However, in the area of Information Technology, that is not the case. Let me underscore that Secretary Powell considers Information Technology a strategic component in implementing U.S. foreign policy. Protecting our information assets and cyber security is paramount to his agenda. In concert with Under Secretary for Management Green, we have committed substantial resources to meet our challenges. We established an Information Assurance office now headed by a senior officer.

What began as a mandate under the Government Information Security Reform Act (GISRA) has since become a challenge that we now fully embrace. In line with the Federal Information Security Management Act (FISMA) requirements and in close consultation with OMB, we conducted an independent assessment of the Department of State's information security environment. We began by doing something that might sound simple, but which is a major challenge for all USG agencies in the ever-developing E-Government world: clearly defining requirements and objectives. We adhered to OMB's definition of what constitutes a general support system versus a major application versus an application, then we conducted a thorough inventory and analysis of all Department IT assets to categorize them and set priorities for analysis and possible remedial action. Of those, 154 are now categorized as major applications or general support systems.

We are making steady IT security progress through effective management, implementation, evaluation and remediation when necessary. To complement this effort, we meet regularly with the Department's Office of the Inspector General -and address

information security issues and potential problems. Equally critical, we have an enhanced cooperative arrangement with the Bureau of Diplomatic Security, which has delegated responsibilities for significant portions of our information security program. Together, the Assistant Secretary for Diplomatic Security and I have identified our mutually supportive roles and outlined our joint strategy to meet our own critical security enhancement imperatives and OMB's aggressive time schedule.

## Measurable Progress

Our recent results in improving information security under FISMA are significant and measurable.

The flagship of our new cyber security efforts is the Systems Authorization Program, more commonly referred to as Certification and Accreditation or simply C&A. In agreement with OMB, our goal is to certify and accredit all existing and emerging systems by September 2004. We have recently embarked on this critical program element and have set monthly targets for authorizations. We plan to have 50 systems, one-third of the total, accredited by the end of FY 2003.

While complex and involved, the quarterly Corrective Action Plan process enables the Department to report on IT security performance indicators and remediation Plans of Action and Milestones (POA&Ms). We have submitted improved POA&Ms the last two quarters.

As you know, these two tools -- C&A and POA&Ms - are major contributors to the President's Management Agenda (PMA) e-Gov score assigned by OMB. I am pleased to report that, over the past three quarters we have moved from "red" to "yellow" to "green" in the progress category and our goal is to move through "yellow" to "green" for status by July 1, 2004.

### **I. State's Cyber Security Program**

The Cyber Security Program at the Department of State is a strategic, layered approach to comprehensive risk management of our information and information assets. In compliance with FISMA, the Department had an independent assessment by the National Institute of Standards and Technology (NIST) review our cyber security program earlier this year and are melding their excellent recommendations into State's security action plans and practices.

Information Assurance has three pillars: - Confidentiality, Integrity and Availability. We recognize that there must be a balance between IT security and business efficiency. Therefore, our approach is based on two tenets:

- Risk must be assessed and reduced to an acceptable level, but cannot be completely -eliminated; and,
- The budget and business needs of the employees must be considered in making risk management decisions.

No single security protection methodology can resist all forms of attack. Using a layered risk management security strategy affords multiple levels of defense and protection -- operational, technical and managerial.

Turning to the operational side, we have made solid strides in operational security and considerable progress in the areas of IT Security Awareness, Training and Education. To heighten cyber security awareness, executive directors report on IT security progress in their quarterly POA&Ms submission to the CIO. According to their reports, approximately 60% of the Department's employees have participated in information security training and/or awareness.

We have maintained a strong perimeter defense by applying standard technical solutions - Firewalls, AntiVirus protection and Intrusion Detection Systems.

I cannot stress enough that cyber threats to the Department are increasing due to the rapid proliferation of technology and the related vulnerabilities created by heavy reliance on emerging technologies and information systems.

In response to the heightened probability of attacks from individuals and groups with malicious intent, including terrorism, State's Virus Incident Response Team (VIRT) has continued to improve technology, process and Department-wide awareness.

Since January of this year, our team has eradicated 155,393 malicious codes. Top viruses included Klez.H, Yaha, Bugbear, Sobig and Lirva. In our VIRT "Home Use Give Away" program, we distributed over 9,000 CDs both domestically and overseas.

The Department of State has played a leading role in the government-wide E-Authentication initiative. Not only will it provide physical access, but also it will be the platform for digital identity and signature. This is a critical element of our forward thinking security and authentication posture and is vital for the protection of our information technology enterprise. To date, approximately 13,000 employee records with photographs have been created while another 10,229 Smart ID Cards are printed and being prepared for distribution by Diplomatic Security. Of those, 2,363 Smart ID Cards with Public Key Infrastructure (PKI) certifications have been distributed to employees.

As part of a continuing effort to ensure the security of the Department's critical infrastructure, the Department deploys a layered defense-in-depth capability. The strategy includes a detect, react and respond approach that emphasizes the analytical capability inherent in the program. Components of this methodology include a 24x7 Network Monitoring Center, a Computer Incident Response Team (CIRT), State's first line of defense, and a Cyber Threat Analysis Cell (CTAC), State's cyber threats think tank.

The Intrusion Detection System (IDS) program enables monitoring and auditing of network and host information systems, thereby, detecting inappropriate, incorrect or anomalous activity. IDS sensors are monitored on a 24x7 basis to protect Department networks against outside penetration, compromise or misuse. Alerts are generated for each possible unauthorized access event. Most recently, the IDS program has been enhanced this fiscal year by the deployment of 298 sensors to the Classified Network at 105 posts.

The Computer Incident Response Team (CIRT) is the focal point for reporting computer security incidents on Department and foreign affairs agency networks. CIRT reports are created and disseminated to senior management as well as security and operations managers. As required, CIRT coordinates with other government agencies to ensure and support needs for criminal prosecution.

CIRT provides computer security incident reports for both internal and external use to be included in the Federal Computer Incident Response Center (FedCIRC). Most recently, on June 17, we signed a Memorandum of Understanding with FedCIRC to formalize our information sharing arrangement. CIRT also participates in the quarterly FedCIRC Partners meetings where federal incident response teams, law enforcement, private sector representatives, academia, and federal agencies responsible for securing the National Information Infrastructure exchange ideas and discuss technical issues.

For example, in the first eight months of FY 2003, the Department had a total of 720 events reported to the CIRT include 557 originating from externally from the Department. Of those 720, 708 of the reports were deemed unsuccessful attempts. The remaining twelve were elevated to "incidents," two were reported to the FedCIRC, as they were of particular interest to the global Federal IT community.

Let me highlight additional accomplishments of the CIRT. During FY 2003, CIRT successfully implemented the use of a hardware/software tool that greatly enhances their ability to analyze network security events. CIRT also provides daily cyber threat information to senior department management and submits a weekly activity report to senior management outlining attempted network intrusions and resolutions.

We are taking a proactive stand as the United States is confronted with increasingly sophisticated computer network attack and information operations capabilities from its adversaries. To address these issues, the Cyber Threat Analysis Cell (CTAC) provides overseas posts and Department management with indications, warnings, descriptions, and diagnoses of threats to the Department's critical cyber infrastructure.

Building out from this strong infrastructure, we have numerous IT programs underway that directly contribute to the security of our information assets. Most recently, we completed "OpenNet Plus," one of our largest IT projects that enables secure desktop access to the Internet to the Department's over 43,000 users. This project was significant from a security point of view in that we ensured all Department domains met basic password and configuration guidelines. In addition, the project routed all Internet access through a central firewall, thereby reducing the risk of having to put individual firewalls in over 300 locations.

Using a similar implementation approach, our Classified Connectivity Program (CCP) provides secure access to our Foreign Service officers and other agency colleagues in over 220 posts around the world. This project is on budget and on schedule for completion by September 30 of this year.

While State has constructed a robust technical defense and solid operational procedures, a number of mechanisms are underway to complement our cyber security program. We have undertaken an ambitious outreach effort.

Senior Agency Information Security Official (SAISO)

The formation, funding and staffing of the Office of Information Assurance is underway. Under the FISMA requirements, I am designating a Senior Agency Information Security Official (SAISO) who will report directly to me. Let me note that the term Chief Information Security Officer (CISO) is used interchangeably with SAISO.

### Coordination with the Office of the Inspector General

The cooperation between my office and the Office of the Inspector General is very constructive. - We meet bi-weekly to discuss plans, programs and problems. The meetings over the past six months have revolved around IT systems inventory, systems authorization and FISMA compliance. The OIG has been and continues to be briefed at the various stages of the Systems Authorization Project. The OIG was thoroughly briefed at various stages of the Systems Authorization Plan development. Other presentations have included the CISO's (used interchangeably with SAISO) FISMA mid-term assessment and the POA&Ms process

### Cyber Security Advisory Group

For this effort to accomplish its target, a bi-weekly meeting with senior representatives from Management, Management Policy, E-Diplomacy, Resource Management and Diplomatic Security is held. While the initial focus was on C&A, the scope of the session has been broadened to encompass discussions on the wide range of information security issues.

### IA Forum

For the Cyber Security Program to be effective, everyone at the State Department needs to be involved. We initiated a monthly IA forum to brief Department system managers on Information Assurance plans, programs and processes. Not only has this improved overall awareness and contributed to the participation of agency components in complying with OMB reporting requirements, but also this has served to be a sounding board for potential issues on the horizon.

### Internal Synergy

We realize for the Department to succeed, we must work collectively, across Bureau lines, to ensure that the Department's critical infrastructure is protected. We must leverage the full complement of talent available to us to guarantee the Department's critical infrastructure is protected. We have redesigned our processes to align them to E-Government requirements and to ensure that the Chief Financial Officer and the Chief Information Officer speak with one voice on IT security. OIG inspections, audits, and reviews verify that processes in place are performing as expected.

Our existing network monitoring, threat detection and response, cyber analysis, incident reporting and education and awareness suite of services insures strong synergy within the Department. For example, the Computer Incident Response Team (CIRT) must rely on the Bureau of Information Resource Management's (IRM) firewall team to have the capability to identify external threats. Together, they evaluate and block suspicious IP addresses that may

adversely affect the Department's networks. Similarly, the CIRT and Cyber Threat Analysis Center (CTAC) work hand-in-glove with IRM's Virus Incident Response Team to respond to malicious events and to maintain a high state of anti-virus readiness. The DS Training Center has developed a series of computer security training courses for all Information System Security Officers.

#### Formation of Cyber Security Specialists Corps

We appreciate your support in providing the resources for cyber security. With the increasing requirements for increased cyber security, we believe the role of Information System Security Practitioners is pivotal in supporting the Cyber Security process both here and abroad. As noted in the OIG's report, Information System Security Officers (ISSOs) overseas do not spend adequate time on ISSO functions; rather IT security duties are viewed as collateral.

To help resolve these issues, we are conducting a study on ways to create a corps of cyber security professionals. Regional bureau executive directors welcome the upcoming study. To further encourage sufficient security practitioners with the appropriate skill set, the Skills Incentive Pay for IT security credentials is being raised.

Meanwhile, the Department is working to enhance its field expertise through the Regional Computer Security Officer (RCSO) program. This program provides timely computer security support and "hands-on" assistance to posts worldwide. RSCO are Foreign Service security engineering officers responsible for ensuring that classified and unclassified networks are installed and maintained according to current Department and U.S. Government security regulations. They provide on-site computer security customer support, training, oversight, and revaluations of unclassified and classified networks.

## **II. Actions to Remedy the deficiencies reported in September 2002 GISRA report**

In the interest of fully addressing the issues, the following paragraphs summarize deficiencies identified in OMB's May report to Congress and progress made by the Department in addressing these deficiencies.

*1. Security funding.*

*Last year's report indicated that State's IT security funding amounted to approximately 22% of the IT budget.*

This figure, more than double industry figures, is based on estimates. In FY 2003, the Office of Information Assurance (IA) has worked closely with the Office of Architecture and Planning's Capital Investment group to develop guidelines for IT security investments. Training has been provided to those filling out IT submissions and the Office of Information Assurance has reviewed all submissions.

Training, management and oversight of the IT Security aspect of IT Capital planning is underway and will be assessed. Furthermore, IA involvement with the newly formed e-Gov Board Advisory Committee and participation in the e-Gov Board Working Group will ensure that IT security considerations are an important factor - in IT investment decisions.

*2. Number of systems reviewed.*

Adhering to OMB's definitions, we have created a single inventory of the Department's IT systems.

In close consultation with the OIG, we expect the official inventory number to be 154 for this year's FISMA reporting. Let me caution that the actual number of systems and to which category they belong continues to change as detailed meetings are held with the bureaus in the pre-certification phase of systems authorization.

*3. Material weaknesses.*

*A) In FY 2001, the IG identified a material weakness in the Department's lack of Certification and Accreditation of its information systems.*

A C&A plan, with timetable, has been developed, and was presented to OMB in March 2003. Department funding was made available in April.

By the end of June 2003, we expect 18 systems to have undergone the process. Our goal is to authorize one third of major applications and general support systems by August 2003 and 100% by August 2004.

*B) According to an IG survey questionnaire, only 15 percent of the Department's systems had security plans.*

A requirement of the pre-certification phase is a current Systems Security Plan (SSP). We have developed a template for the SSP development. During the initial C&A cycle, this will help systems managers with SSPs as required as they undergo C&A.

*C) The IG found a significant weakness in information security management at overseas missions. Specifically, the IG determined that the information systems security officers (ISSO) generally were not performing all the requisite duties of the position.*

IT security work typically constitutes collateral duties of those designated as ISSOs. Many managers place more emphasis on other responsibilities. We believe awareness and training will solve this problem. To alleviate this, the Bureau of Diplomatic Security (DS) training center has developed a suite of role-based IT security courses with distinct audiences in mind such as the security practitioner, the IT professional, and most recently, the manager at all levels. Additionally, cyber security is being added to the Foreign Service Institute's summer training session for Administrative Officers.

*D) The IG reported that State had made some progress in assessing information security at missions and bureaus as part of its implementation of OpenNet Plus, the Department's program to provide worldwide desktop Internet access to its employees. Missions must show that they comply with existing security standards prior to receiving Internet services from OpenNet Plus. As of September 3, 2002, 20 bureaus and 84 missions had met the requirements of independent verification and validation (IV&V) of their respective IT infrastructures indicating compliance with the Department's IT security configuration and have subsequently been connected to OpenNet Plus.*

The OpenNet Plus project was completed in May 2003 with the connection of over 43,000 users at over 300 overseas posts and domestic offices.

*E) Lack of information security performance measures to support strategic goals.*

In August 2002, the CIO issued IT security performance measures to the executive directors of all bureaus based on OMB GISRA guidance. New performance measures will be issued when OMB releases FISMA guidance. In FY 2004, the CIO will reformulate and reissue general performance measures and will specifically target overseas missions as well as domestic bureaus.

*F) Weaknesses in the critical infrastructure protection program that have not been addressed.*

State has adopted an alternative to Project Matrix - the State Secure Infrastructure Management Systems (SSIMS). SSIMS is an efficient, cost effective alternative that meets State's information security and global access requirements. The Department's Critical Infrastructure (CIP) Governance Board has approved the SSIMS project plan and equipment for the pilot. Once tested and relational databases populated, SSIMS will be hosted on SIPRNET where the data can be used and shared at the secret level.

The Undersecretary for Management (M) in April 2002 reinvigorated the Critical Infrastructure Protection (CIP) Governance Board and appointed the Assistant Secretary for Resource Management as chairman. This Board consists of other Assistant Secretaries and Directors under the "M" family (Human Resources, Consular Affairs, Administration, Resource Management, Information Resource Management, Diplomatic Security and the Office of Overseas Building Operations as well as regional and functional bureaus.

The CIP Governance Board has aligned CIP remediation efforts with the Department's budget and planning process to achieve CIP objectives. The board has moved all Tier 1 and 2 CIP remediation priorities from "red" to "green" in just one year. This includes our top priority of establishing redundant communications capabilities at the Department's new alternate communications site. This effort was completed in less than a year and under budget.

The draft CIP plan was presented to the CIP Governance Board in April for review and bureau specific changes. The final plan will be presented to the Governance Board in August.

### *G. Financial Systems Reporting*

*The Department had its 2001 and 2002 financial statements audited by an independent auditor at the direction of the IG. This independent auditor cited a "material weakness" for the Department's information systems security for networks in domestic operations.*

The auditor identified four areas to be addressed to resolve the weakness:

#### *1) Certification and Accreditation*

*All new systems and applications are thoroughly vetted by the Bureau of Diplomatic Security for security and information assurance before installation and use.*

The Department has initiated a comprehensive Systems Authorization Plan, encompassing Certification and Accreditation which subjects all general support systems and major applications to a consistent, standardized, measurable and repeatable systems authorization process, including a thorough review of access controls. This plan was recently presented to the President's Office of Management and Budget (OMB), and OMB advised the Department that from its initial review of this plan, it was pleased with the plan.

#### *2) Penetration Testing*

*An ongoing, cyclical program of vulnerability assessments for all systems including penetration testing.*

Both the general support systems and the major financial systems are categorized at NIST SP 800-37 Security Classification Level 3 which means they will be submitted to penetration testing during C&A.

#### *3) Patch Management*

*Patches are installed on a real-time basis.*

An effective Patch Management program is essential for both IT Security compliance with FISMA and the Department's controls over its financial systems as addressed by the independent auditor.

In January of this year, the CIO took over operation of the Department's Patch Management program from the Bureau of Diplomatic Security. As Department needs to expand and strengthen its patch management capability, we are embracing the use of FedCIRC's Patch Authentication and Dissemination Capability (PADC) tool as the centerpiece of a new, more robust patch management program. Policy

is being developed, based upon NIST SP800-40, to support this strengthened program and the Office of Enterprise Network Management is planning the operational structure. While an earlier request for supplemental funding to support this initiative was unsuccessful, I intend to revisit this in the near future. Once in place, the improved patch management capability will significantly strengthen our defense-in-depth IT security posture by reducing the vulnerabilities presented by the implementation of defective software.

#### 4) Remediation of Weaknesses

*Management respond to and expeditiously corrects findings and weaknesses identified in vulnerability assessments and penetration tests.*

As part of the penetration-testing program, rapid mitigation actions have been taken to address several issues in the past, and will continue to be available if appropriate and necessary in the future.

At the June 12, 2003 meeting of the Management Controls Steering Committee - the CIO, at the suggestion of the IG, presented a potential reportable condition on IT security. The Committee determined that there was considerable oversight from the Under Secretary for Management and the OMB on IT security and that one more layer of oversight would not be effective. The issue was tabled until the September meeting when the CIO will provide a status report.

The major financial application Regional Financial Management System (RFMS) has recently completed its certification phase of the C&A process. Five of six critical findings have been corrected and 55 of 60 other findings have been remediated. The application is now in final risk assessment and I expect to make an accreditation decision this month.

#### *4. Systems Authorization*

*The IG reported on system certification and accreditations. During FY 2002, the Under Secretary for Management mandated the Department-wide implementation of the National Information Assurance Certification and Accreditation Process (NIACAP) in a timely and efficient manner. The Under Secretary approved the DS and IRM roadmap for implementing this plan.*

The C&A program was initiated in mid-2003. The roadmap was completely revised and the C&A process is a blend of NIACAP and the emerging NIST guidance.

5. *Critical asset prioritization and protection methodologies.*  
Overall, the IG found that the Department did not specifically comment on critical asset prioritization and protection methodologies.

The CIP Board has prioritized remediation of Tier 1 vulnerabilities based on the findings of the 2000 Vulnerability Assessment Report (VAR). The 2000 VAR identified and prioritized our CIP vulnerabilities, which are organized by tiers, Tier 1 being the most critical.

6. *Training*

*The IG did not specifically address the area of training employees in IT security. However, the Department reported that in FY 2002, approximately 2,800 employees had been identified as having significant security responsibilities and that all of them have received specialized training. State indicated that security "awareness" is required of all employees and that as of the close of the FY 2002 third quarter, 9,665 employees out of 31,975 agency employees, including contractors, had received specialized "awareness" briefings, including users of OpenNet Plus.*

The Department's IT Security Training program has made specific progress in aligning security training with OMB mandates and establishing processes and procedures to enable necessary tracking of performance. IRM and DS are working closely to provide performance indicators and goals to be reported quarterly in the Corrective Action Plan and annually in the FISMA report to OMB.

*State indicated that only some of all known security weaknesses are addressed by the Department's Plans of Action and Milestone (POA&M) reports. POA&Ms were not currently integrated as a complete and comprehensive, single-source for eliminating known and documented vulnerabilities for programs and systems within the Department.*

State's POA&Ms process was immature at the time of the September 2002 GISRA report. In fact, in October 2002, only a simple Department-level POA&AM was submitted with the quarterly Corrective Action Report. Since then, the development of a data collection tool, a series of workshops and information messages has elicited the participation of over 90% of bureaus. These introduced bureau-level cyber security performance measures for security documentation, awareness and training, and system and program

assessments. All bureaus are aware of the performance measures and over 90% are participating. These system and program-level documents are monitored throughout the lifecycle and referenced in capital investment decisions.

*7. Agency integration of security and capital planning.*

Top Department of State management is committed to integrating security and capital planning. The Department is overhauling its Capital Planning and Investment Control process and has created a new board called the e-Gov Program Board, chaired by the Under Secretary for Management, aided by the CIO and CFO, to oversee IT investment. The Assistant Secretary-level e-Gov Board is supported by a Deputy Assistant Secretary-level Advisory board, which in turn is supported by a working group. IT security interests are well represented at all levels by the CIO, the SAISO and the Office of Information Assurance, respectively. This effort represents a new culture at State in the awareness of cyber security in decision-making at the most senior levels.

**III. Progress**

Since the 2002 GISRA submission, the Department has made significant changes to its Cyber Security Program that will provide the cornerstone for managing and enhancing a solid information assurance foundation. To recap,

- o At the CIO's invitation, NIST conducted an independent programmatic review to aid in improving the Department's Cyber Security Program. Multiple recommendations were implemented immediately and those requiring longer-term remediation will be incorporated in the Department-level POA&Ms.
- o 96% of bureaus are contributing to the quarterly Corrective Action Plan updates and providing system and program level POA&Ms.
- o IRM developed a single, agreed-on inventory of Department systems
- o Systems Authorization is underway and on schedule. In the first three months, 18 systems have been through the process. Site accreditation will begin in FY 2004.

- o We are treating the first C&A cycle as a project although we fully understand that this is a cyclical, recurring activity. Due to the aggressive schedule imposed by OMB (to authorize all systems by the end of FY 2004) we have pooled resources from two bureaus to make one team, funded the project centrally and are providing individual, focused assistance to systems owners and systems managers. A key measure of success of the C&A project will be whether IT security is institutionalized at the end of the project.
- o Throughout the first C&A cycle system, owners and system managers are being sensitized to IT security considerations. They are being provided assistance as required to complete security documentation, and concurrently, in an independent initiative, they are receiving training to ensure that appropriate certification and other security cost are part of their life-cycle budgets.
- o New systems are addressing security from the outset and will undergo C&A so that they are authorized before being put into operation. Regular awareness sessions for all users, establishing a cyber security corps and mandatory training for the security practitioner will assist in institutionalizing cyber security throughout the Department.
- o The patch management program is being revitalized.
- o The OpenNet Plus project, in bringing desktop Internet access to all employees, has improved security at bureaus and overseas missions. OpenNet Plus finished under budget and on schedule. CCP is doing the same on the classified side.
- o The suite of IT security training courses has been extended, including a course targeting senior management.

As a Department, I believe we have a solid beginning in place and recognize we have a long road to achieving performance based cyber security management. Realizing these challenges, Secretary Powell said it best when he said, "the success of U.S. diplomacy depends in no small measure on whether we exploit the promise of the technology revolution." With the effective management of cyber security, I am confident we will accomplish this.