STATEMENT OF VIVEK KUNDRA
FEDERAL CHIEF INFORMATION OFFICER,
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET

BEFORE THE
SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION, FEDERAL SERVICES, AND
INTERNATIONAL SECURITY

October 29, 2009

More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense

Good afternoon Chairman Carper, Ranking Member McCain, and members of the Subcommittee. Thank you for the opportunity to testify on the state of Federal information security.

Our Nation's security and economic prosperity depend on the stability and integrity of our Federal communications and information infrastructure. As stated in *The Cyberspace Policy Review*, the 60-day clean slate look at cyber activities ordered by the President, threats to cyberspace pose some of the most serious economic and national security challenges of the 21st century for the United States. The group of State and non-state actors who target U.S. citizens, businesses, and Federal agencies is growing. US-CERT, the computer response center for civilian agencies, sees millions of attempts daily to access open ports and vulnerable applications on Federal networks.

Historically, the Federal Government has not been as effective as necessary in its cyber defense. An inadequate cyber security workforce, a focus on compliance rather than outcomes, and a cumbersome and time-consuming process for collecting information regarding agency security postures have hindered our cyber security management capabilities.

To address these issues, OMB has taken the following actions:

- Expedited hiring authority for 1,000 cyber security positions at the Department of Homeland Security;
- Launched CyberScope, an automated, streamlined platform for secure reporting to replace the old, less secure manual process for the collection of agency cyber security information;
- Created a taskforce comprised of representatives of the Federal CIO Council, which includes the CIOs of civilian agencies, the Department of Defense, and National Intelligence Community; the Council of Inspectors General on Integrity and Efficiency; the National Institute of Standards and Technology; the Department of Homeland

Security; and the Information Security and Privacy Advisory Board to develop new reporting metrics that focus on outcomes not processes; and

- Required agencies to report detailed cost information on security spending beginning with FY 2010.

The Road to FISMA

The cyber security environment in the Federal Government has been in constant evolution, due to the ever-changing nature of technology as well as the need to meet the increasingly complex threats we face. Over the past twenty years, Congress has enacted legislation to address these complex issues.

The Computer Security Act of 1987 sought to improve the security and privacy of sensitive information in Federal computer systems and to establish acceptable security practices for such systems. However, information technology was not considered a critical part of the management agenda for Federal agencies. It was not until 1996, with the passage of the Clinger Cohen Act, that the position of the Chief Information Officer (CIO) was created across Federal agencies, recognizing the need for a single executive to lead information technology at each agency.

In 1999, Y2K highlighted our reliance on the information technology that powers our digital economy. The Government Information Security Reform Act (GISRA) of 2001 established information security program, evaluation, and reporting requirements for Federal agencies yet sunset by 2002. Recognizing the Nation's continued dependence on IT, Congress passed the Federal Information Security Management Act (FISMA) in 2002.

The Current State of FISMA Implementation

In the seven years it has been in place, FISMA has raised the level of awareness of the critical importance of information security in the agencies and in the country at large. It has also strengthened agency reporting requirements and established mechanisms for the collection of agency information. For example, based on agency FISMA submissions, security awareness training has become prevalent across the Federal Government for employees and contractors. Agencies and departments are now reporting inventory numbers for their systems, and CIOs play a critical role in managing information security in the agencies. However, continued progress must be made to realize FISMA's full vision of a secure and vigilant Federal Government.

When FISMA was first enacted, OMB approached the question of metrics by concentrating on compliance. During the first few years of FISMA reporting, the required metrics evolved as initial benchmarks were met.

These metrics were lagging indicators focused on compliance rather than outcomes. Agencies reported infrequently and, in many cases, only annually. This occurred in an environment where threat vectors change daily. Moreover, the information collected does not reflect the readiness of the agencies to deal with the reality of modern threats. Even information

as basic as the cost of compliance or the number of days to apply a critical patch is not readily available.

The economic prosperity of our Nation relies upon, and is powered by, the digital infrastructure. Yet, security in the Federal Government is not where it needs to be. The Nation's approach to cyber security over the past 15 years has failed to keep pace with mounting threats. We are taking actions to improve the situation but are only at the beginning of what needs to be done. The Federal Government must remain committed to protecting the digital infrastructure upon which we so heavily depend.

I) EXPANDING THE WORKFORCE

As the Department of Homeland Security (DHS) grows into its role of protecting the homeland in cyberspace, it must have a skilled workforce capable of securing networks, understanding the threats we face, and assisting Federal agencies in defending their networks. Recently, OMB worked closely with the Office of Personnel Management to extend special hiring authority to DHS to meet its growing needs.

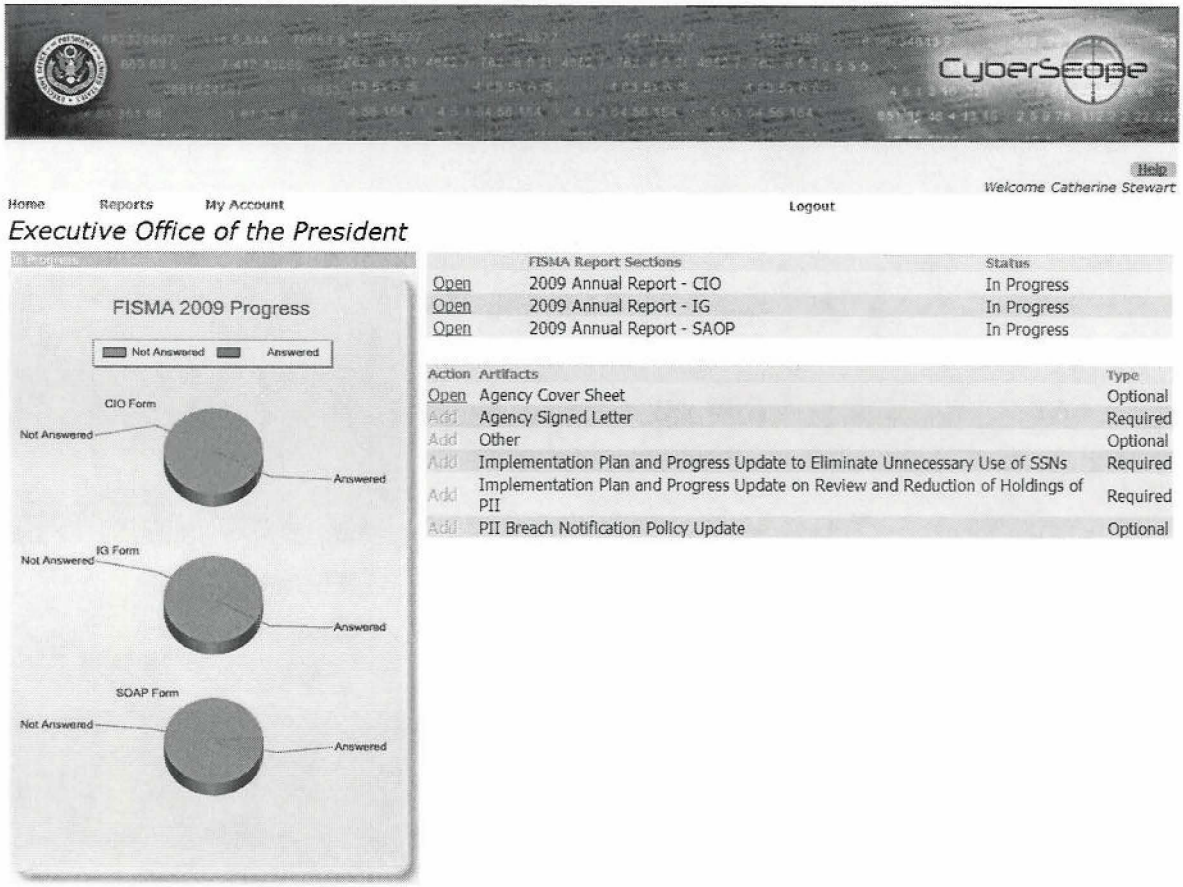
On October 1, 2009, DHS Secretary Janet Napolitano announced that DHS has the authority to hire up to 1,000 new cyber security professionals over the next three years to fill staffing gaps at various DHS agencies. DHS will look to fill critical cyber security roles including: cyber risk and strategic analysis; cyber incident response; vulnerability detection and assessment; intelligence and investigation; and network and systems engineering. This new hiring authority will enable DHS to recruit skilled cyber analysts, developers and engineers to serve their country by helping to secure the nation against cyber threats.

II) CYBERSCOPE: A MODERN PLATFORM FOR FISMA REPORTING

Prior to the 2009 reporting cycle, OMB received via email over 100 individual spreadsheets from agencies and paper copies of the Inspector General reports in response to FISMA reporting requirements. It took three FTEs working for a full month to compile and analyze the data submissions. This manual spreadsheet process was laborious, time consuming, and unsecure. Furthermore, the lack of meaningful analysis, the vulnerable reporting methodology, and the manual nature of the process inhibited clear, timely, and comprehensive insight into the security posture of the Federal Government's information technology systems.

On October 19, 2009,O MB launched an interactive data collection tool—CyberScope—enabling agencies to fulfill their FISMA reporting requirements through a modern digital platform.The broad range of meaningful information collected, the use of secure two-factor authentication, and the online access to data provides for a more efficient and effective reporting process.

In spring of next year, OMB will unveil a cyber security dashboard, unlocking the value of agency FISMA submissions in a timely, comprehensive, and secure manner. The streamlined collection format allows for better research and reporting across Federal agencies, OMB, and GAO.



A sample CyberScope screenshot using test data.

Rather than relying on unencrypted emails and unprotected spreadsheets, CyberScope requires users to login via a secure identity card and an accompanying unique PIN number.[1] The use of the PIV card for logging into CyberScope is the first time this credential has been used for a Government-wide system.

CyberScope empowers its 600 estimated agency users to manage their internal reporting and information collection processes as best suits their individual needs. OMB conducted training sessions prior to the launch of CyberScope and utilized much of the feedback to improve the system. Going forward, CyberScope's extensible platform is the performance-based solution to years of inefficient and unsecure collection of agency security data.

Although the agency focus to-date has been on compliance, some agencies have adopted a performance-based approach. For example, the Department of State (DoS) is one such agency. DoS faces unique security challenges as it serves both domestic employees and U.S. officials at embassies and consulates worldwide. The DoS network supports 285 foreign posts and consists

[1] The Personal Identity Verification (PIV) card was mandated for use by all Federal employees by Homeland Security Presidential Directive 12 (HSPD-12).

of 5,000 routers and 40,000 hosts. Although ultimate responsibility and accountability resides with the CIO, individual posts have a degree of responsibility for management of the network.

To provide better insight into its security posture, DoS has moved to a security dashboard. Cyber security information is gathered through automated processes and is integrated into a central database. In some cases, data are accessed on-demand directly from source systems. DoS also uses a scoring process based on a set of ten groups of criteria spanning from scans to security settings to the vulnerability of a host. Because scores are visible to other system managers across the agency, the system fosters an atmosphere of peer-based competition.

DoS' use of a security dashboard provides its CIO and other senior managers secure access to meaningful, dynamic data, ultimately yielding better insight into its security posture and enhanced protection for its networks.

III) PERFORMANCE-BASED METRICS

What gets measured gets done; metrics are policy statements. As long as OMB metrics continue to measure compliance, agencies and departments will continue to march toward that goal. However, we can never get to security through compliance alone.

In September 2009, OMB established a task force to develop new, outcome-focused metrics for information security performance for Federal agencies. To solicit the best ideas, OMB has reached out across the Federal community, as well as to the private sector. This task force is concentrating on developing metrics that will advance the security posture of agencies and departments. Understanding that metrics are a policy statement about what Federal entities should concentrate resources on, the task force is developing metrics that push agencies to examine their risks and make substantial improvements in their security.

Participants in the task force include: the Federal CIO Council, which includes the CIOs of civilian agencies, the Department of Defense,a nd Office of the Director of National Intelligence; the Council of Inspectors General on Integrity and Efficiency; the National Institute of Standards and Technology; the Department of Homeland Security; and the Information Security and Privacy Advisory Board. In addition, the Government Accountability Office (GAO) serves as an observer to this taskforce.

The task force is currently developing forward-looking metrics focused on improving security at agencies rather than merely demonstrating compliance. Additionally, the task force is working with OMB to develop a roadmap for future reporting under FISMA which will incorporate real-time metrics and enhance Government-wide situational awareness.

OMB plans to release for public comment the draft metrics for FY 2010 reporting later this fall. Upon receipt and analysis of comments, OMB will release the final metrics for FY 2010 reporting and the roadmap for future reporting efforts in the first quarter of 2010. Agencies will report on performance-oriented metrics in the fall of 2010.

As part of this effort, OMB is also working on a roadmap for the future. As other cyber security activities progress, such as the Comprehensive National Cybersecurity Initiative

(CNCI), OMB is considering the role and participants of security information collection. For example, more frequent reporting of outcome based metrics, near or at real-time, is imperative for developing situational awareness across the Federal enterprise.

IV) Improved Insight Into the Cost of Security

In FY 2010, for the first time, we are asking agencies for detailed cost estimates and the actual amounts spent on security. Historically, as part of the annual budget process, agencies reported only the percentage of spending related to cyber security for each IT investment. However, this was not broken down into distinct categories, such as personnel costs, reporting costs, certification & accreditation (C&A) costs, and security management costs. The only other cyber security-related cost data point collected was the amount spent for training by the agencies. This lack of detailed information precludes the level of meaningful analysis needed to assess the efficiency and effectiveness of Federal information security spending.

Recognizing that the best security is "baked in" to information technology investments and not added in separately, we know that this is the beginning of the process of obtaining relevant cost data. Analysis of the preliminary cost data will be provided in the FY 2009 FISMA Report to Congress, to be delivered in March 2010.

In the coming years, access to this data will allow OMB to evaluate the efficiency of the Federal expenditure on security. Right now, we cannot answer key questions such as: "Are we spending too much on certification and accreditation, considering its benefits?" Even basic questions, such as, "How many cyber security employees are there across the Federal Government?" are unknown. Collection of detailed information, especially when combined with the performance-based metrics, will allow both OMB and agency management to make informed, risk-based decisions on where to allocate scarce resources.

Closing

From the launch of CyberScope to the hiring of up to 1,000 new DHS cyber security experts, the Administration is committed to strengthening our Federal cyber defense. The actions we are taking will both enable critical insight into agency security postures and help enhance protection of our nation's systems. Ultimately, this will lead to more effective, efficient, and secure IT across all Federal agencies.

The threats we face are numerous, evolving faster than our cyber defense, and have the potential to do great harm. A secure, trusted computing environment in the Federal Government is the responsibility of everyone involved from the agency heads to those charged with oversight. It entails employees, contractors, and the American people working together to create a culture of vigilance and security to enable us to continue to efficiently leverage the power of technology. This will not be easy nor will it take place overnight. Our current actions represent important steps towards a stronger Federal cyber defense, but we must remain ever-vigilant.