STATEMENT OF VIVEK KUNDRA
FEDERAL CHIEF INFORMATION OFFICER,
ADMINISTRATOR FOR ELECTRONIC 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

May 19, 2009

Good morning, Chairwoman Watson, Ranking Member Bilbray, and members of the Subcommittee. Thank you for the opportunity to testify on the state of Federal information security.

The security of Federal information systems is a major concern of this Administration. Our nation's security and economic prosperity depend on the stability and integrity of our Federal communications and information infrastructure. Safeguarding these important interests will require balanced decision-making that integrates and harmonizes our national and economic security objectives with our privacy rights, civil liberties, and open government. As a first step, the President has directed a 60-day review of cybersecurity policies and efforts throughout the government. OMB is working closely along with other agencies with Acting Senior Director Melissa Hathaway of the National Security Council and her team on this review.

During the last twenty years, the United States and the world have been moving from a paper-based world to a digital world. Advances in technology are fundamentally changing the way business is done, increasing productivity, and providing the American people easy access to services in ways previously structurally impossible.

Essential to these new capabilities is the presence of communications networks that securely carry sensitive information. Yet, as we have unleashed new transactions over this network, a new class of risks has emerged. The American people need to trust that the information they are submitting to or receiving from the government is accurate, reliable, and secure.

However, recent successful breaches at the Federal Aviation Administration and at the vendor that hosts USAjobs.gov demonstrate that the current state of information security at Federal agencies is not what the American people have the right to expect. The Federal Information Security Management Act (FISMA) has been in place for 7 years. It has raised the level of awareness in the agencies and in the country at large, but we are not where we need to be.

In our initial review of information security issues, the following issues have surfaced:

- The performance information currently collected under FISMA does not fully reflect the security posture of Federal agencies;
- The processes used to collect the information are cumbersome, labor-intensive, and take time away from meaningful analysis, and;
- The Federal community is focused on compliance, not outcomes.

While the current reporting metrics may have made sense when FISMA was enacted, they are largely compliance based. They are trailing, rather than leading, indicators. We need metrics that give insight into agencies' security postures and possible vulnerabilities on an on-going basis.

To evaluate new metrics, we are taking a collaborative approach. We are working with the community of Federal agency Chief Information Officers and Chief Information Security Officers, as well as the Inspectors General and the National Institute of Standards and Technology, to consider more effective security performance metrics -- ones that show current status and are predictive in nature. In addition, we are reaching out to a broad array of organizations, across the public and private sectors and academia.

Today, agencies and IGs are heavily focused on compliance. The creation of a secure, transparent, collaborative environment requires a risk-based approach. We will never achieve our security goals through compliance alone because security threats are fluid and constantly changing. Each new technology, new employee, and new program represents the potential for additional security weakness. Agencies need to adopt a risk-based approach to security, to look at activities, people and programs on an on-going basis.

The Administration is committed to creating a trusted, secure Federal computing environment that makes information transparent to the American people while protecting privacy and confidentiality. While the actions I have spoken about here will assist in creating that environment, they alone are not enough. 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.

Thank you for this opportunity to testify on this important issue, and I look forward to your questions.