Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks

Release Date: April 8, 2008

Information technology has grown to provide both government and the private sector with an efficient and timely means of delivering essential services around the world. As a result, these critical systems remain at risk from potential attacks via the Internet. It is the policy of the United States to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, the economy, government services, and the national security of the United States.

The Federal Government is continually increasing capabilities to address cyber risk associated with critical networks and information systems. On January 8, 2008, President Bush approved National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which formalized a series of continuous efforts designed to further safeguard Federal Government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats.

While efforts to protect our Federal network systems from cyber attacks remain a collaborative, government-wide effort, the Department of Homeland Security (DHS) has the lead responsibility for assuring the security, resiliency and reliability of the Nation's Information Technology (IT) and communications infrastructure. Current measures to prevent future attacks and intrusion attempts include:

- Hiring additional personnel to support the **U.S. Computer Emergency Readiness Team (US-CERT)**, DHS' 24x7 watch and warning center for the Federal Government's Internet infrastructure. US-CERT, a public/private partnership, operates around-the-clock to help government and industry analyze and respond to cyber threats and vulnerabilities.

- Expanding the **EINSTEIN Program** to all Federal departments and agencies. This will provide government officials with an early warning system to gain better situational awareness, earlier identification of malicious activity, and a more comprehensive network defense. The EINSTEIN Program helps identify unusual network traffic patterns and trends which signal unauthorized network traffic so security personnel are able to quickly identify and respond to potential threats.

- Consolidating the number of external connections including Internet points of presence for the Federal Government Internet infrastructure, as part of the Office of Management and Budget's (OMB) **"Trusted Internet Connections Initiative,"** will more efficiently manage and implement security measures to help bring more comprehensive protection across the federal ".gov" domains.

- Creating a **National Cybersecurity Center** to further our progress in addressing cyber threats and increasing cybersecurity efforts. This Center will bring together federal cybersecurity organizations, by virtually connecting and in some cases, physically collocating personnel and resources to gain a clearer understanding of the overall cyber security picture of Federal networks. Secretary Chertoff appointed Rod Beckstrom on March 20, 2008 to serve as Director of the National Cyber Security Center.

- Expanding the **National Cyber Investigative Joint Task Force** (NCIJTF), to include representation from the U.S. Secret Service and several other federal agencies. This existing cyber investigation coordination organization overseen by the Federal Bureau of Investigation will serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations.

- Working towards a **stronger supply chain defense** to reduce the potential for adversaries to manipulate IT and communications products before they are imported into the U.S. To address this challenge, the Federal Government is exploring protections into our federal acquisition process and developing a multi-faceted strategy to reduce risk at the most appropriate stage of the IT and communications product lifecycle.

- Facilitate coordination and information sharing between the Federal Government and private sector to reduce cyber risk, disseminate threat information, share best practices and apply appropriate protective actions as outlined within the **National Infrastructure Protection Plan (NIPP)** framework. For example, DHS created a Control Systems Vulnerability Assessment Tool to help all critical infrastructure sectors assess certain policies, plans and procedures currently in place to reduce cyber vulnerabilities and leverage recognized standards.

- Led the nation's largest cyber security exercise, known as **Cyber Storm II,** in March 2008, bringing together participants from federal, state and local governments, the private sector, and the international community in order to examine and strengthen the nation's cyber security preparedness and response capabilities in response to a simulated cyber attack across several critical sectors of our economy. Cyber Storm II and other exercises help ensure that public and private sectors are prepared for an effective response to attacks against our critical systems and networks.

- Partnering with academia and industry to **expand cyber education** for all U.S. Government employees, particularly those who specialize in IT, and enhance worksite development and recruitment strategies to ensure a knowledgeable workforce capable of dealing with the evolving nature of cyber threats.

- **Increasing funding for IT security** through the President's FY 2009 Budget Request of $7.2 billion for these efforts, an increase of $600 million over the $6.6 billion dedicated to this area in FY 2008 across the Federal Government.

###

This page was last reviewed/modified on April 8, 2008.