Executive Summary

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of 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 their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

This *National Strategy to Secure Cyberspace* is part of our overall effort to protect the Nation. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *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, 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.

The *National Strategy to Secure Cyberspace* outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The *Strategy* highlights the role of public-private engagement. The document provides a framework for the contributions that we all can make to secure our parts of cyberspace. The dynamics of cyberspace will require adjustments and amendments to the *Strategy* over time.

The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all. Therefore, the *National Strategy to Secure Cyberspace* helps reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them.

Strategic Objectives

Consistent with the *National Strategy for Homeland Security*, the strategic objectives of this *National Strategy to Secure Cyberspace* are to:

- Prevent cyber attacks against America's critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur.

Threat and Vulnerability

Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.

A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security. The required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date. We should not, however, be too sanguine. There have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities.

Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.

In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.

Cyber attacks on United States information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures.

The Government Role in Securing Cyberspace

In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government response is most appropriate and justified. Looking inward, providing continuity of government requires ensuring the safety of its own cyber infrastructure and those assets required for supporting its essential missions and services. Externally, a government role in cybersecurity is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under provisioning of critical shared resources; and raising awareness.

Public-private engagement is a key component of our Strategy to secure cyberspace. This is true for several reasons. Public-private partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

A federal role in these and other cases is only justified when the benefits of intervention outweigh the associated costs. This standard is especially important in cases where there are viable private sector solutions for addressing any potential threat or vulnerability. For each case, consideration should be given to the broad-based costs and impacts of a given government action, versus other alternative actions, versus non-action, taking into account any existing or future private solutions.

Federal actions to secure cyberspace are warranted for purposes including: forensics and attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against organized attacks capable of inflicting debilitating damage to the economy. Federal activities should also support research and technology development that will enable the private sector to better secure privately-owned portions of the Nation's critical infrastructure.

Department of Homeland Security and Cyberspace Security

On November 25, 2002, President Bush signed legislation creating the Department of Homeland Security (DHS). This new cabinet-level department will unite 22 federal entities for the common purpose of improving our homeland security. The Secretary of DHS will have important responsibilities in cyberspace security. These responsibilities include:

- Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems;
- Coordinating with other agencies of the federal government to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and nongovernmental organizations including

the private sector, academia, and the public; and

- Performing and funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

Consistent with these responsibilities, DHS will become a federal center of excellence for cybersecurity and provide a focal point for federal outreach to state, local, and nongovernmental organizations including the private sector, academia, and the public.

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 and 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, multi-level 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.

A National Effort

Protecting the widely distributed assets of cyberspace requires the efforts of many Americans. The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, and participation in, public-private partnerships to raise cybersecurity awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations.

People and organizations across the United States have already taken steps to improve cyberspace security. On September 18, 2002, many private-sector entities released plans and strategies for securing their respective infrastructures. The Partnership for Critical Infrastructure Security has played a unique role in facilitating private-sector contributions to this Strategy. Inputs from the critical sector's themselves can be found at http://www.pcis.org. (These documents were not subject to government approval.)

These comprehensive infrastructure plans describe the strategic initiatives of various sectors, including:

- Banking and Finance;
- Insurance;
- Chemical;
- Oil and Gas;
- Electric;
- Law Enforcement;
- Higher Education;
- Transportation (Rail);
- Information Technology and Telecommunications; and
- Water.

As each of the critical infrastructure sectors implements these initiatives, threats and vulnerabilities to our infrastructures will be reduced.

For the foreseeable future two things will be true: America will rely upon cyberspace and the federal government will seek a continuing broad partnership with the private sector to develop, implement, and refine a *National Strategy to Secure Cyberspace*.