STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, AND INTERNATIONAL SECURITY
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

July 28, 2006

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about cyber security: recovery and reconstitution of critical networks.

The President has directed Federal agencies to work with State and local governments as well as the private sector to enhance the protection of our Nation’s critical infrastructure. The Department of Homeland Security (DHS) is coordinating this effort.

The Office of Management and Budget (OMB) oversees the implementation of government-wide policies, standards, and guidelines for the Federal government’s information technology security programs. My testimony today will focus on OMB activities to improve the security and resilience of the Federal government’s critical cyber assets.

Maintaining Telecommunication Services During a Crisis or Emergency

Last year, the Director of OMB issued a regulation (M-05-16 dated June 30, 2005) on maintaining telecommunication services during a crisis or emergency. This regulation was issued in response to Section 414 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act. The regulation required each agency to review its telecommunication capabilities in the context of planning for contingencies and continuity of operations situations.

OMB also asked each agency to confirm they were complying with directives issued by the National Communications System (NCS) and guidance issued by the Federal Emergency Management Agency (FEMA). As background, NCS was established by Executive Order 12472 in 1984 and has a unique status and set of responsibilities regarding national security/emergency preparedness (NS/EP) telecommunications within the federal government. NCS directives establish policies and procedures for NS/EP telecommunications, and FEMA provides guidance to Federal Executive branch departments and agencies for use in developing contingency plans and programs for continuity of operations.

In August 2005, all large agencies submitted reports on the status of their telecommunication services. In addition, forty small and independent agencies provided the requested information. OMB and NCS worked together to review the responses. Our analysis revealed the need for additional guidance to the agencies regarding the use of redundant and physically separate telecommunications service entry points into buildings and the use of physically diverse local network facilities.

In October 2005, the NCS hosted a Route Diversity Forum outlining route diversity theory and highlighting the procedures for agency self-assessment and NCS suggested ways to ensure adequate route diversity. Over seventy Federal agency representatives attended the forum. NCS has recently developed a Route Diversity Methodology enabling agencies to self-assess their facilities to determine their level of route diversity. Information regarding this methodology is available on the NCS website.

Procurement of Telecommunication Services

When an agency initiates new telecommunications procurements, the agency must determine the appropriate level of availability, performance and restoration that is required, in accordance with the agency's continuity of operations plans.

The General Service Administration's Networx program will serve as the primary replacement for the expiring FTS2001 telecommunications contracts. The Networx procurements will specify telecommunications infrastructure security requirements to protect contractor network services, infrastructures, and information processing resources against cyber and physical threats, attacks, or system failures. Networx contractors must comply with security law and policy such as OMB Circular A-130, the Federal Information Security Management Act and the National Institute of Standards and Technology Federal Information Processing Standards.

In developing Networx, GSA has defined a full spectrum of Security Services to meet individual agency needs. These include Managed Tiered Security Service with different network security levels, Managed Firewall Service, Intrusion Detection and Prevention Service, Managed E-Authentication Service, Vulnerability Scanning Service, Anti-Virus Management Service, Incident Response Service, and Secured Managed E-mail Service.

With regard to recovery and reconstitution of critical networks, the Networx program specifies telecommunications requirements for compliance with NS/EP directives, as established by the NCS in accordance with Executive Order 12472. This will ensure that Networx telecommunications capabilities are continuously ready to meet the needs of Federal agencies during national emergencies. Additionally, Networx will fully interoperate with the NCS's Government Emergency Telecommunications System and Wireless Priority System.

Identification and Protection of Critical Cyber Infrastructure

On December 17, 2003, the President signed Homeland Security Presidential Directive (HSPD) -7, "Critical Infrastructure Identification, Prioritization and Protection." This directive established the national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

HSPD-7 required the heads of all Federal agencies to develop and submit to the Director of OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they owned or operated. The plans were due July 31, 2004. All agencies with HSPD-7 responsibilities submitted the protection plans.

In OMB's reporting guidance, we asked agencies to address critical infrastructure identification, prioritization, protection, and contingency planning to include the recovery and reconstitution of essential capabilities. Twenty four agencies confirmed they owned or operated nationally critical systems and assets. These are assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, or public health or safety.

OMB worked with DHS' National Cyber Security Division to develop scoring criteria and evaluate the protection plans. We provided each agency with a written response explaining our approval or disapproval of the agency's cyber security plan and highlighting areas where improvement was needed.

The evaluations conducted in 2005 have been used to inform DHS' development of the National Infrastructure Protection Plan (NIPP). The NIPP will provide for a more detailed analysis of critical infrastructure inside the federal government.

In May 2005, OMB added continuity of operations planning criteria to the President's Management Agenda scorecard. All agencies wishing to maintain green status on the E-Government scorecard are required to test their contingency plans on an annual basis. OMB tracks statistics related to contingency plan testing through quarterly performance updates provided by the agencies in fulfillment of Federal Information Security Management Act (FISMA) policies.

Improving the Security of Federal Information Systems

Each year, as required by FISMA, agency Chief Information Officers and program officials conduct IT security reviews of the systems that support their programs. Additionally, agency Inspectors General are asked to perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews are reported annually to OMB. As part of their evaluations, agencies are asked to categorize their information systems, including contractor systems into high, moderate, or low impact and document the security controls implemented for each. OMB has stated as a rebuttable presumption all cyber critical infrastructure and key resources identified in an agency's HSPD-7 plans are high impact as are all systems identified as necessary to support agency continuity of operations. Systems necessary for continuity of operations purposes include for example, telecommunication systems identified in agency reviews under OMB's regulation on maintaining telecommunications service during a crisis.

OMB has found agency senior managers are paying greater attention to IT security. Chief Information Officers maintain plans of action and milestones (POA&Ms) to ensure program and system level IT security weaknesses are tracked and corrected. The agencies include in their plans the name of the person responsible for correcting the weakness, the resources required and the target completion date. The plans are updated by the agencies on a quarterly basis and agencies report their status and progress to OMB. These updates help to inform the quarterly assessment of the President's Management Agenda scorecard.

Incident Response

The National Cyber Response Coordination Group (NCRCG) is the principal federal interagency mechanism to coordinate preparation for and response to cyber incidents of national significance. The group is co-chaired by DHS, the Department of Justice and the Department of Defense. OMB is a member of the group along with other agencies having a statutory role in cyber security, cybercrime, or protection of critical infrastructure. Member-agencies meet on a monthly basis to identify issues and concerns.

During a cyber incident, the member agencies would integrate their capabilities in order to assess the scope and severity of the incident, govern response and remediation efforts, and guide senior policymakers. The NCRCG would use their established relationships with the private sector and state and local governments to help manage a cyber crisis and develop recovery strategies.

In February 2006, DHS sponsored the national level cyber exercise "Cyber Storm." During this exercise, NCRCG member agencies tested their concept of operations as well as communications with critical infrastructures. Additionally, in June 2006, DHS staged the fourth Top Officials Command Post Exercise (TopOff) to test the government's response to terrorist events. The exercise involved over 4,000 representatives from federal, state and local governments along with private sector participants.

Conclusion

In conclusion, each agency is responsible for ensuring the continued availability of its mission essential and national security/emergency preparedness telecommunications services. Strategic improvements in security and continuity of operations planning can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. The Administration is committed to a federal government with secure and resilient information systems. We will continue to work with agencies, Congress and the GAO to ensure appropriate risk-based and cost-effective IT security programs, policies and procedures are put in place to protect the Federal government’s critical cyber infrastructure.