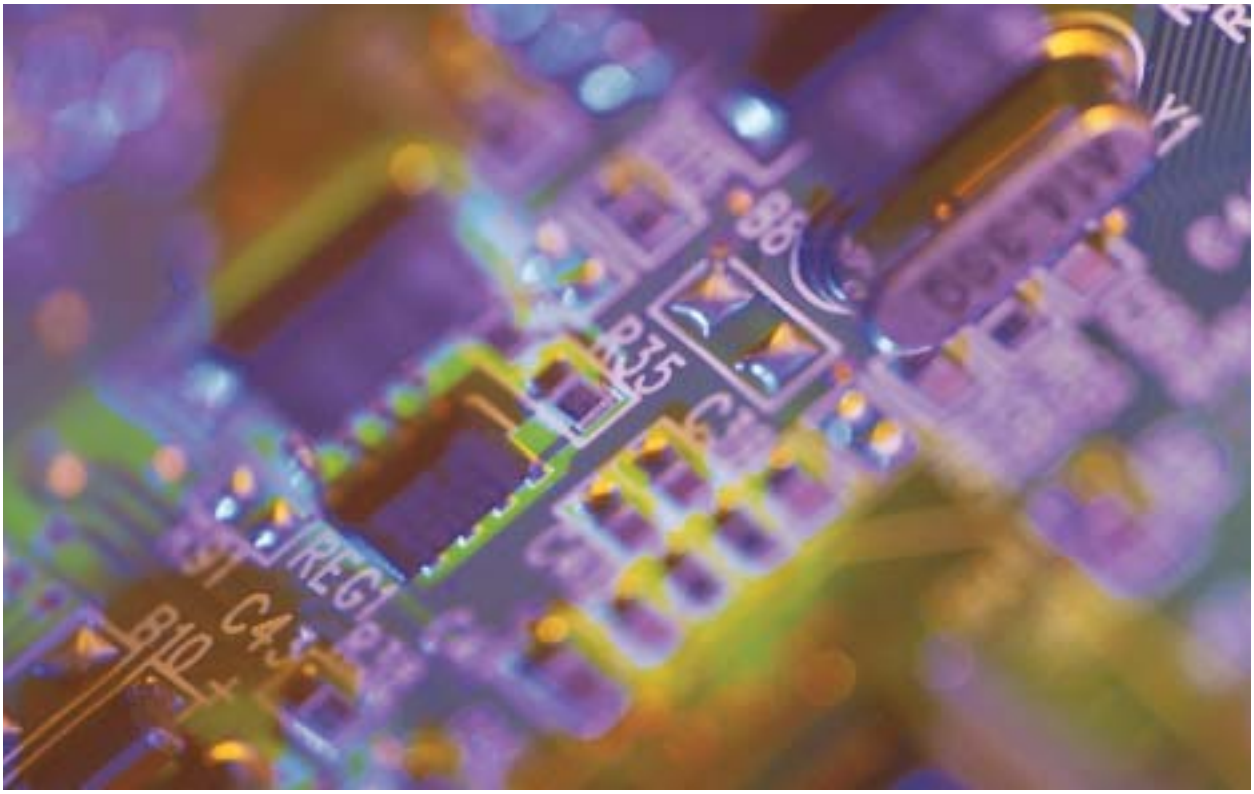

National Policy and Guiding Principles

National Policy, Principles, and Organization

This section describes the national policy that shapes the *National Strategy to Secure Cyberspace* and the basic framework of principles within which it was developed. It also outlines the roles and missions of federal agencies.

National Policy

The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. These three functions now depend on an interdependent network of critical information infrastructures that we refer to as "cyberspace."

It is the policy of the United States to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services, and the national security of the United States. Disruptions that do occur should be infrequent, of minimal duration and manageable and cause the least damage possible. The policy requires a continuous effort to secure information systems for critical infrastructure and includes voluntary public-private partnerships involving corporate and nongovernmental organizations.

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

- Prevent cyber attacks against our critical infrastructures;
- Reduce our national vulnerabilities to cyber attack; and,
- Minimize the damage and recovery time from cyber attacks that do occur.

Guiding Principles

In January 2001, the Administration began to review the role of information systems and cybersecurity. In October 2001, President Bush issued Executive Order 13231, authorizing a protection program that consists of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems. The Federal Information Security Management Act (FISMA) and Executive Order 13231, together with other relevant Presidential directives and statutory authorities, provide the framework for executive branch cyberspace security activities.

The protection of these cyber systems is essential to every sector of the economy. The development and implementation of this program directive has been guided by the following organizing principles:

1. *A National Effort:* Protecting the widely distributed assets of cyberspace requires the efforts of many Americans. The federal government alone cannot 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. The government's role in securing cyberspace includes promoting better security in privately owned infrastructures when there is a need to:
    - Convene and facilitate discussions between and with nongovernmental entities;
    - Identify instances where the "tragedy of the commons" can affect homeland, national, and economic security; and
    - Share information about cyber threats and vulnerabilities so nongovernmental entities can adjust their risk management strategies and plans, as appropriate.

    In every case, the scope for government involvement is limited to those cases when the benefits of intervention outweigh the direct and indirect costs.

    Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government promotes the creation of, and participation in, public-private partnerships to raise awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations. Many sectors have undertaken the important step of developing ISACs, which facilitate communication, the development of best practices, and the dissemination of security-related information. In addition, various sectors have developed plans to secure their parts of cyberspace, which complement this *Strategy*, and the government intends for this productive and collaborative partnership to continue.
2. *Protect Privacy and Civil Liberties:* The abuse of cyberspace infringes on our privacy and our liberty. It is incumbent on the federal government to avoid such abuse and infringement. Cybersecurity and personal privacy need not be opposing goals. Cyberspace security programs must strengthen, not weaken, such protections. Accordingly, care must be taken to respect privacy interests and

other civil liberties. Consumers and operators must have confidence their voluntarily shared, nonpublic information will be handled accurately, confidentially, and reliably. The federal government will lead by example in implementing strong privacy policies and practices in the agencies. As part of this process, the federal government will consult regularly with privacy advocates and experts.

3. *Regulation and Market Forces:* federal regulation will not become a primary means of securing cyberspace. Broad regulations mandating how all corporations must configure their information systems could divert more successful efforts by creating a lowest-common-denominator approach to cybersecurity, which evolving technology would quickly marginalize. Even worse, such an approach could result in less secure and more homogeneous security architectures than we have now. By law, some federal regulatory agencies already include cybersecurity considerations in their oversight activity. However, the market itself is expected to provide the major impetus to improve cybersecurity.

4. *Accountability and Responsibility:* The *National Strategy to Secure Cyberspace* is focused on producing a more resilient and reliable information infrastructure. When possible, it designates lead executive branch departments or agencies for federal cyberspace security initiatives. On November 25, 2002, the President signed the *Homeland Security Act of 2002* establishing the Department of Homeland Security (DHS). DHS will be responsible for many of the initiatives outlined in the *National Strategy to Secure Cyberspace*. The *Strategy* also recommends actions federal, state and local governments, the private sector, and the American people can take to help secure cyberspace.

5. *Ensure Flexibility:* Cyber threats change rapidly. Accordingly, the *National Strategy to Secure Cyberspace* emphasizes flexibility in our ability to respond to cyber attacks and manage vulnerability reduction. The rapid development of attack tools provides potential attackers with a strategic advantage to adapt their offensive tactics quickly to target perceived weaknesses in networked information systems and organizations' abilities to respond. Flexible planning allows organizations to reassess priorities and realign resources as the cyber threat evolves.

6. *Multi-Year Planning:* Securing cyberspace is an ongoing process, as new technologies appear and new vulnerabilities are identified. The *National Strategy to Secure Cyberspace* provides an initial framework for achieving cyberspace security objectives. Departments and agencies should adopt multi-year cybersecurity plans for sustaining their respective roles. Other public- and private-sector organizations are also encouraged to consider multi-year plans.

Department of Homeland Security and Cyberspace Security

DHS unites 22 federal entities for the common purpose of improving homeland security. The Department also creates a focal point for managing cyberspace incidents that could impact the federal government or even the national information infrastructures. The Secretary of Homeland Security will have important responsibilities in cyberspace security, including:

- Developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States, including information technology and telecommunications systems (including

CRITICAL INFRASTRUCTURE LEAD AGENCIES

LEAD AGENCY	SECTORS
Department of Homeland Security	• Information and Telecommunications • Transportation (aviation, rail, mass transit, waterborne commerce, pipelines, and highways (including trucking and intelligent transportation systems) • Postal and Shipping • Emergency Services • Continuity of Government
Department of the Treasury	• Banking and Finance
Department of Health and Human Services	• Public Health (including prevention, surveillance, laboratory services, and personal health services) • Food (all except for meat and poultry)
Department of Energy	• Energy (electric power, oil and gas production, and storage)
Environmental Protection Agency	• Water • Chemical Industry and Hazardous Materials
Department of Agriculture	• Agriculture • Food (meat and poultry)
Department of Defense	• Defense Industrial Base

satellites) and the physical and technological assets that support such systems;

- Providing crisis management support in response to threats to, or attacks on, critical information systems;
- Providing technical assistance to the private sector and other governmental entities with respect to emergency recovery plans that respond to major failures of critical information systems;
- Coordinating with other federal agencies to provide specific warning information and advice about appropriate protective measures and countermeasures to state and local government agencies and authorities, the private sector, other entities, 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.

Designation of Coordinating Agencies

A productive partnership between the federal government and the private sector depends on effective coordination and communication. To facilitate and enhance this collaborative structure, the government has designated a "Lead Agency" for each of the major sectors of the economy vulnerable to infrastructure attack. In addition, the Office of Science and Technology Policy (OSTP) coordinates research and development to support critical infrastructure protection. The Office of Management and Budget (OMB) oversees the implementation of governmentwide policies, principles, standards, and guidelines for federal government computer security programs. The Department of State coordinates international outreach on cybersecurity. The Director of Central Intelligence is responsible for assessing the foreign threat to U.S. networks and information systems. The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) lead the national effort to investigate and prosecute cybercrime.

The government will continue to support the development of public-private partnerships. Working together, sector representatives and federal lead agencies assess their respective sectors' vulnerabilities to cyber or physical attacks and, accordingly, recommend plans or measures to eliminate significant exposures. Both technology and the threat environment can change rapidly. Therefore, sectors and lead agencies should frequently assess the reliability, vulnerability, and threat environments of the Nation's infrastructures and employ appropriate protective measures and responses to safeguard them.

The government's full authority, capabilities, and resources must be available to support critical infrastructure protection efforts. These include, as appropriate, crisis management, law enforcement, regulation, foreign intelligence, and defense preparedness.