STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY

February 28, 2008

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the Administration's Comprehensive National Cybersecurity Initiative. My remarks today will focus on the progress we have made in improving the security of the government's information and information technology (IT) systems as well as our strategy for managing the risk associated with our government services in this ever changing IT environment. In our increasingly interconnected and interdependent environment, security risks left unaddressed by one agency can exponentially compound security risks faced by all of us. These weaknesses prevent agencies from achieving program goals and erode the public's trust in us.

Information security and privacy are extremely important issues for the Administration. On March 1, 2008, the Office of Management and Budget (OMB) will provide our fifth annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). This report will go into detail on our improvements and remaining weaknesses for both security and privacy.

OMB policies and subsequent National Institute of Standards and Technology (NIST) guidance focus on a risk-based, cost-effective approach and reflect the balance between strong security and mission needs. Agencies are responsible for implementing the policies and guidance for their unique mission requirements within their capital planning and investment control processes. Agency officials who own and operate the agency business programs are ultimately responsible and accountable for ensuring security is integrated into those program operations. Our oversight is achieved in two primary ways -- via the budget and capital planning process, and through independent program reviews.

Our work on the cyber initiative is focused on closing gaps in areas of continued weakness – implementing existing security policy, and managing non-secure external connection, including Internet points of presence. Please note our work is happening concurrently on all of the programs described.

Effectively Implementing Existing Security Policies

Securing cyberspace is an ongoing process, so as new technologies appear and new vulnerabilities are identified, NIST provides guidance to Federal agencies on securing networks, systems, and applications. Recommendations include user awareness briefings as well as training for technical staff on security standards, procedures, and sound

security practices. As required by 44 U.S.C. § 3543, Federal agencies must adopt and comply with standards promulgated by NIST, and identify information security protections consistent with these standards.

For example, agencies must complete certification and accreditation (C&A) -- a fundamental security procedure required by law and policy. As of Q1 FY 08, 985 systems (9.5% percent of all systems) operate without a complete C&A. Based on our annual reports to Congress, the percentage of systems C&A'd rise each year we need to be at 100%. When performed correctly, C&As identify the risks when operating an information system, tests controls necessary to mitigate them, and provides program managers a level of assurance the systems supporting their programs operate at an acceptable level of risk.

In addition to following existing policy, agencies are continuing to take advantage of GSA's SmartBUY program when acquiring security products and services. SmartBUY is a Federal government procurement vehicle designed to promote effective enterprise level software management. By leveraging the government's immense buying power, SmartBUY has saved taxpayers millions of dollars through government wide aggregate buying of Commercial Off the Shelf (COTS) software products. Agencies are utilizing new SmartBUY agreements to acquire quality security products at lower costs.

In one recent example, GSA and DoD established a SmartBUY agreement for products certified through the NIST FIPS 140-2 Cryptomodule Validation Program. These certified products will be used to encrypt data at rest. This benefit is not confined solely to Federal agencies, since the Blanket Purchase Agreement (BPA) was written so that states and local governments can also take advantage of this opportunity.

In addition to the encryption BPA, GSA worked to complete two BPA's for credit monitoring services deemed necessary by an agency in the event of a breach of personally identifiable information (PII), as well as risk assessment services for when a breach occurs. More information about the BPA related to credit monitoring services can be found in our OMB Memorandum M-07-04, "Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf. More information about the BPA to assist agencies to assess risk associated with data loss can be found in our OMB Memorandum M-08-10, "Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2008/m08-10.pdf.

Currently, the Information System Security Line of Business (ISSLOB) is working across Federal agencies and with GSA to assess the feasibility of additional security related SmartBUY and BPA opportunities for situational awareness and discovery tool sets.

Managing Multiple Non-Secure External Connections

Agencies connect to the Internet to deliver timely information and services to the public, but each new connection multiplies threats and vulnerabilities. Agencies can consolidate or reduce unnecessary connections while still accomplishing program goals. Per OMB guidance, agencies must reduce and/or consolidate their external connections including those to the internet by June 2008 with a target of no more than 50 access points in total for the civilian agencies.

As agencies reduce the number of internet connections, they are also determining whether to transition, and if so, their transition strategy, to Networx. As you know, FTS2001/Crossover Bridge contracts, which provide services for telecommunications and networking services, for current customers will expire in May and June 2010. The Networx program is the primary replacement vehicle for these expiring contracts. We believe that this transition will provide an opportunity for agencies to consolidate and optimize their external access points including internet connections and obtain secure telecommunications technologies and services. Networx Universal and Enterprise Service contracts were awarded in March and May 2007, respectively.

OMB anticipates agencies choosing to use the Networx contract can leverage the transition process and service offerings to meet the goal of reducing the number of external connections including Internet points of presence. OMB has asked the Federal Chief Information Officers (CIO) Council to prepare a cost-benefit analysis regarding the use of the Networx contract.

The Interagency Management Council's Transition Working Group (TWG) has asked agencies seeking to qualify for transition cost reimbursement to complete Fair Opportunity decisions by September 2008. GSA recommends agencies target the completion of Fair Opportunity decisions by March 2008 to ensure sufficient time to complete transition of services prior to the expiration of FTS2001/Crossover Bridge contracts.

Currently, one major agency has completed a Fair Opportunity Analysis and selected a service provider (Treasury). As of February 2008, GSA has received 21 Statements of Work (SOWs), and anticipates at least 58 more SOWs from major agencies by September 2008.

The TWG deadline for agencies to submit all transition orders is April 2010. GSA recommends agencies target the submission of all transition orders to the extent possible for January 2009 to allow sufficient time for service providers to complete the processing of all orders and establish service on the new contracts before the expiration of FTS2001/Crossover Bridge contracts.

In concert with Networx transition, Einstein will be deployed at the appropriate external connections, including Internet points of presence; 14 departments and/or agencies have

currently deployed Einstein. Einstein is an intrusion detection system managed by DHS to collect, analyze, and share aggregated network computer security information across the Federal government. As a result of these deployments, agencies maintain an awareness of their network while DHS maintains awareness of government-wide information security threats and vulnerabilities. With this information, agencies will be able to quickly take corrective action and reduce their risk to a manageable level.

Agencies are also taking advantage of products and services offered by the Information System Security Line of Business (ISSLOB). This initiative, led by DHS and OMB was introduced in the Spring of 2005. An inter-agency Task Force identified common solutions to be shared across government. The Task Force identified common solutions in four areas: security training; FISMA reporting; situational awareness/incident response; and selection, evaluation and implementation of security solutions.

All agencies were asked to submit proposals to either become a Shared Service Center (SSC) for other agencies, or migrate to another agency from which they would acquire expert security awareness training services and FISMA reporting services. DHS helped coordinate the selection of SSCs, and agency implementation of these services.

As of November 2007, 12 agencies had implemented security awareness training services provided by three approved SSC, and 13 agencies had begun using FISMA reporting services provided by two approved SSC. As a result, agencies are beginning to reduce duplicative investment in common security tools, ensuring a baseline level of training and reporting performance, and are able to refocus their efforts to other complex and critical security issues at their agency. OMB expects agencies will fully report the number of employees trained via the ISSLOB in their fiscal year 2008 annual FISMA report.

Finally, vulnerabilities result from weaknesses in technology as well as improper implementation and oversight of technological products. Over the past year, in collaboration with NIST, the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops which are running Microsoft Windows XP or VISTA. This set of controls, known as the Federal Desktop Core Configuration (FDCC) is currently being implemented across the Federal enterprise. By implementing a common configuration, we are gaining better control of our Federal systems, and allowing for closer monitoring and correction of potential vulnerabilities. Security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. In particular, security configurations help protect connections to the Internet and limit the download of Internet applications to only authorized professionals.

In addition to the desktop configuration, we are also working with the vendor community to make their applications safer. As part of this program, NIST has developed testing tools for use by both Federal agencies and vendors. NIST awarded Security Content Automation Protocol (SCAP) Validation to three products as of February 4, 2008. These products and their associated validation information can be found at http://nvd.nist.gov/scapproducts.cfm. Three independent laboratories have been

accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) for SCAP Product Validation testing. The list of accredited labs is available at the same URL. We are very optimistic this program will greatly enhance the security of our Federal desktops, and, of our Federal enterprise as a whole. To help agency procurement officers ensure that new acquisitions include common security configurations, we have provided agencies with recommended procurement language. This language can be found in our Memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf. Currently, the Federal Acquisition Council is in the process of adding similar language to the Federal Acquisition Regulation.

These initiatives described in my testimony today in combination with other Administration initiatives (including: IPv6, HSPD-12, minimum communications capabilities for continuity of government and continuity of operation plans, and IT Infrastructure Line of Business) address our potential security gaps, help agencies optimize their information infrastructure, and facilitate appropriate network consolidation and configuration. In turn, agencies will be able to better manage their information infrastructure, allowing them to reduce risks to an acceptable level.

In closing, OMB is committed to a Federal government with resilient information systems. The dangers posed by the Internet must not be allowed to significantly affect agency business processes or disrupt services to the citizen. I would like to acknowledge the significant work of agencies and IGs in conducting the annual reviews and evaluations. This effort gives OMB and the Congress much greater visibility into agency security status and progress.

While notable progress in resolving IT security weaknesses has been made, problems remain in agency implementation and new threats and vulnerabilities continue to materialize. Work remains to continue to improve the security of the information and systems supporting the Federal government's missions and manage the risk associated with these systems. To address these challenges, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets.