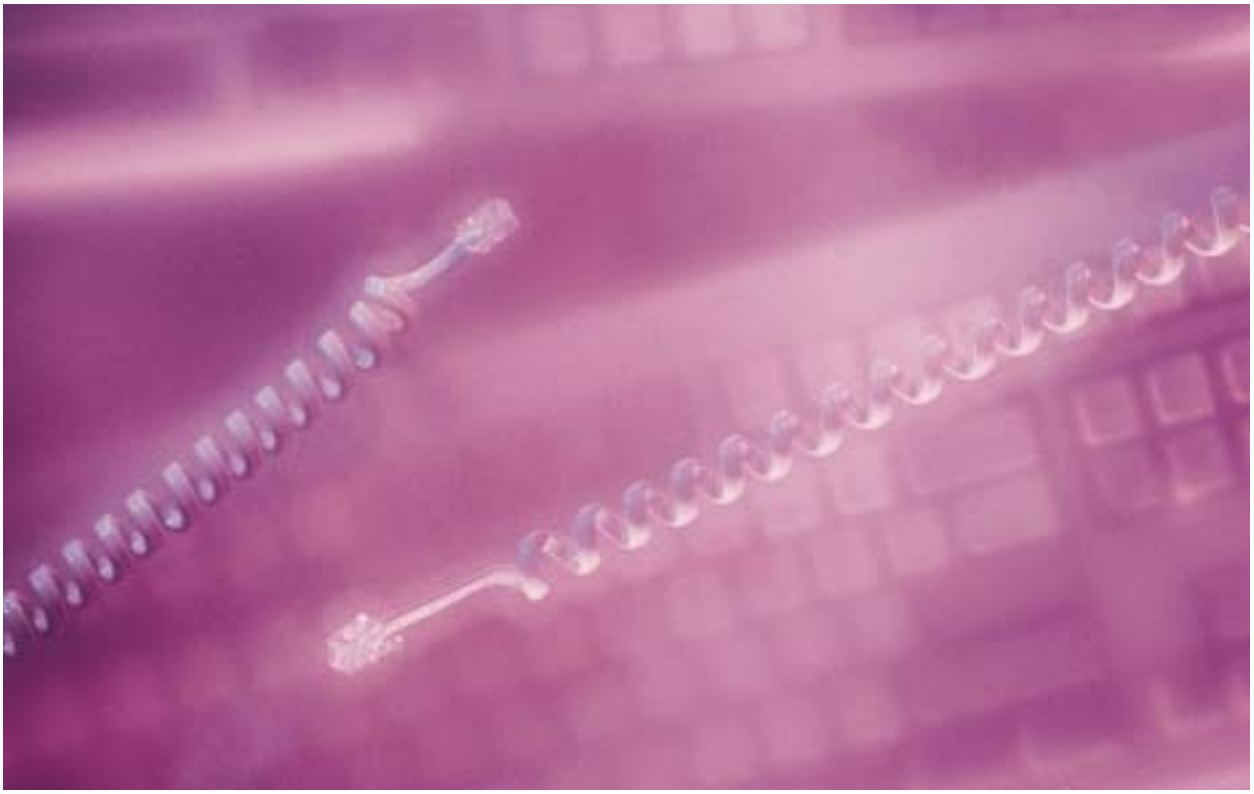

Introduction

A Nation in Cyberspace

Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. Unfortunately, recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them. (See, *Cyberspace Threats and Vulnerabilities*.)

This *National Strategy to Secure Cyberspace* is part of an overall effort to protect the Nation. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control, or with which they interact. Securing

cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.

A Unique Problem, a Unique Process

Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from private-sector and academic innovation. Government alone cannot sufficiently secure cyberspace. Thus, President Bush has called for voluntary partnerships among government, industry, academia, and nongovernmental groups to secure and defend cyberspace. (See, *National Policy and Guiding Principles*.)

In recognition of this need for partnership, the process to develop the *National Strategy to Secure Cyberspace* included soliciting views from both the public and private sectors. To do so, the White House sponsored town hall meetings on cyberspace security in ten metropolitan areas. Consequently, individual sectors (e.g., higher education, state and local government, banking and finance) formed workgroups to create initial sector-specific cyberspace security strategies. Additionally, the White House created a Presidential advisory panel, the National Infrastructure Advisory Council, consisting of leaders from the key sectors of the economy, government, and academia. The President's National Security Telecommunications Advisory Committee reviewed and commented on the *Strategy*.

In September 2002, the President's Critical Infrastructure Protection Board sought comments from individuals and institutions nationwide by placing a draft version of the *Strategy* online for review. Thousands participated in the town hall meetings and provided comments online. Their comments contributed to shaping the *Strategy* by narrowing its focus and sharpening its priorities.

This process recognizes that we can only secure cyberspace successfully through an inclusive national effort that engages major institutions throughout the country. The federal government designed the *Strategy* development process to raise the Nation's level of awareness of the importance of cybersecurity. Its intent was to produce a *Strategy* that many Americans could feel they had a direct role in developing, and to which they would be committed.

Although the redrafting process reflects many of the comments provided, not everyone will agree with each component of the *National Strategy to Secure Cyberspace*. Many issues could not be addressed in detail, and others are not yet ripe for national policy. The *Strategy* is not immutable; actions will evolve as technologies advance, as threats and vulnerabilities change, and as our understanding of the cybersecurity issues improves and clarifies. A national dialogue on cyberspace security must therefore continue.

In the weeks following the release of the draft *Strategy*, Congress approved the creation of the Department of Homeland Security (DHS), assigned to it many agencies that are active in cybersecurity, and directed it to perform new cybersecurity missions. This *Strategy* reflects those changes. Congress passed and the President signed the *Cyber Security Research and Development Act* (Public Law 107-305), authorizing a multi-year effort to create more secure cyber technologies, to expand cybersecurity research and development, and to improve the cybersecurity workforce.

Five National Cyberspace Security Priorities

The *National Strategy to Secure Cyberspace* is a call for national awareness and action by individuals and institutions throughout the United States, to increase the level of cybersecurity nationwide and to implement continuous processes for identifying and remedying cyber vulnerabilities. Its framework is an agenda of

five broad priorities that require widespread voluntary participation. Each individual program consists of several components, many of which were drawn from the draft *Strategy's* recommendations and related public comments.

Addressing these priorities requires the leadership of DHS as well as several other key federal departments and agencies. As part of the Office of Management and Budget (OMB)-led budget process, and with the support of Congress, these departments and agencies now have the task of translating the *Strategy's* recommendations into actions.

Corporations, universities, state and local governments, and other partners are also encouraged to take actions consistent with these five national cyberspace security priorities, both independently and in partnership with the federal government. Each private-sector organization must make its own decisions based on cost effectiveness analysis and risk-management and mitigation strategies.

The *National Strategy to Secure Cyberspace* articulates five national priorities. The first priority focuses on improving our ability to respond to cyber incidents and reduce the potential damage from such events. The second, third, and fourth priorities aim to reduce the numbers of cyber threats and our overall vulnerability to cyber attacks. The fifth priority focuses on preventing cyber attacks with the potential to impact national security assets and improving 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 take place effectively at a national level, the United States requires 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 attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. To prepare for the possibility of major cyber attacks, America needs a national cyber disaster recovery plan. The National Cyberspace Security Response System will involve public and private institutions and cyber centers to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

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

By exploiting vulnerabilities in our cyber systems, an organized cyber attack may endanger the security of our Nation's critical infrastructures. Cyberspace vulnerabilities occur in the critical infrastructure enterprises and government departments themselves, in their external supporting structures (such as the mechanisms of the Internet), and in unsecured sites across the interconnected network of networks. Vulnerabilities exist for several reasons including technological weaknesses, poor security-control implementation, and absences of effective oversight.

A National Cyberspace Security Threat and Vulnerability reduction program will include coordinated national efforts conducted by governments and the private sector to identify and remediate the most serious cyber vulnerabilities through collaborative activities, such as sharing best practices and evaluating and implementing new technologies. Additional program components will include raising cybersecurity awareness, increasing criminal justice activities, and developing national security programs to deter future cyber threats.

Priority III: A National Cyberspace Security Awareness and Training Program

Many information-system vulnerabilities exist because of a lack of cyberspace security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers, chief executive officers, and corporate boards. These vulnerabilities can present serious risks to the infrastructures even if they are not actually part of the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certifications for personnel further complicate the task of reducing vulnerabilities.

The National Cyberspace Security Awareness and Training Program will raise cybersecurity awareness in companies, government agencies, universities, and among the Nation's computer users. It will further address shortfalls in the numbers of trained and certified cybersecurity personnel.

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 that rely on each of the critical infrastructure sectors, which are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. With respect to investment in cyberspace security, government can lead by example by fostering a marketplace for more secure technologies through large procurements of advanced information assurance technologies. A program to implement such products will help to ensure that federal computer systems and networks are secure. The federal government will also assist state and local governments with cybersecurity awareness, training, and information exchange.

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—regardless of where an attack originates. Facilitating our ability to do so requires a system of international cooperation to enable the information sharing, reduce vulnerabilities, and deter malicious actors.

Actions and Recommendations

The *Strategy* highlights actions that the federal government will take and makes recommendations to our partners in nongovernmental organizations. The actions and recommendations (A/R) are italicized throughout the Strategy and numbered according to the associated priority. For example A/R 1-1 is the first action or recommendation in Priority I. Appendix A provides a summary of all of the A/Rs proposed.