EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

March 24, 2010

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

BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT

"Federal Information Security: Current Challenges and Future Policy Considerations"

Good morning, Madam Chairwoman and members of the Subcommittee. Thank you for the opportunity to testify on the state of Federal information security and the current challenges and future policy considerations.

The globally interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the economy, civil infrastructure, public safety, and national security. To realize the full benefits of the digital revolution, the American people must have confidence that sensitive information is not compromised, their communications with the government are secure, their privacy and civil liberties are protected, and that the Federal infrastructure is not infiltrated. Achieving trusted communications and information infrastructure will ensure that the United States achieves the full potential of the information technology revolution.

The group of actors who target U.S. citizens, businesses, and Federal agencies is growing. US-CERT, the computer readiness center for civilian agencies, sees millions of attempts daily to access open ports and vulnerable applications on Federal networks.

Cybersecurity is a Presidential priority and, across the Administration, we are working on this issue. I am working closely with the President's Cybersecurity Coordinator, Howard Schmidt, and the Federal Chief Technology Officer, Aneesh Chopra. As Cybersecurity Coordinator, working as part of both the National Security Staff and the National Economic Council, Mr. Schmidt is coordinating cybersecurity activities across the government, including those under the Comprehensive National Cybersecurity Initiative (CNCI). As the Federal Chief Technology Officer, Aneesh Chopra is focused on advanced, "game-changing" technologies that help the government meet not only the threats of today, but those of the future as well. As the Federal Chief Information Officer, I am charged with OMB's responsibilities under the Federal Information Security Management Act (FISMA).

Eight years ago, when FISMA was enacted, the internet and the mobile computing revolution were not as pervasive as they are now. Today, agencies are leveraging technologies and business models such as cloud computing, mobile platforms, social media, and third-party platforms to increase efficiency and effectiveness. For example, the Department of Veterans Affairs contracts with mortgage services to service VA-owned home loans. These new models increase efficiency but leave agencies struggling with the question of how to apply FISMA's requirements in an environment where system and enterprise

boundaries no longer define the security points. Effective cybersecurity is vital to our national prosperity and economic stability; however, cyber incidents continue to impact the Federal Government.

2009 FISMA REPORT SUMMARY

In the past eight years, agencies have made significant progress in complying with FISMA requirements. For example in Fiscal Year 2002, 35% of agency systems had tested contingency plans; whereas, by the end of Fiscal Year 2009, 86% of agency systems had tested contingency plans. In 2002, 60% of agency systems had tested security controls; whereas, in 2009, 90% agency systems had tested security controls.

Agencies have also reported improvements in their compliance with Certification and Accreditation (C&A) requirements such as assessing their systems for risks and creating system security plans. In 2002, 47% of all agency systems had a Certification & Accreditation in place; whereas, in 2009, 95% of systems had a Certification & Accreditation in place.

Similarly, agencies reported substantial progress in the training of employees with significant security responsibilities, increasing the skills of the Federal cybersecurity workforce. In 2002, 37% of employees with significant security responsibilities were trained; whereas in 2009, 90% were trained.

Agencies also provided details on headcount and training costs in their FY 2009 FISMA reports. In FY 2009, agencies reported 64,450 FTEs dedicated to cybersecurity; however, 90% of those FTEs reported reside within the Department of Defense. Of the $6.8 billion in total cybersecurity spending reported by agencies in the FY 2009 budget, $54.6 million (less than 1%) was spent on training. This amount includes the annual security awareness required for all Federal employees and contractors, as well as training for employees with significant cybersecurity responsibilities.

Despite the improvements as reported by agencies, the Federal Government's communications and information infrastructure is still far from secure. The FISMA measures reported on annually have led agencies to focus on compliance. However, we will never get to security through compliance alone.

KEY ISSUES IN FEDERAL CYBERSECURITY

President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity." As a result, in February 2009, the President directed the National Security Council and Homeland Security Council to conduct a review of the plans, programs, and activities underway throughout government that address our communications and information infrastructure (i.e., "cyberspace"), in order to develop a strategic framework to ensure that the U.S. Government's initiatives in this area are appropriately integrated, resourced, and coordinated.

There are a number of issues that contribute to our vulnerabilities, including:

I. **Lack of Coordination –** There has been no single individual or entity with the responsibility to coordinate Federal Government cybersecurity-related activities, both within the Federal Government and with the private sector. Many departments and agencies have disparate responsibilities with regards to cybersecurity. Furthermore, even for specific cyberthreats and incidents, agency responses are often fragmented and uncoordinated with each other. Independent efforts are not sufficient to address the challenges without a central coordination mechanism, an updated national strategy, an action plan developed and coordinated across the Executive Branch, and the support of Congress.

II. **Culture of Compliance –** For too long, Federal agencies have focused on reporting on security rather than gaining meaningful insight into their security postures. For example, over the last six years, the Department of State spent $133 million amassing a total of 50 shelf feet, or 95 thousand pages, of

security documentation for about 150 major IT systems. This works out to roughly $1,400 per page on paper "snapshots" that are often outdated a few days after being published.

III. **Lack of an Enterprise Approach** – Currently, security information is scattered throughout agencies in different systems that do not communicate with each other. For example, in previous security incidents, some agencies had difficulty determining how many of their computers were vulnerable, how many were patched, and how many were infected across their enterprises. Similarly, defense of Federal networks is fragmented and lacking clear situational awareness.

IV. **Energize National Agenda for Cybersecurity Research & Development –** The United States needs to harness the full benefits of innovation to address cybersecurity concerns. Currently, multiple agencies have cybersecurity R&D activities on-going. The challenge is to focus these activities to achieve the most significant advances and to give the Federal Government and the public stronger cybersecurity.

ADVANCING THE SECURITY POSTURE OF THE FEDERAL GOVERNMENT

To advance the security posture of the Federal Government, the Administration is taking a number of actions, including focusing on coordination, shifting to a performance-based culture, taking an enterprise approach to cybersecurity, and developing an integrated plan for research and development.

I. Focusing on Coordination

To address the lack of coordination, the Administration has taken the following steps.

Cybersecurity Coordinator – On December 22, 2009, the President appointed Howard Schmidt as his Cybersecurity Coordinator. Mr. Schmidt has the responsibility of orchestrating the many important cybersecurity activities across the government; in particular, those related to the Comprehensive National Cybersecurity Initiative (CNCI), and serves as a key member of the President's National Security Staff. Mr. Schmidt oversees Federal-wide coordination of the President's cybersecurity agenda, while working in tandem with the private sector on cybersecurity.

Coordination in cybersecurity research and development is discussed below in section IV.

II. Shifting to a Performance-Based Culture

For too long, the focus in Federal security has been on compliance rather than performance. In 2009, we began moving agencies to a performance-based culture.

Declassified Description of the Comprehensive National Cybersecurity Initiative – The CNCI constitutes an essential component of cybersecurity efforts within the Federal Government. On his first full day in office, in a memorandum on open government to all Federal departments and agencies, President Obama said, "My Administration is committed to creating an unprecedented level of openness in government." Building on this statement, on March 2, 2009, the Administration revised the 2008 classification guidance for the CNCI. An unclassified description of the CNCI and each of the 12 initiatives under the CNCI is now publicly available.

Transparency is particularly vital in areas such as the CNCI where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity. Transparency provides the American people with the ability to partner with government and participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties.

Launch of CyberScope – On October 19, 2009, OMB launched an interactive data collection tool—CyberScope—enabling agencies to fulfill their FISMA reporting requirements through a modern digital platform. The broad range of information collected, the use of secure two-factor authentication using Personal Identity Verification (PIV) cards, and the online access to data provide for a more efficient and effective reporting process , allow for the collection of more complex metrics and enable more meaningful analysis of agency security postures. CyberScope empowers its 600 estimated users to manage their internal reporting and information collection processes as best suits their individual needs, while allowing OMB better access to agency security information.

Performance-Based Metrics – 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 reached out across the Federal community as well as to the private sector. This task force concentrated on developing metrics that would 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 developed metrics that will push agencies to examine their risks and make substantial improvements in their security. Participants in the task force included: the Federal CIO Council; the Council of Inspectors General on Integrity and Efficiency; NIST; the Department of Homeland Security; the Information Security and Privacy Advisory Board; and the National Security Council Cybersecurity Coordinator. In addition, the Government Accountability Office (GAO) served as an observer to this taskforce.

The result of the work done by the taskforce is a three-tiered approach for FY 2010 FISMA reporting for agencies through CyberScope: data feeds; security posture questions; and agency interviews.

Continuous Monitoring – The key element to managing an information security program is information—about agencies' security postures, activities and threats. Agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way. The many levels of agency management all need different levels of this information presented to them in ways that enable timely decision making.

A critical aspect for agency officials of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system. Conducting a thorough point-in-time assessment of the deployed security controls is a necessary but not sufficient condition to demonstrate security due diligence. An effective organizational information security program also includes a rigorous continuous monitoring program integrated into the system development life cycle. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system.

Collection of Information Security Costs – In this reporting cycle, for the first time, OMB asked agencies for detailed cost estimates and the actual amounts spent on information security. Historically, as part of the annual budget process, agencies reported only the percentage of spending related to cybersecurity for each IT investment. However, this information was not broken down into distinct categories, such as personnel costs, reporting costs, certification and accreditation (C&A) costs, and security management costs. This lack of detailed information precluded 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 or well after the investments have been deployed, OMB needs to determine where, in the life cycle development of systems, agencies are spending their resources. The information collected for FY 2009 is the beginning of the process of obtaining this crucial cost data.

In the coming years, access to continually refined cost data will allow OMB to evaluate the efficiency of Federal expenditures on security. The collection of detailed information, especially when combined with performance-based metrics, will allow both OMB and agency management to make informed, risk-based decisions on where to allocate scarce resources.

TechStat – In June 2009, we launched the IT Dashboard, which allows the American people to monitor IT investments across the Federal Government. Building on the foundation of the dashboard, we launched TechStat Accountability Sessions this past January. A TechStat accountability session is a face-to-face, evidence-based review of an IT program with OMB and agency leadership, powered by the IT Dashboard and input from the American people. TechStat sessions enable the government to turnaround, halt or terminate IT investments that do not produce dividends for the American people. Investments are carefully analyzed with a focus on problem solving that leads to concrete action to improve performance. In particular, we have applied this approach to Federal IT security projects. For instance, several of the TechStats conducted to date have focused on security such as agency HSPD-12 implementation efforts.

III. Enterprise Approach to Cybersecurity

To achieve true situational awareness and to fully harness the power of the Federal Government to address the challenges of cybersecurity, we must take an enterprise approach. We are taking a number of steps to move us forward, including:

Improve the Effectiveness of the Cybersecurity Workforce – The White House has formed an interagency working group to establish the National Cybersecurity Education Initiative. This working group defined four tracks of work that are now underway:

- Track 1 – A National Awareness Campaign led by the Department of Homeland Security;
- Track 2- A Formal Cybersecurity Education program led by the Department of Education;
- Track 3 – A Federal Workforce Structure program led by the Office of Personnel Management and the Department of Defense; and
- Track 4 – A National Workforce Training and Professional Development Program led by the Departments of Homeland Security and Defense, and the Office of the Director of National Intelligence.

Achieve a Consistent Security Posture – Through initiatives such as the Trusted Internet Connections (TIC) initiative and the Federal Desktop Core Configuration (FDCC), we are standardizing good security practices across the Federal enterprise. The TIC initiative is composed of two distinct efforts. The first is to reduce the target profile of Federal agencies by decreasing the number of external access points. The second is to implement an Intrusion Detection System using passive sensors to identify when unauthorized users attempt to gain access to those networks.

The FDCC establishes a consistent security configuration for desktops and laptops running Windows-based software across Federal agencies. This configuration includes basic security measures such as turning off ActiveX controls, a common infection vector, by default.

Coordinate Incident Response – The President's Cyberspace Policy Review identified response and coordination efforts around cyber incidents as a key area for improvement. As a result, the Department of Homeland Security, in coordination with the White House and various stakeholders from government and industry, is developing a new National Cyber Incident Response Plan (NCIRP). The NCIRP will outline key cyber roles and responsibilities across the Nation, linking all levels of government and the private sector. It is intended to describe how every day, steady-state cyber incident management activities expand to manage incidents that require a coordinated National response.

Leverage Federal Purchasing Power – We are leveraging Blanket Purchase Agreements (BPAs) and other government-wide acquisition vehicles to enable agencies to purchase security tools in an efficient manner. For instance, in Q4 2009, a BPA was announced that included tools to help agencies develop an accurate inventory of information resources managed at their agency, and maintain an up-to-date awareness of information regarding cybersecurity threats.

Implement Federal Identity Management – The ability of Federal agencies to accept credentials of other agencies' employees is fundamental to government-wide coordination. As part of this effort, OMB continues to oversee the implementation of the strong Federal identity management scheme outlined in Homeland Security Presidential Directive 12 (HSPD-12) ("Policy for a Common Identification Standard for Federal Employees and Contractors") which requires agencies to follow specific standards and business processes for the issuance and use of Personal Identity Verification (PIV) smartcard credentials. When used in accordance with NIST guidelines, the credentials provide a number of benefits including secure access to Federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities. As of December 1, 2009, over 5 million PIV credentials (82 percent of those needed) had been issued to the Federal workforce, as reported by agencies.

Moving beyond Federal identity management, the Cyberspace Policy Review also calls for development of a "cybersecurity focused identity management vision and strategy." In response to this requirement the White House has established an effort to develop a National Strategy for Secure Online Transactions. The goal of this effort is to improve the trustworthiness and security of online transactions by facilitating the establishment of interoperable trust frameworks and implementation of improved authentication and authorization technology and processes for all online transaction participants, across Federal, civil, and private sectors. OMB, in conjunction with the Federal CIO Council, has developed PIV-interoperability policy and criteria for acceptance of non-Federal credentials.

IV. Develop an Integrated Plan for Research & Development

The President's Cyberspace Policy Review calls for sharing responsibility for cybersecurity by improving the partnership between the private sector and government; and encouraging innovation in game-changing technologies in coordination with industry and academia. This expands on the goal of the Comprehensive National Cybersecurity Initiative (CNCI) to strengthen the future cybersecurity environment by coordinating and redirecting research and development efforts across the Federal Government.

These goals have been embraced under White House leadership. Progress includes (1) The National Cyber Leap Year, gathering input from more than 300 private sector white papers and a National Summit to develop a shared game-changing R&D strategy focused on moving target, tailored trustworthy spaces, and cyber economic incentives; (2) a joint Financial Services Sector/government task group, developing a real-traffic cybersecurity testbed; and (3) a working group of industry leaders, university researchers, and government representatives formed around cybersecurity insurance as a market force for improved security.

The Cybersecurity and Information Assurance (CSIA) Interagency Working Group coordinates R&D activities for unclassified efforts, the Special Cyber Operations Research and Engineering (SCORE)

group for classified activities, and the Senior Steering Group for Cybersecurity (SSG) bridges these groups and provides overall direction and guidance. Research supported under these efforts and conducted in both government and private settings includes cybersecurity metrics, security automation, network protection and defense, secure software engineering, and other areas to create the next generation of cybersecurity capabilities.

CLOSING

The Administration has taken a number of steps to improve cybersecurity across the Federal Government in the past year. However, security is a journey, not a destination. The threats we face are numerous, evolving faster than our cyber defense, and have the potential to do great harm. We are moving forward. For example, the Government has won praise for the work we did to contain Conficker. A representative of the Conficker Working Group said, "For the first time the government is taking the lead in a technical security issue, rather than lagging."[1]

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 while respecting the privacy and civil liberties of the American people. 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. I look forward to continuing to confront the challenges our Nation faces in cyberspace in concert with Cybersecurity Coordinator Schmidt and Chief Technology Officer Chopra.

I thank the Committee for this opportunity to appear here today and I look forward to not only answering any questions that you might have but also to working in partnership with you on these critical issues for our government and our nation.

[1] Government Computer News, "Have Agencies Scrubbed the Conficker Work From Their Systems?', March 19, 2010, http://gcn.com/articles/2010/03/19/conficker-cleanup-031910.aspx