Statement of
Susan Swart
Chief Information Officer
Bureau of Information Resource Management
United States Department of State

Senate Subcommittee on Federal Financial Management,
Government Information, Federal Services, & International Security,
Committee on Homeland Security and Governmental Affairs

Hearing on Agencies in Peril:
Are We Doing Enough to Protect Federal IT
and Secure Sensitive Information?

342 Dirksen Senate Office Building
March 12, 2008
2:30 p.m.

Good afternoon Chairman Carper, Ranking Member Coburn, and distinguished Members of the Subcommittee:

I am pleased to have this opportunity to testify before the Subcommittee concerning the protection of both federal information technology and the information that resides upon that information technology. My statement will offer an overview of the Department's information security program followed by a few suggestions on enhancing FISMA.

To meet Secretary Rice's requirement for the confidentiality, integrity, and availability of IT systems and networks in the conduct of diplomacy, the Department employs a strategic, layered approach to comprehensive risk management of our information and information assets. This security strategy, which we call "Defense in Depth," provides the Department multiple levels of defense and protection through a matrix of operational, technical, and managerial security controls. We focus on identifying and mitigating emerging threats because of our vast overseas exposure.

The diverse and global nature of the Department's operation presents a unique set of challenges to continually provide the highest level of information security compliance. Over our unclassified network, the Department weekly processes about 25,000,000 e-mails and instant messages from our more than 50,000 employees and contractors at 100 domestic and 260 overseas locations. Also, on a weekly basis, we block 3.5 million spam e-mails, intercept 4,500 viruses and detect over a million anomalous external probes to our network. The evolving regulatory environment and the escalating threat environment place a considerable burden upon Department resources. The Department's dynamic personnel landscape, composed of Civil Service, Foreign Service, Locally Engaged Staff and contractors operating at posts throughout the world requires a level of coordination that is unparalleled to that experienced by any other agency. The Department is largely able to overcome any cultural barriers through the use of coalitions and collaborative efforts focused on specific compliance requirements and other tangible improvements. As an example, the Cairo embassy, which employs hundreds of locally engaged staff representing numerous different cultures who speak a number of different

languages is held to the same standard as the Malabo embassy, which employs less than 50 full-time staff. Moreover, the Department is able to leverage the expertise gleaned from its extensive information sharing relationships with other civilian, law enforcement and intelligence agencies to enhance its IT security practices.

At the direction of former Secretary of State Powell, and embraced by Secretary Rice, the Department embarked on an aggressive program to modernize its IT systems and networks ensuring that every employee had Internet access. While Internet access can and has greatly facilitated the conduct of diplomacy, it also brings inherent risks. To begin addressing risks on its sensitive but unclassified network, the Department leveraged its experience handling classified information and narrowed Internet access points. In a continuation of this theme, the Department has been actively involved with the Trusted Internet Connection effort. The Department's architecture includes requisite perimeter security tools and devices, virus detection and response capability, an effective patch management program, network operations and traffic flow analysis, intrusion detection, Einstein deployment and response capability, security configuration controls and compliance verification to name a few. At each of our domestic and overseas locations we employ U.S citizen Information System Security Officers. At 10 overseas locations, we also have highly-trained, mobile, cyber security engineers.

It is worth noting that the cyber security team at State won the National Security Agency's prestigious Frank B. Rowlett Award for its organizational excellence in information assurance in 2005 – a first for the State Department. In 2005 and 2007, the Department's Chief Information Security Officer was one of three finalists selected for the individual excellence in information assurance – another first for the Department of State. Additionally, a number of individual members have won IT community-wide recognition for their contributions and leadership.

In a recent OMB report issued to Congress it was stated:

> The 25 major agencies of the Federal government continue to improve information security performance relative to C&A rates and testing of contingency plans and security controls. Several larger agencies reported

especially notable progress regarding these measures, including NASA, the **Department of State**, Treasury, and DoD (emphasis added).

Some of the specific and measurable efforts the Department has undertaken to achieve a robust, effective and efficient information security program are listed below.

Information Security Steering Committee / Governance

In furtherance of FISMA's goal and intent of providing a comprehensive information security framework, the Department established an Information Security Steering Committee with the hope of bringing together the Department's strongest minds to tackle the complexities and subtleties that information security poses. The Committee is a Deputy Assistant Secretary level working group consisting of a cross section of Department officials including: owners of technology and security senior managers. In addition to meeting statutory requirements, the forum provides a high-level opportunity to ensure that the principles of sound information security management are instilled upon all Department employees as they fulfill their roles, regardless of geographic location.

One of the Committee's first actions was to address the Department's lackluster Congressional FISMA grade[1] by utilizing Integrated Information Security Teams composed of subject matter experts from the different segments of the Department – policy specialists, operators, and managers.

Last year's annual "90 Day Push" project focused on improving two key information security requirements—Annual Testing and System/Website Inventory. With respect to Annual Testing, workshops were conducted to increase the knowledge of all bureaus' that have information systems, explaining the annual testing methodology according to NIST guidance and to assist bureaus' in completing their responsibilities. The sessions encouraged buy-in from the bureaus to hold workshops and complete annual testing requirements. Follow-up hands on testing workshops encouraged system owners to conduct their bureau's systems re-categorizations and self-assessments by the deadline. At the end of last year's annual 90 Day Push, all goals for

[1] The FISMA grades are issued by Congressman Tom Davis in the annual FISMA report card.

Annual Testing were met. With respect to Inventory, an information system inventory data call was conducted. The inventory data call reached out to all overseas posts and domestic bureaus to collect and certify all existing systems and applications. Upon completion, 100% of Department systems and websites were certified and validation has been initiated.

Another example was the establishment of a team charged with developing a Department Information Security Program Plan. The Plan identifies the relevant laws, regulations, and policies; delineates responsibilities; describes the governance mechanism: and, catalogues the elements of the Department's operational, defense-in-depth cyber security strategy. While the Plan was fully approved by the members of the Security Committee, it was done with the understanding that the Plan is a living document responding to changes in technology and the threat environment.

Based upon the hard and tireless efforts of numerous Department officials, the Department expects to receive a significantly improved FISMA grade this year.

In addition to FISMA, the Department takes every opportunity to enhance its information security posture through additional measures and approaches. Accordingly, I would like to highlight a few of these efforts.

Independent Financial Auditor Review

Back in 2003, the Department of State was cited by an independent financial auditor for having a "fragmented information security program" that "allowed for vulnerabilities to arise in the areas of external and internal system security controls." As a result, the Department's information security program was identified as a "material weakness". The audit and the resulting "material weakness", was conducted pursuant to the Federal Managers' Financial Integrity Act of 1982.

Through the collaborative efforts of numerous officials throughout the Department, the Department made definitive, continuous and measurable progress in addressing the independent financial auditor concerns. The Department prepared and updated on a quarterly basis Corrective Action Plans establishing specific actions and defined milestones associated with

correcting cited deficiencies. In the span of two years, the independent financial auditor downgraded the "material weakness" first to a "reportable condition" and then to a "deficiency". Given our present progress, the matter is expected to be formally closed at the end of this fiscal year when the independent financial auditor completes its annual audit per OMB A-123 Circular.

Retooling Certification and Accreditation

In 2006, my predecessor established a working group, comprised of bureau executive directors, to focus on Certification and Accreditation (C&A) of the Department's systems. The working group established three certification pilots to reinforce the requirement for increased bureau involvement in the C&A function. A report of the success of these pilots, and other security governance functions that further the institutionalization of security into program areas was forwarded to the CIO's office. To execute the findings of the report, the Department instituted "Green Teams" composed of subject matter experts to manage and oversee C&As, and "Tiger Teams" to contact and conduct C&As directly with the State Department bureaus. The restructured process allowed for appropriate ownership of C&As within the bureaus, while consistently providing an oversight function and escalation point for both bureaus and Tiger Teams. These changes have been received positively throughout the Department and have been hailed as more cost effective and transparent resulting in increased communications among all interested parties. Specifically, C&A costs were reduced by more than 70% in FY07 Q2 and Q3.

In addition the Department's C&A efforts, the Department's vulnerability scanning tools provide system administrators across the world-wide enterprise with "Daily Validation" reports of vulnerabilities that exist within their zone of control in the following categories: patch management, anti-virus updates, standard operating environment compliance, and configuration compliance of mandated security settings. The tools provide appropriate and timely risk management data to administrators who have the means and ability to address any issues at the local level. Additionally, grades are assigned to ensure continued vigilance and assist senior manager oversight and resource allocation for IT security.

Largely through the combined efforts of the Certification and Accreditation program and the Evaluation and Verification Program, the Department achieved "Green-Green" status on the

Expanded Electronic Government portion of the President's Management Agenda (PMA) Scorecard for four consecutive quarters. "Green-Green" was achieved in Quarter 4 (Q4) in Fiscal Year 2006 (FY06), and in Q1, Q2, and Q3 in FY07. While the Department has slipped from 100% to 98% with its Certification and Accreditation totals, it has been and continues to be the Department goal to remain at 100%.

Information Systems Security Line of Business

From its very earliest stages of development, the Department has been an ardent supporter of the federally-focused Information System Security Line of Business. From the onset, the Department dedicated staff and resources to the initial working group responsible for identifying the aspects of information security that would most readily lend themselves to a Shared Services model. A Shared Services model is where one agency is responsible for providing service to another agency. At the development stage, key Department of State personnel assisted by drafting requisite documents to ensure the most appropriate agency would be selected to serve as a Shared Service Center. During the selection stage, a Joint Department of State and USAID collaborative effort, known as JSAS, was selected by OMB as only one of three agencies to serve as a Shared Service Center for information security awareness training. Presently, the Department of State and USAID information security awareness training solution is providing service to four other agencies totaling over 40,000 government employees and contractors in addition to their own employees and contractors. The Department of State continues to provide support to the Information Systems Security Line of Business through participation on half a dozen working groups.

Protection of Privacy

The Department continues its commitment to comply with Privacy Act provisions, protecting the rights of American citizens and aliens admitted for permanent residence and safeguarding personal information regardless of physical format. More than a decade ago the Assistant Secretary for Administration was designated the Department's Senior Official for Privacy. More recently, the Department formed the Privacy Protection Governance Board to heighten awareness and ensure the protection of personally identifiable information in all aspects of the Department's programs and activities. The Board brings together Assistant Secretaries from

throughout the Department to address the interdependencies among the security, technology, and business aspects requisite to minimizing and reducing the collection, use, and dissemination of personal information -- and especially Social Security Numbers -- and to safeguarding this sensitive information in all formats, particularly in today's dynamic electronic environment. The Department's accomplishments include the development of a Breach Notification Policy; Core Response Group procedures; reduction and elimination of the use or dissemination of Social Security Numbers; communication through websites, collectives, worldwide cables, and Department Notices; awareness building for the business owners of personal information; review of business practices and process; and enhanced attention to Privacy Impact Assessments in the Certification and Accreditation Process as reported in FISMA. While we have made considerable progress, we recognize that more work needs to be done to protect personal information within the Department.

With respect to the OMB 07-16 requirements, the Department has the following practices in place:

The Department of State is in the process of encrypting all of its mobile computing devices. The Department leveraged its PKI contract to provide encryption protection at no additional cost to the Department. The solution is fully compliant with applicable NIST standards and guidelines (FIPS 140-2).

The only means for a Department user to remotely access the Department's unclassified network is through a two-factor authentication system that combines a hand-held random generating password device and a separate password authenticated by the Department's network.

The Department's remote access solution referenced above utilizes a "time-out" function requiring user re-authentication after 15 minutes of inactivity, a standard exceeding the requirement.

As referenced in GAO's PII report, the Department along with ten other agencies are researching technical solutions to address logging for all computer-readable data extracts from databases holding sensitive information and verify that the extracts have been deleted within 90 days.

Possible Enhancements to FISMA Implementation

In December 2002, FISMA represented a valiant step forward in how the federal agency community viewed information security. The statute's requirement to "develop, document and implement" an information security program throughout a system's lifecycle was a shift in philosophy for many personnel. Although Certification and Accreditation and FISMA Plans of Actions & Milestones have now become common-place vernacular for many non-information security personnel, there is still room for improvement in the area of FISMA implementation.

FISMA provides for an annual independent evaluation of the agency's information security program. Although well-intentioned at the time, the independent annual "evaluation" has the potential for creating ambiguities. Notably, GAO reports in April 2005, July 2005, and June 2007 have all identified the lack of a common Inspector General reporting framework as a deficiency of the FISMA evaluation process. In the GAO's own words, the "lack of a common methodology, or framework, has culminated in disparities in audit scope, methodology, and content. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency." FISMA implementation could be improved through an agreement amongst IG's upon a common evaluation framework.

Another enhancement would be the addition of metrics that account for an agency's ability to detect, respond to and react to cyber security threats and manage vulnerabilities. For example, as the CIO, I have the ability to leverage a wide array of independent Department security services including continuous network monitoring, technical countermeasures, counter intelligence services, threat analysis, and physical and technical security programs, related to a separate mandate to protect life, information and property around the world. The absence of recognition of these efforts may misrepresent our efforts towards FISMA compliance. Prior GAO reports in April 2005 and June 2007 have likewise identified the lack of reporting on incident response metrics as a shortcoming in the FISMA evaluation process.

Mr. Chairman, I want to conclude by reiterating the State Department's unyielding commitment to information security. I thank you and the Subcommittee members for this opportunity to speak before you today and would be pleased to respond to any of your questions.