ADDITIONAL RESOURCES

The National Strategy to Secure Cyberspace

A White House Report

Cybersecurity is cited as a critical element of homeland security in a national strategy crafted by the Bush Administration.

In February 2003, the White House released The National Strategy to Secure Cyberspace, a 76-page document outlining a sustained, multi-faceted approach to safeguarding the nation's vital communications technologies. The strategy was developed after several years of intense consultations among thousands of individuals—officials at all levels of government, experts from the private sector, and other concerned citizens. The following excerpts reflect the course the United States pursuing to protect the complex, inter-connected, computer-based systems vital to today's society.

Critical Priorities for Cyberspace Security

The National Strategy to Secure Cyberspace articulates five national priorities including:

I. A National Cyberspace Security Response System;

II. A National Cyberspace Security Threat and Vulnerability Reduction Program;

III. A National Cyberspace Security Awareness and Training Program;

IV. Securing Governments' Cyberspace; and

V. National Security and International Cyberspace Security Cooperation.

The first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events. The second, third, and fourth priorities aim to reduce threats from, and our vulnerabilities to, cyber attacks. The fifth priority is to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

Priority I: A National Cyberspace Security Response System

Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to be effective at a national level, the United States needs a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Privacy and civil liberties must be protected in the process. Because no cybersecurity plan can be impervious to concerted and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly.

The National Strategy to Secure Cyberspace identifies eight major actions and initiatives for cyberspace security response:

1. Establish a public-private architecture for responding to national-level cyber incidents;

2. Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments;

3. Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace;

4. Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;

5. Improve national incident management;

6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;

7. Exercise cybersecurity continuity plans for federal systems; and

8. Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities.

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. Lesser-secured sites on the interconnected network of networks also present potentially significant exposures to cyber attacks. Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products.

The National Strategy to Secure Cyberspace identifies eight major actions and initiatives to reduce threats and related vulnerabilities:

1. Enhance law enforcement's capabilities for preventing and prosecuting cyberspace attacks;

2. Create a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities;

3. Secure the mechanisms of the Internet by improving protocols and routing;

4. Foster the use of trusted digital control systems/supervisory control and data acquisition systems;

5. Reduce and remediate software vulnerabilities;

6. Understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications;

7. Prioritize federal cybersecurity research and development agendas; and

8. Assess and secure emerging systems.

Priority III: A National Cyberspace Security Awareness Training Program

Many cyber vulnerabilities exist because of a lack of cybersecurity awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers (CIOs), chief executive officers, and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructures regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multilevel certification programs for cybersecurity professionals complicate the task of addressing cyber vulnerabilities.

The National Strategy to Secure Cyberspace identifies four major actions and initiatives for awareness, education, and training:

1. Promote a comprehensive national awareness program to empower all Americans — businesses, the general workforce, and the general population—to secure their own parts of cyberspace;

2. Foster adequate training and education programs to support the Nation's cybersecurity needs;

3. Increase the efficiency of existing federal cybersecurity training programs; and

4. Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications.

Priority IV: Securing Governments' Cyberspace

Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services in the agriculture, food, water, public health, emergency services, defense, social welfare, information and telecommunications, energy, transportation, banking and finance, chemicals, and postal and shipping sectors that depend upon cyberspace for their delivery. Governments can lead by example in cyberspace security, including fostering a marketplace for more secure technologies through their procurement.

The National Strategy to Secure Cyberspace identifies five major actions and initiatives for the securing of governments' cyberspace:

1. Continuously assess threats and vulnerabilities to federal cyber systems;

2. Authenticate and maintain authorized users of federal cyber systems;

3. Secure federal wireless local area networks;

4. Improve security in government outsourcing and procurement; and

5. Encourage state and local governments to consider establishing information technology security programs and participate in information sharing and analysis centers with similar governments.

Priority V: National Security and International Cyberspace Security Cooperation

America's cyberspace links the United States to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding and defending its critical systems and networks. Enabling our ability to do so requires a system of international cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.

The National Strategy to Secure Cyberspace identifies six major actions and initiatives to strengthen U.S. national security and international cooperation:

1. Strengthen cyber-related counterintelligence efforts;

2. Improve capabilities for attack attribution and response;

3. Improve coordination for responding to cyber attacks within the U.S. national security community;

4. Work with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global "culture of security;"

5. Foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge; and

6. Encourage other nations to accede to the Council of Europe Convention on Cybercrime, or to ensure that their laws and procedures are at least as comprehensive.

The complete text of The National Strategy to Secure Cyberspace is available at www.whitehouse.gov/pcipb.