The President's Critical Infrastructure Protection Board

THE NATIONAL STRATEGY TO SECURE CYBERSPACE

For Comment

SEPTEMBER 2002

DRAFT

CONTENTS

PRESIDENT'S CRITICAL INFRASTRUCTURE
PROTECTION BOARD

SEPTEMBER 18, 2002

Subject: *A National Strategy to Secure Cyberspace*

President Bush directed the development of a *National Strategy to Secure Cyberspace* to ensure that America has a clear road map to protect a part of its infrastructure so essential to our way of life. On the pages that follow is a draft of that road map, developed in close collaboration with key sectors of the economy that rely on cyberspace, State and local governments, colleges and universities, and concerned organizations.

These public-private partnerships that formed in response to the President's call have developed their own strategies to protect the parts of cyberspace on which they rely. They are made available online today. Other groups, representing other sectors, have recently formed, and have begun the process of developing strategies. Town hall meetings were held around the country, and fifty three clusters of key questions were published to spark public debate. Even more input is needed. This unique partnership and process is necessary because the majority of the country's cyber resources are controlled by entities outside of government. For the Strategy to work, it must be a plan in which a broad cross-section of the country is both invested and committed.

Eight more town hall meetings will be held around the country in the next few weeks to further solicit and receive the views of concerned citizens. Comments on the *National Strategy to Secure Cyberspace* may be sent via the feedback link at **www.securecyberspace.gov** by November 18, 2002. The National Infrastructure Advisory Committee, leaders from the concerned sectors of industry, academia, and State and local government will add their comments and advice to that received from the town hall meetings and web site. The President will review and approve the Strategy in the next several months.

Technology will continue to change rapidly. New vulnerabilities and threats will be uncovered. Elements of our present programs may be determined to be ineffective in the future. America's cybersecurity strategy must be dynamic and continually refreshed to adapt to the changing environment.

For the foreseeable future, two things will be true: America will rely upon cyberspace and the Federal government will seek a continuing broad partnership to develop, implement, and refine a *National Strategy to Secure Cyberspace*. We invite you to closely review the proposed strategy and share your input and expertise.

Richard A. Clarke
CHAIR

Howard A. Schmidt
VICE CHAIR

INTRODUCTION

Introduction

Issued earlier this year, the *National Strategy for Homeland Security* addresses a very specific and uniquely challenging threat—terrorism in the United States—and provides a comprehensive framework for organizing the efforts of Federal, State, local and private organizations whose primary functions are often unrelated to national security. Cyberspace is essential to both homeland security and national security; its security and reliability support the economy, critical infrastructures, and national defense. Accordingly, the *National Strategy to Secure Cyberspace* is an implementing strategy, which supports both the *National Strategy for Homeland Security* and the *National Security Strategy of the United States*. The *National Strategy to Secure Cyberspace* describes initiatives to secure U.S. information systems against deliberate, malicious disruption and to foster an increased national resiliency. This Strategy, together with a complementary *Homeland Security Physical Protection Strategy*, provides the strategic foundation for the nation's efforts to protect its infrastructures.

Strategy as Place

This document, together with the accompanying online material from the private sector and academia, is a Strategy of the steps the United States will take to secure the information technology networks and systems that are necessary for the nation's economy, defense, and critical services to operate. Those networks, and the related information technology equipment and software that make them work together, make up our cyberspace.

The Strategy Will Evolve

- as more of the nation devises strategies for securing parts of cyberspace;
- as component strategies become more detailed and refined with experience;
- as technology changes and brings new security challenges and capabilities;
- as more is learned about changing vulnerabilities and threats;
- as consensus forms on ideas proposed for discussion in earlier releases; and,
- as some of the initial ideas mature.

This Strategy is a place where many parts of our nation will describe what they plan to do, and what their strategy is to secure their part of cyberspace. In this Strategy, readers will see plans from and for a diverse group of Americans: teachers, military officers, privacy experts, doctors, stock brokers, police, civil servants, computer scientists, State government officials, corporate CEOs, and Federal officials.

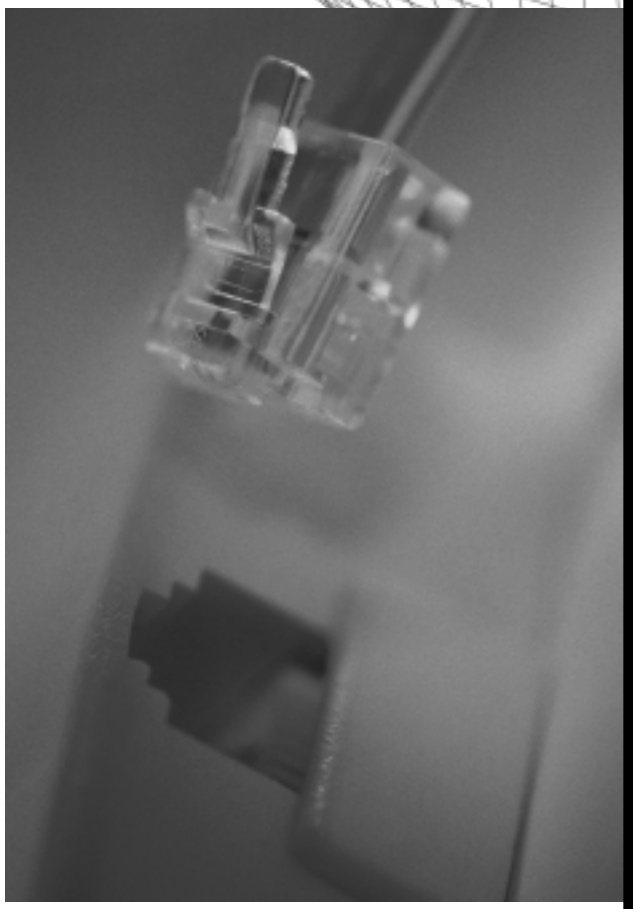
It is also a place where Americans can get advice, whether they are a home user of the Internet, a small business person, the Chief Information Officer of a "small cap" enterprise, a city mayor, a State Governor, a Chief Executive Officer of a Fortune 100 company, or a member of the board of directors of a company of any size.

Strategy as Process

This Strategy is not written in stone. The President's Critical Infrastructure Protection Board (PCIPB) plans to periodically issue, online, new releases of the Strategy as it evolves. The introduction to each release will highlight updates from the previous version.

Component strategies were developed by stakeholders and customers of cyberspace. Representatives of companies that own and operate critical infrastructures came together to draft how banking and finance, electric power, railroads, and other sectors could secure their parts of cyberspace. Community colleges and major universities teamed to plan for securing cyberspace at academic institutions. Big city police and small town sheriffs collaborated on the cyberspace security needs of law enforcement. Congressional committees in both houses held hearings on cybersecurity and related topics. Dozens of national associations met and devoted thousands of hours in developing contributions to this Strategy.

These groups have developed strategies for how they will help secure the portions of cyberspace that they own or operate, because each user of cyberspace must play a role in securing it. That fact does not absolve the Federal government of its responsibilities, which are many and outlined in the Strategy. It does, however, underline the reality that the Federal government alone cannot secure cyberspace. We must all do our part. We will be as successful as the sum of those efforts.



To stimulate debate and discussion, the President's Board solicited the views of experts across the country on what are the key issues and questions that should be addressed by the Strategy. The accumulated questions were then placed on web pages sponsored by a government agency, an association, and a private organization. Many citizens offered their views. This initial release of the Strategy proposes answers for most of the questions and places others in "Agenda Boxes" for continued national dialogue.

As a further part of the national dialogue, the President's Critical Infrastructure Protection Board hosted public town meetings in the spring of 2002, prior to the initial release of the Strategy. These meetings were held in cities around the country.

In addition, the Commerce Department's Critical Infrastructure Assurance Office (CIAO) sponsored meetings with State and local government officials from several States, which included national-level conferences held in Austin, Texas, February 12-13, 2002, and Princeton, New Jersey, April 23-24, 2002.

Following the Internet launch of the initial release, additional town meetings and State forums may be held as part of the effort to maintain national dialogue on securing cyberspace.

Additional meetings around the country are possible and initial planning is underway. Further details will be posted on the web site, **www.secure-cyberspace.gov**, as events are confirmed.

The National Strategy to Secure Cyberspace Supplements other Strategies

The *National Strategy to Secure Cyberspace* supplements the *National Strategy for Homeland Security* and the *National Security Strategy of the United States*. Its "Policy and Principles" section, together with President Bush's Executive Order 13231, provides the Administration's policy guidance on cyberspace security.

Town Hall Meetings Held:

- Denver, Colorado
- Portland, Oregon
- Chicago, Illinois
- Atlanta, Georgia

Future Town Hall Meetings Planned For:

- San Antonio, Texas
- Boston, Massachusetts
- New York City, New York
- San Diego, California
- Philadelphia, Pennsylvania
- Pittsburgh, Pennsylvania
- Phoenix, Arizona

The President's Critical Infrastructure Protection Board

After a review initiated at the outset of the Administration, President Bush signed Executive Order 13231 (*Critical Infrastructure Protection in the Information Age*) in October, 2001 creating the President's Critical Infrastructure Protection Board. The Board is the central focus in the Executive Branch for cyberspace security. It is composed of senior officials from more than 20 departments and agencies. The President created a series of interagency committees that report to the Board on issues such as Education, Research, Incident Response, and Interdependencies.

Some sections of this Strategy are more detailed than others. However, as the Strategy evolves in subsequent editions, it will attempt to address all of the major problems of cybersecurity in appropriate detail. The Strategy is a roadmap for the Administration, the Congress, State and local governments, sectors of the economy, higher education, and the American Internet consumer.

The recommendations are directed at many audiences, including the Administration itself. The Strategy does not substitute for the normal decision-making process about budgets and policies. While there are many recommendations in the Strategy that do not require additional resources, those that do will be considered in the normal processes. Many of the recommendations will become the work of the President's Critical Infrastructure Protection Board and its interagency committees.

Subsequent editions of the Strategy will reflect the decisions made in the FY04 budget process and the work of the Board and its committees, as well as progress by individual departments and agencies.

Strategy for Cyberspace, in Cyberspace

The printed version of this release references places in cyberspace where strategies developed by various groups, as well as other useful material, may be found. Because of size limitations, the hard copy does not contain the text of all references. However, the online version contains hyperlinks to referenced materials. In this paper document, you will find these core components of the Strategy:

- the Case for Action: Cyberspace Threats and Vulnerabilities;
- the Policies and Principles Guiding the Strategy;
- Highlights of the Strategy; and,
- the Five Levels of the National Strategy (the home user, the large enterprise, critical sectors, the nation, and the global community).

Throughout the five levels in the online version, agenda boxes will highlight:

LEVELS

R1	**RECOMMENDATIONS**	*Specific actions that government and nongovernment entities can take to promote cybersecurity.*
P1	**PROGRAMS**	*Existing efforts in cybersecurity.*
D1	**DISCUSSIONS**	*Issues highlighted for continued analysis, debate, and discussion.*

Table: i-1: Sample Agenda box

In the paper document, "Recommendations and Programs and Discussions" will be summarized at the end of each level. Over time, "Discussions" should either result in "Recommendations" or end with no action. Similarly, "Recommendations" should evolve. In some instances they might become initiatives undertaken by individuals or private organizations. In other cases, they may become efforts or programs sustained by government. Because of the changing nature of cyberspace some of the recommendations might be discarded if, on closer examination, they are determined not to be feasible or cost effective as programs. Subsequent releases of the Strategy will update these outcomes.

The Strategy is hyperlinked to documents and web pages owned and operated by nongovernment organizations, trade associations, academic institutions, State and local governments, and corporations. Their content is determined by them alone and their inclusion does not constitute automatic acceptance of their views by the Federal government. They are included because the National Strategy is not intended to be a Federal government prescription, but rather a participatory process.

Please join this process to help secure cyberspace, so that the United States can continue to reap the benefits of the Information Technology Revolution in education, health sciences, the economy, E-Government, and national defense. Only by securing cyberspace can the next level of benefit it offers be tapped to its full potential.

CYBERSPACE THREATS AND VULNERABILITIES: A CASE FOR ACTION

A week after the terrorist attacks on September 11, a less physically destructive but economically significant attack was striking leading financial services firms a few blocks away from the World Trade Center site. Its significance was not in the amount of damage caused, which was considerable, but because it may foreshadow what we could face in the future. The attack was called NIMDA ("ADMIN" spelled backwards), and for a nation that has become dependent on computer networks, it was a wake-up call.

NIMDA was an automated cyber attack, a blend of a computer worm and a computer virus; it propagated across the nation with enormous speed and tried several different ways to infect computer systems it invaded, until it got in and destroyed files. It went from nonexistent to nationwide in an hour, lasted for days, and attacked 86,000 computers. NIMDA caused significant problems in well-protected industries, forcing firms offline, shutting down customer access, and requiring some firms to rebuild systems entirely. The actual financial cost of the NIMDA attack is unknown because there is no consistent method to track such damage. However, industry sources estimate that the overall financial impact of cyber attacks resulting from malicious code could have been $13 billion in the year 2001.

Case for Action—Key Themes

- Cyber incidents are increasing in number, sophistication, severity, and cost.
- The nation's economy is increasingly dependent on cyberspace; this has introduced unknown interdependencies and single points of failure.
- A digital disaster strikes some enterprise every day. Infrastructure disruptions have cascading impacts, multiplying their cyber and physical effects.
- Fixing vulnerabilities before threats emerge will reduce risk.
- It is a mistake to think that past levels of cyber damage are accurate indicators of the future. Much worse can happen.
- The common defense of cyberspace depends on a public-private partnership.
- Everyone must act to secure their parts of cyberspace.

Two months before NIMDA, a cyber attack called Code Red had infected 150,000 computer systems in 14 hours, causing billions of dollars in losses. Such attacks demonstrate the growing sophistication and destructiveness of cyber attacks. The volume of attacks is also up: Carnegie Mellon University's Computer Emergency Response Team's [CERT] Coordination Center reported 3,700 attacks in 1998, and at current rates will report over 110,000 in 2002. Other teams report similar, dramatic growth in cyber attacks. That trend is likely to continue.

A Nation Now Fully Dependent on Cyberspace

For the United States, the Information Technology Revolution quietly changed the way business and government operate. Without a great deal of thought about security, the nation shifted the control of essential processes in manufacturing, utilities, banking, and communications to networked computers. As a result, the cost of doing business dropped and productivity skyrocketed. The trend towards greater use of networked systems continues.

By 2002, our economy and national security are fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of cyberspace. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets.

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 into millions of other computer networks, which, make most of the nation's essential services work. While the Internet has grown enormously and globally, it has also grown increasingly insecure. People in almost every country on the globe can access a network that, in turn, is ultimately connected to networks that run critical functions in the United States.

Cyber attacks on U.S. information networks occur regularly and 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 identify and deter those with the capabilities and intent to harm national infrastructures.

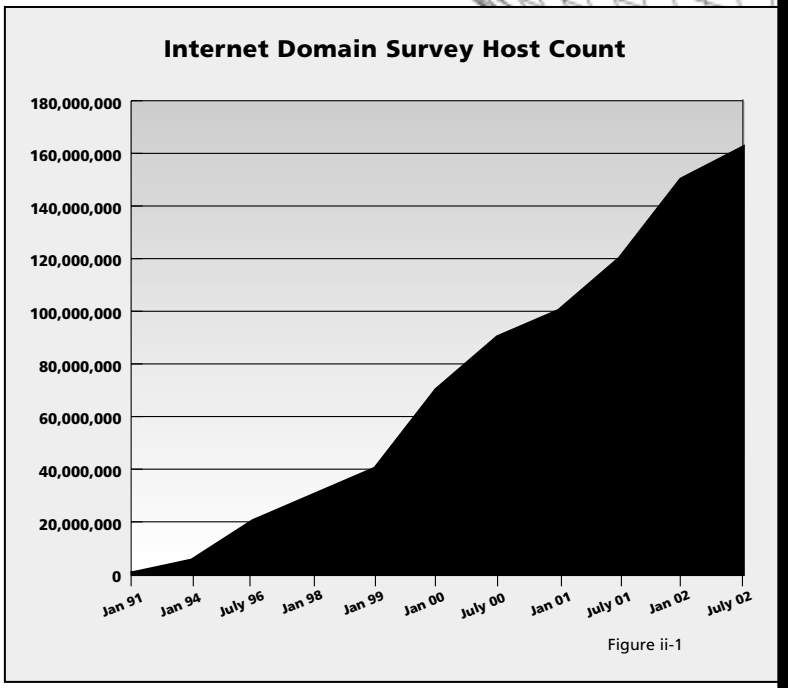


Figure ii-1

A Range of Threats

A spectrum of actors conduct attacks against the information infrastructure. They range from "script kiddies" who download malicious software from the Internet to carry out the equivalent of annoying graffiti attacks in cyberspace; to hackers who merely want to demonstrate their destructive skills; to trusted "insiders" who exploit their access to computer systems to cause damage; to criminal organizations that engage in fraud, extortion, and theft in cyberspace; and to terrorists and potential enemy nation states spying on us now, and developing plans that would enable them, in a future conflict, to damage our economy and weaken or control the physical and cyber systems the United States needs to fight back.

Identifying those who did or might attack provides an opportunity to not only stop them and bring them to justice (whether, for example, through arrests in the case of criminals, or military means in the case of acts of information warfare), but also to learn their skill sets and better focus national protection efforts.

Consider the Following Scenario...

A terrorist organization announces one morning that they will shut down the Pacific Northwest electrical grid for six hours starting at 4:00PM; they then do so. The same group then announces that they will disable the primary telecommunication trunk circuits between the U.S. East and West Coasts for a half day; they then do so, despite our efforts to defend against them. Then, they threaten to bring down the air traffic control system supporting New York City, grounding all traffic and diverting inbound traffic; they then do so. Other threats follow, and are successfully executed, demonstrating the adversary's capability to attack our critical infrastructure. Finally, they threaten to cripple e-commerce and credit card service for a week by using several hundred thousand stolen identities in millions of fraudulent transactions, if their list of demands are not met. Imagine the ensuing public panic and chaos.

What makes this scenario both interesting and alarming is that all of the aforementioned [types of] events have already happened, albeit not concurrently nor all by malicious intent. They occurred as isolated events, spread out over time; some during various technical failures, some during simple exercises, and some during real-world cyber attacks. All of them, however, could be effected through remote cyber attack...

An excerpt from a letter to the President from 50 scientists, computer experts and former intelligence officials.

Reduce Vulnerabilities, in the Absence of Known Threats

While the nation must deal with specific threats, waiting to fix any important vulnerability in the critical infrastructure until learning of an impending attack by an identified attacker is an unacceptably risky strategy for potential victims. Both the Code Red and NIMDA cyber attacks of 2001 burst onto the nation's networks with little or no warning and spread so fast that many victims did not have a chance to hear the alarms. Even if they had, many victims did not have time, knowledge, or tools to protect themselves. Creating defenses against these attacks would have taken days in some cases.

A key lesson from these cyber attacks and others like them is that those who rely on networked computer systems need to identify and remedy their vulnerabilities now, rather than wait for an attacker to be stopped or until alerted of an impending attack. No one has yet been arrested for launching the Code Red or NIMDA attacks. However, it is important to note that computer attacks are serious felonies and perpetrators are being caught with increasing regularity.

Identifying vulnerabilities by having a group of trained professionals complete an information technology security audit can take 2-3 months. Remedying the most serious vulnerabilities by creating a multi-layered defense and a resilient network may take several additional months. Then the process must be regularly repeated.

New Vulnerabilities Requiring Continuous Response

The process of securing networks and systems must be continuous because new vulnerabilities are created or discovered regularly. CERT/CC notes that not only are cyber incidents and the number of attacks increasing at an alarming rate, so too are the number of vulnerabilities that an attacker can utilize. Identified computer security vulnerabilities—problems with software and hardware that permit unauthorized entry or damage to a network—more than doubled in the last year, with 1,090 separate vulnerabilities reported in 2000, and 2,437 reported in 2001.

Installing a network security device is not a substitute for a constant focus on keeping defenses up to date. In a recent survey by the Computer Security Institute, 90 percent of respondents used anti-virus software, but 85 percent had been damaged by a virus. In the same survey, 89 percent had installed computer firewalls and 60 percent had intrusion detection systems, yet 90 percent reported security breaches had taken place and 40 percent had their systems penetrated from outside their network. The majority of security vulnerabilities can be mitigated with good security practices. As these survey numbers indicate, good security practices include not just installing those devices, but operating them correctly and keeping them current, including regular patching and virus updates.

A Mapping of Code Red Penetration on a Portion of the Internet

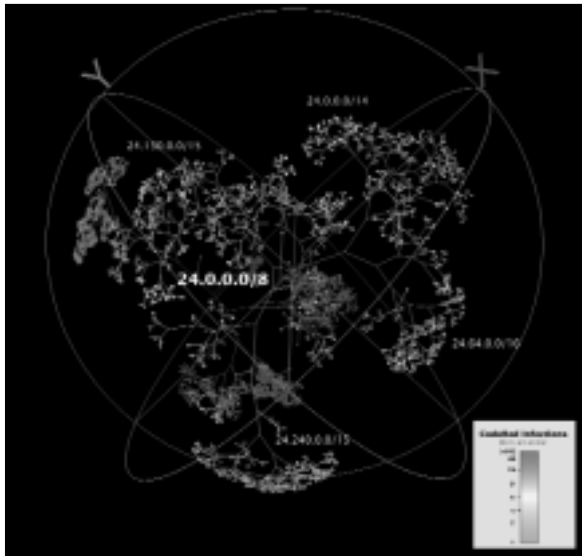


Image courtesy UCSD/CAIDA (www.caida.org) © 2002 The Regents of the University of California. Figure ii-2

Cybersecurity and Opportunity Cost

For individual companies and for the national economy as a whole, improving computer security often requires investing attention, time, and money. President Bush requested that Congress increase funds to secure Federal computers by 64 percent in FY03.

President Bush's investment in securing Federal computer networks will eventually reduce expenditures through cost saving E-Government solutions, modern enterprise management, and by reducing opportunities for waste and fraud.

For the national economy and, in particular, for the information technology industry, the dearth of trusted, reliable, secure information systems is a barrier to future growth. Much of the promise and potential of continued growth in the economy, as a result of the Information Technology Revolution, has yet to be realized. That unrealized opportunity, including e-commerce and business-to-business (B2B) activity, is in part deterred by computer security risks. Vulnerability in cyberspace places

more than transactions at risk; it can jeopardize intellectual property, business operations, infrastructure services and consumer trust.

Investment in cybersecurity is not just more costly overhead. There is a return on security investment. Surveys have repeatedly shown that:

- the costs associated with a severe computer attack are likely to be greater than the preemptive investment in a cybersecurity program would have been; and,
- designing strong security into the information systems architecture of an enterprise can reduce overall operational costs by enabling cost-saving processes such as remote access and customer or supply chain interactions that could not occur in networks lacking appropriate security.

These results suggest that with greater awareness of the issues, companies may find benefit in increasing their level of cybersecurity. Greater awareness and voluntary efforts are critical components of this Strategy.

Individual and National Risk Management

Prior to the events of September 11, damage from overseas terrorist networks in the United States had been very limited. In one day that changed. One estimate places the increase in cost to our economy from attacks to U.S. information systems at 400 percent over four years. While those losses remain relatively limited, that too could change abruptly.

Every day in America an individual company, or a home computer user, suffers damage and losses from cyber attacks that, on an individual level, are significant, perhaps even catastrophic. The ingredients exist for that kind of damage to also occur on a national level, to the networks and systems upon which the nation depends:

- potential adversaries have the intent;
- the tools of destruction are broadly available; and,
- the vulnerabilities of the nation's systems are many and well known.

These factors mean that no strategy can completely eliminate risk, but the nation can and must act to manage risk responsibly and to minimize the potential damage that could be done by exploiting vulnerabilities. By noting this in a public document, we are not telling potential foes something that they and others do not already know. In 1997, a Presidential Commission identified the risks in a seminal public report. In 2000, the first national plan to address the problem was published. In 2001, President Bush, citing these risks, issued an Executive order making cybersecurity a priority issue and increased funding to secure Federal networks. In 2002, the President moved to consolidate and strengthen Federal cybersecurity agencies.

Government Alone Cannot Secure Cyberspace

Yet despite this awareness and these measures, the risk continues to our national information networks and the critical systems they manage. Reducing that risk requires an active, unprecedented, partnership among diverse components of our country and our global partners.

The Federal government should not and, indeed, could not, secure the computer networks of privately owned banks, energy companies, transportation firms, or other parts of the private sector. The Federal government should not intrude into homes and small businesses, into universities, or local agencies and departments to create secure computer networks.

Each American who depends on cyberspace, the network of information networks, must secure that part that they own or for which they are responsible.

The Federal government can help to empower Americans to do just that, by:

- raising awareness;
- sharing information about vulnerabilities and solutions;
- fostering partnerships with and among private sector groups, and others;
- stimulating improvements in technology;
- increasing the number of skilled personnel;
- investigating and prosecuting cybercrime;
- protecting Federal computers; and,
- promoting increased security for the networks upon which the economy and national security depend.

Ultimately, cyberspace security is not about "good ones and zeroes attacking bad ones and zeroes in the ether." It is about whether when one throws the switch the electricity comes on, or whether the money Americans have invested and deposited is there, and whether this country is secure. U.S. physical infrastructure has been protected since it emerged in the 19th century. For example, railroad police were created to mitigate threats to the vast transportation networks.Those problems of physical security remain, but are now matched by the problems of cybersecurity. The two problem sets are related. A cybersecurity problem can render physical structures insecure and vice versa. Government and industry must analyze those interactions and interdependencies, but must also place a special focus on the unique and new vulnerabilities posed by reliance on cyberspace.

Vulnerabilities Reported: 1995-2001

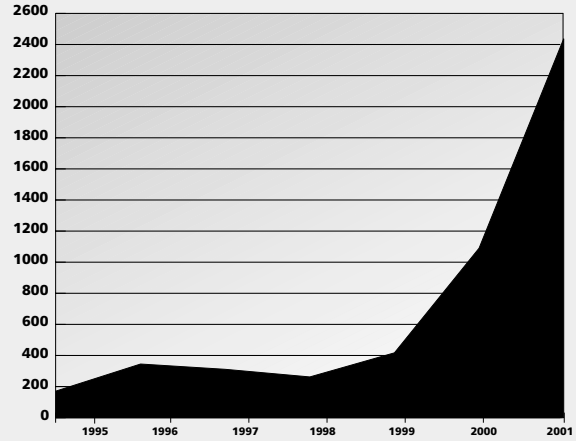


Figure ii-3: Source CERT CC ©

Incidents Handled: 1988 - 2001

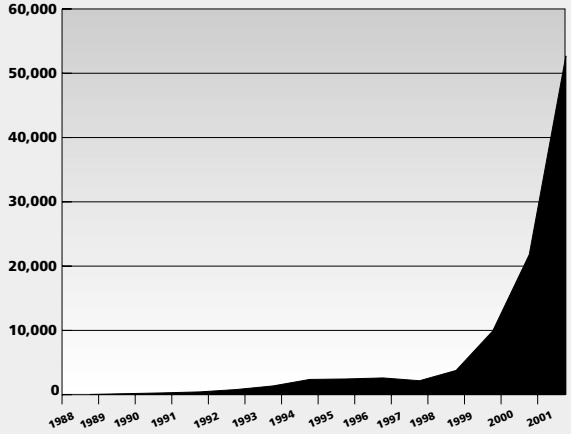


Figure ii-4
Source: Internet Software Consortium (www.isc.org)

NATIONAL POLICIES AND GUIDING PRINCIPLES

The National Strategy to Secure Cyberspace supplements the *National Strategy for Homeland Security* and the *National Security Strategy of the United States*. This "Policy and Principles" section, together with President Bush's Executive Order 13231, provides the Administration's policy guidance on cyberspace security. The policy statements and recommendations in this Strategy are subject to Executive Order 13231 and other relevant Executive orders relating to national security, and nothing herein alters the authorities, roles or responsibilities of U.S. government officials under the National Security Act or other relevant statutes.

This document is the first ever *National Strategy to Secure Cyberspace*. The purpose of the Strategy is to engage, empower, and establish efforts to secure cyberspace. Engaging and empowering America to secure cyberspace is an exceedingly complex mission that requires coordinated and focused effort across society—the Federal government, State and local governments, the private sector, and the American people. The Strategy seeks to implement the President's national policy objectives and principles for securing cyberspace.

Statement of National Policy

The Information Technology Revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures—cyberspace.

Continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems are needed to minimize disruption and maximize reliability.

The United States will achieve and maintain the ability to protect our nation's critical infrastructures from natural events and intentional acts that would significantly diminish the abilities of:

- the Federal government to perform key homeland security and national security missions, and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver essential public services; and,
- the private sector to ensure the orderly functioning of the economy and the delivery of essential infrastructure services.

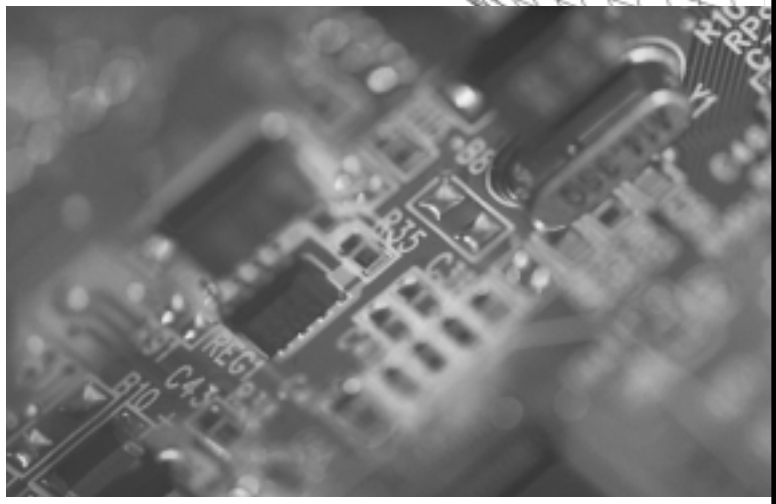
This policy acknowledges that no security measures will be 100 percent reliable. Nonetheless, it strives to ensure that any interruptions or manipulations of these critical functions will be infrequent, brief, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Many of the nation's critical infrastructures have historically been physically and logically separate systems with little interdependence. Advances in information technology and the necessity of improved efficiency, however, have precipitated a steadily and rapidly increasing amount of automation in, and interconnection among, these systems.

The USA PATRIOT Act defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." America's critical infrastructures include energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, government, defense industrial base, food, agriculture, and postal and shipping.

This Strategy also recognizes that maintaining the integrity of the national economic and social fabric over the long term requires attention, not only to the security of information systems, but also to the related societal structures on which those systems depend. Accordingly, the Strategy incorporates affirmative measures designed to enhance and augment these supporting structures.

Though the United States possesses both the world's strongest military and largest national economy, these two aspects of the nation's power increasingly rely upon certain critical infrastructures, which include cyber-based information systems. As witnessed on September 11,



enemies of the United States—nations, groups, and, indeed, even individuals—are prepared to strike in unconventional ways. These adversaries have explicitly stated the intention, not only to strike at U.S. citizens, but to attack the nation's infrastructures and cyberspace—the pillars of the economy.

Guiding Policy Principles

In January 2001, the Administration began a review of the role of information systems and cybersecurity. In October 2001, President Bush issued Executive Order 13231, which authorized a protection program consisting of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. 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:

Embrace Private-Public Partnerships

The protection of critical infrastructures is necessarily a shared responsibility since approximately 85 percent of the nation's critical infrastructure facilities are owned and operated by the private sector, and many critical government operations depend on these private facilities.

Because the targets of attacks on the nation's critical infrastructure would likely include both facilities in the economy and those in the government, addressing potential vulnerabilities will require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security interests. The private sector has been intensively engaged in a closely coordinated effort with the Federal government to address these issues. One important step taken by many sectors has been the development of information sharing and analysis centers (ISACs) to facilitate communication and the dissemination of security-related information. In addition, various sectors have developed plans to secure their parts of cyberspace, which complement this National Strategy. It is the government's hope and intention that this productive and collaborative partnership will continue.

The nation must focus on mechanisms for prevention and crisis management, such as the identification and remediation of vulnerabilities, education, research and development, alert and warning methodologies, and the development of measures to support these efforts. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control, and to provide the government with the information necessary to assist them in that task. For its part, the Federal government, in working to safeguard its own information systems, should strive to serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the greatest extent possible, act with reciprocity to distribute the results of its endeavors to the private sector.

Avoid Regulation

In order to engage the private sector fully, the Federal government recognized that participation by owners and operators in the private-public partnership would have to be voluntary. To encourage maximum participation by the private sector in this partnership, the U.S. Government, to the extent feasible, has sought to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector. Accordingly, the government has relied on the incentives that the market provides as the first choice for addressing the problem of critical infrastructure protection, and would turn to regulation only in the face of a material failure of the market to protect the health, safety, or well-being of the American people.

Safeguard Civil Liberties and Privacy

The interests of security and personal privacy need not be antithetical to one another. Indeed, to a large degree, by securing the integrity of communications over the Internet, the measures advocated in this Strategy seek to protect individual privacy and, thus, complement those interests. Nevertheless, in crafting measures to increase the nation's security, one must exercise caution to avoid undermining those fundamental values and characteristics of free society that the nation is seeking to protect in the first place. Accordingly, care must be taken to respect privacy interests and other civil liberties. Consumers and operators must have confidence that information will be handled accurately, confidentially, and reliably.

Coordinate with Congress

To ensure that the approaches adopted to secure America's cyberspace systems enjoy broad support and consensus, the Executive branch will work with Congress on approaches and programs to meet the goals of our national policy. As appropriate, the Executive branch may ask Congress to enact legislation to advance this Strategy.

Cooperate with State and Local Governments

American democracy is rooted in the precepts of federalism—a system of government in which State governments share power with Federal institutions. This structure of overlapping Federal, State, and local governance has more than 87,000 different jurisdictions and provides unique opportunity and challenges for cyberspace security efforts. State and local governments, like the Federal government, operate large, interconnected information systems upon which critical government services depend. The opportunity comes from the expertise and commitment of local agencies and organizations involved in cybersecurity. The challenge is to develop interconnected and complementary systems that are reinforcing rather than duplicative and that ensure essential requirements are met. Accordingly, all critical infrastructure and cyberspace protection plans and actions shall take into consideration the needs, activities, and responsibilities of State and local governments and first responders.

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
Treasury	• Banking and Finance
Health and Human Services	• Public Health (including prevention, surveillance, laboratory services, and personal health services) • Food (all except for meat and poultry)
Energy	• Energy (electric power, oil and gas production, and storage)
Environmental Protection Agency	• Water • Chemical Industry and Hazardous Materials
Agriculture	• Agriculture • Food (meat, and poultry)
Defense	• Defense Industrial Base

Designation of Coordinating Agencies

To facilitate and enhance coordination and communication between the Federal government and the private sector upon which effective partnership depends, the government has designated a "Lead Agency" for each of the major sectors of the economy vulnerable to infrastructure attack. The designated lead agencies, and their sector counterparts, are listed in the table on the previous page. 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) is responsible for the development and oversight of the implementation of governmentwide policies, principles, standards, and guidelines for Federal government computer security programs. The State Department is responsible for coordinating international outreach on cybersecurity. The Director of Central Intelligence is responsible for assessing the foreign threat to the United States networks and information systems. The Department of Justice and the Federal Bureau of Investigation (FBI) lead the national efforts in investigating and prosecuting cybercrime.

Working together, the sector representatives and the lead agencies assess the vulnerabilities of their sectors to cyber or physical attacks and recommend plans or measures to eliminate significant vulnerabilities. Because technology and the nature of the threats to the nation's critical infrastructures continue to change rapidly, the sectors and lead agencies should frequently assess the reliability, vulnerability, and threat environments of the nation's infrastructures and employ protective measures and responses that are robustly adaptive. Finally, in keeping with the partner relationship, the full authority, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness must be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

Guiding Strategic Principles

The *National Strategy to Secure Cyberspace* is the sum of the efforts of individuals, groups, and institutions from around the country. The end point of these efforts is to create a secure, trusted, robust, reliable, and available infrastructure to support America's economy, national security, and critical services for the foreseeable future.

Cyberspace is a complex network that connects diverse infrastructures, enterprises, and nations. These connections occur over multiple paths owned by many different operators. Securing this network does not mean ensuring that no one element or connecting path is ever lost. Instead, it means ensuring that the network is resilient in the face of disruption or losses, that paths may be replaced by others, and that network elements are redundant and difficult to permanently disable. The security of individual elements within cyberspace, and their continued evolution with changing conditions, creates this resiliency.

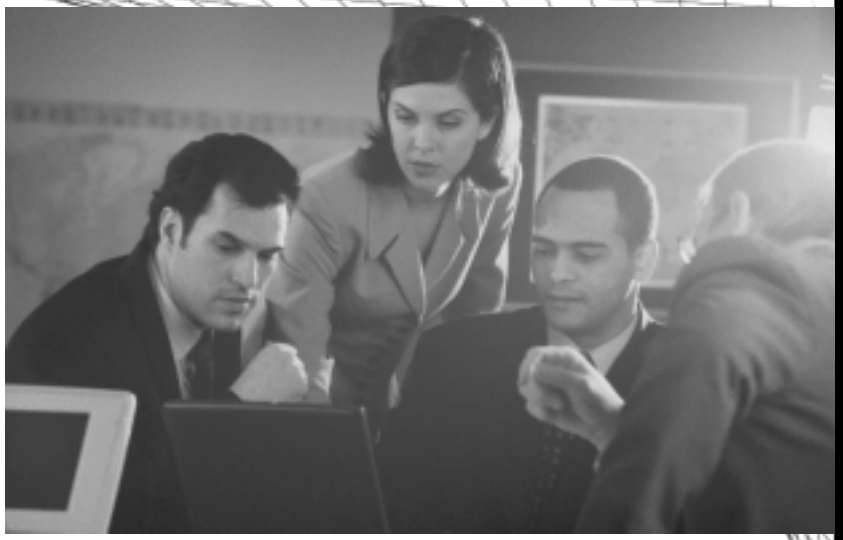
Thus, to create a secure and resilient cyberspace, the nation must acknowledge and act accordingly on to two strategic security principles: (1) that the security of the entire infrastructure will depend on the security of each component, and (2) that threats and vulnerabilities will evolve, and that security must evolve at an equal or higher rate.

Secure the parts of cyberspace to achieve security of the whole

The security of cyberspace rests on the security of all of its components. In cyberspace, attackers can be anywhere at the speed of light. No geographic safety exists. Networks may prove vulnerable to attacks both from outside and inside the network. Components within an otherwise secure network may still be compromised by insiders, downloaded software, or its compromised neighbors. Placing a wall around the perimeter of a network is not adequate to achieve security.

Once one computer or element in the network is compromised, it can be used to compromise others. Similarly, unsecured sectors of the economy or government can and are being used as platforms to attack other sectors. Disruptions in one sector also have cascading effects that can disrupt multiple other parts of the infrastructure. To combat these vulnerabilities, the security of the infrastructure must not be dependent on a single layer, group or focal point, but rather must be found in multiple layers, distributed defenses, and the ability to recover quickly from any attack.

To improve cybersecurity, the nation must secure cyberspace at each level of activity. Accordingly, each individual and sector must be aware of its roles and responsibilities in securing its part in cyberspace. Each sector and each individual depends on the others to make cyberspace secure. Therefore, the nation must secure cyberspace through awareness and information; identified roles and partnerships at all levels, and through Federal leadership in securing Federal cyber systems. Such leadership also includes preventing and deterring cybercrime, electronic espionage, and information warfare.



Rapidly evolve security measures to stay ahead of changing technology and vulnerabilities

New vulnerabilities in systems accrue at an alarming rate. Vulnerabilities are created as new software is developed and new technologies emerge. They are identified over time and through use. At the same time, new and ever more advanced tools are developed to exploit them. Security policies, practices, and technology must adapt. The nation must develop a security infrastructure that can evolve one step ahead of would be attackers.

Only now are experts beginning to imagine what impact nanotechnology and quantum computing will have on the current cyberspace. These innovations and others will introduce unforeseen changes in the way networks operate and the way they can be made secure. The nation must invest in education and training, technology, and coordination of activity if it is to understand these changes and remain the world leader in the development and application of new technologies for cyberspace security.

HIGHLIGHTS

This section summarizes and provides a framework for the rest of the document. It highlights in one place the most important recommendations that will be discussed in later sections.

Strategy

The security of cyberspace depends vitally on all owners of the nation's cyber infrastructure, from the home user to the Federal government. Each individual and organization has a responsibility to secure its own portion of cyberspace. The Strategy is designed to empower each person and each organization to do its part. It provides a roadmap for how to achieve cybersecurity and provides tools to better empower all Americans to do so.

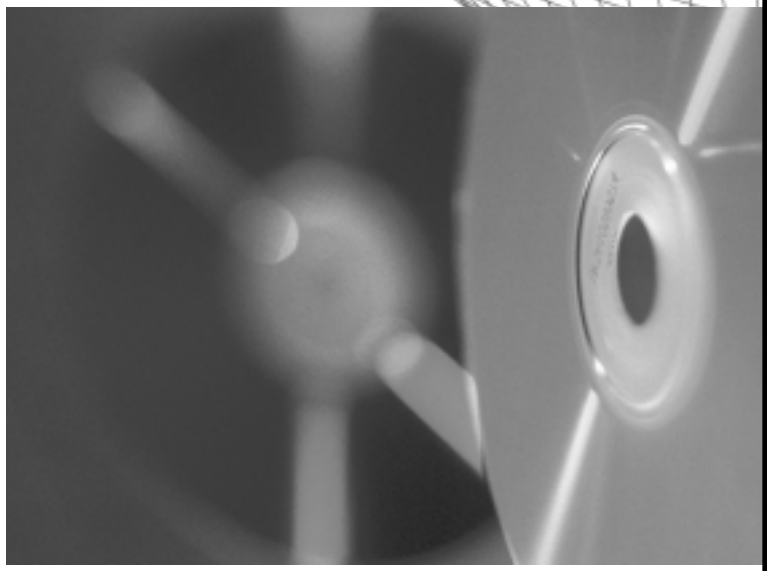
To create this strategic roadmap, the owners of each major component of cyberspace have been developing their own plans for securing their portions of the infrastructure. Some of these plans are already developed and are contained in this document. Others will be added over time. Together they will reflect a national partnership between private sectors, government, and individuals to vigorously create, maintain, and update the security of cyberspace.

The overall national strategic goal is to empower all Americans to secure their portions of cyberspace. This strategic goal will be accomplished through six major tools for empowering people and organizations to do their part:

1. **Awareness and Information:** Educate and create awareness among users and owners of cyberspace of the risks and vulnerabilities of their system and the means to mitigate these risks.
2. **Technology and Tools:** Produce new and more secure technologies, implement those technologies more quickly, and produce current technologies in a more secure way.
3. **Training and Education:** Develop a large and well-qualified cybersecurity workforce to meet the needs of industry and government, and to innovate and advance the nation's security capabilities.
4. **Roles and Partnerships:** Foster responsibility of individuals, enterprises, and sectors for security at all levels through the use of market forces, education and volunteer efforts, public-private partnerships, and, in the last resort, through regulation or legislation.
5. **Federal Leadership:** Improve Federal cybersecurity to make it a model for other sectors by increasing accountability; implementing best practices; expanding the use of automated tools to continuously test, monitor, and update security practices; procuring secure and certified products and services; implementing leading-edge training and workforce development; and deterring and preventing cyber attacks.
6. **Coordination and Crisis Management:** Develop early warning and efficient sharing of information both within and between public and private sectors so that attacks are detected quickly and responded to efficiently.

In each section of this Strategy, the reader will find some or all of these themes reflected in two ways. First, the introduction to each section lays out the strategic goals for that audience or level of the Strategy. Second, each section highlights ongoing programs, recommendations, and topics for discussion that will serve to develop the strategic goals.

In this section, these strategies and supporting actions are summarized. In this National Strategy, the reader will find new recommendations for actions, and numerous questions and topics for debate. It will be the goal of the Federal government to help facilitate the evolution of these discussions so that they become recommendations. Recommendations will evolve, in turn, and some will become initiatives of individuals, organizations, or government.



Summary of Recommendations by Section

The National Strategy calls for actions at all levels and across all sectors. Some of the major strategic innovations called for in this document are highlighted below. A detailed discussion of each of these innovations is included in the pages that follow.

Awareness and Information

The Strategy identifies the need for increased awareness about the vulnerability of America's cyber infrastructure and provides information that each person, company, organization, and agency can use to help make cyberspace more secure. It recommends:

- Home users and small businesses should recognize that they have an important role to play in securing cyberspace, including securing their own computer systems, accessing the Internet in a secure manner and drawing on best practices that can be found at a number of web sites including: **www.StaySafeOnline.info**, **www.nipc.gov**, and **www.crsc.nist.gov**.
- The President's Critical Infrastructure Protection Board's Awareness Committee should foster a public-private partnership to develop and disseminate cybersecurity awareness materials, specifically, audience-specific tools and resources for annual awareness training.
- State and local governments and private entities should identify or develop guidelines covering cyber awareness, literacy, training, and education, including ethical conduct in cyberspace, tailored to each level of a student's education.

Technology and Tools

The Strategy identifies the need for increased cybersecurity-related research. It recommends:

- A public-private partnership should, as a high priority, develop best practices and new technology to increase security of digital control system (DCS) and supervisory control and data acquisition (SCADA) systems in utilities, manufacturing, and other networks. In the interim, owners and operators of pipelines and power grids that rely on DCS/SCADA systems should closely examine the risks of Internet connections and take appropriate actions, such as implementing secure authentication within 24 months. Other industries with heavy reliance on DCS/SCADA should consider doing the same. The Department of Energy's recent guidelines provide information on securing SCADA systems.
- The President's Critical Infrastructure Protection Board should coordinate with the Director of the Office of Science and Technology Policy on a program of Federal government research and development including near-term (1-3 years), mid-term (3-5 years), and long-term (5 years out and longer) IT security research. Federally funded near-term IT security research and development for FY04 and beyond should include priority programs identified by OSTP and the R&D Committee. Existing priorities include, among others, intrusion detection, internet infrastructure security (including protocols e.g. BGP, DNS), application security, denial of service, communications security (including SCADA system encryption and authentication), high assurance systems and secure system composition.
- Public-private partnerships should identify cross-sectoral cyber and physical interdependencies. They should develop plans to reduce related vulnerabilities, in conjunction with programs proposed in *National Strategy for Homeland Security*. It is within the scope of the National Infrastructure Simulation and Analysis Center to assist with these efforts.

Training and Education

The Strategy addresses the existing gap between the need for qualified IT professionals and America's ability to train and develop these workers. Specific recommendations include:

- States should consider creating Cyber Corps scholarship-for-service programs at State universities, to fund the education of undergraduate and graduate students specializing in IT security who are willing to repay their grants by working for the states. The existing Federal Cyber Corps scholarship-for-service program should be assessed for possible expansion to additional universities, with both faculty development and scholarship funding. The program could also add a faculty and program development effort with community colleges.
- The CIO council and relevant Federal agencies should consider establishing a "Cyberspace Academy," linking Federal cybersecurity and computer forensics training programs.
- IT security professionals, associations, and other appropriate organizations should explore approaches to and the feasibility of a nationally recognized certification program, including a continuing education and retesting program. The Federal government could assist in the establishment of such a program, and, if it is created, consider requiring that Federal IT security personnel be appropriately certified.

Roles and Partnerships

The Strategy recognizes that all Americans have a role to play in cybersecurity, and identifies the market mechanisms for stimulating sustained actions to secure cyberspace. It recommends:

- CEOs should consider forming enterprisewide corporate security councils to integrate cybersecurity, privacy, physical security, and operational considerations.

- State and local governments should consider establishing IT security programs for their departments and agencies, including awareness, audits, and standards. State, county, and municipal associations could provide assistance, materials, and model programs.
- Internet service providers, beginning with major ISPs, should consider adopting a "code of good conduct" governing their cybersecurity practices, including their security-related cooperation with one another.
- The Federal government should identify and remove barriers to public-private information sharing and promote the timely two-way exchange of data to promote increased cyberspace security.
- Colleges and universities should consider establishing together: (a) one or more information sharing and analysis centers (ISACs) to deal with cyber attacks and vulnerabilities; (b) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (c) one or more sets of best practices for IT security; and (d) model user awareness programs and materials.

Federal Leadership

The Strategy recognizes the pressing need to make Federal cyberspace security a model for the nation. It recommends:

- In order to enhance the procurement of more secure IT products, the Federal government, by 4Q FY03, will complete a comprehensive program performance review of the National Information Assurance Program (NIAP) to determine the extent to which NIAP is cost effective and targets a clearly identified security gap; whether it has defined goals to close the gap, whether it is achieving those goals, and the extent to which program improvements, streamlining, or expansion are appropriate and cost effective.
- Federal departments should continue to expand the use of automated, enterprisewide security assessment and security policy enforcement tools, and actively deploy threat management tools to preempt attacks. By 3Q FY03, the Federal government will determine whether specific actions are necessary (e.g., through the policy or budget processes) to promote the greater use of these tools.
- By the end of 2Q FY03, consider the cost effectiveness of a scenario-based security and contingency preparedness exercise for a selected cross-government business process. Should such an exercise take place, any security weaknesses shall be included as part of agencies' Government Information Security Reform Act (GISRA) corrective action plans.
- Federal departments and agencies must be especially mindful of security risks when using wireless technologies. Federal agencies should consider installing systems that continuously check for unauthorized wireless connections to their networks. Agencies should carefully review the recent NIST report on the use of wireless technologies and take into account NIST recommendations and findings. In that regard, agency policy and procedures should reflect careful consideration of additional risk reduction measures including the use of strong encryption, bi-directional authentication, shielding standards and other technical security considerations, configuration management, intrusion detection, incident handling, and computer security education and awareness programs.
- As part of the annual departmental IT security audits, agencies should include a review of IT-related privacy regulation compliance.

Coordination and Crisis Management

The Strategy identifies a pressing need for a comprehensive national analysis and warning capability. It recommends:

- ISPs, hardware and software vendors, IT security-related companies, computer emergency response teams, and the ISACs, together, should consider establishing a Cyberspace Network Operations Center (Cyberspace NOC), physical or virtual, to share information and ensure coordination to support the health and reliability of Internet operations in the United States. Although it would not be a government entity and would be managed by the private sector, the Federal government should explore ways in which it could cooperate with the Cyberspace NOC.
- Industry should, in voluntary partnership with the Federal government, complete and regularly update cybersecurity crisis contingency plans, including a recovery plan for Internet functions.
- The law enforcement and national security community should develop a system to detect a national cyber attack (cyber war) and a plan for immediate response. As part of this process, the appropriate entities should establish requirements and options.
- Owners and operators of information system networks and network data centers should consider developing remediation and contingency plans to reduce the consequences of large-scale physical damage to facilities supporting such networks. Where requested, the Federal government could help coordinate such efforts and provide technical assistance.
- The United States should work with individual nations and with nongovernmental organizations (e.g., Forum of Incident Response and Security Teams (FIRST)), and international organizations (e.g., International Telecommunications Union (ITU)), to promote the establishment of national and international watch and warning networks that will be designed to detect and prevent cyber attacks as they emerge. In addition, such networks could help support efforts to investigate and respond to attacks.

Six tools for empowerment discussed for each level of audience

The Strategy provides a roadmap to help Americans understand their part in securing cyberspace. To make this roadmap easier to use, it is divided into audience levels: **Level 1** for home users and small businesses, **Level 2** for large enterprises, **Level 3** for sectors including government, private industry, and higher education, **Level 4** for national issues and efforts, and **Level 5** for discussion of global issues. Each of these levels and their sub-levels will have its own strategic goal. These goals will be supported by strategic actions that the nation will take to achieve the goals.

The six tools for empowerment (see page 11) will help drive corresponding strategic actions at each level. Some or all of the six tools may be employed at each level. For example, "Awareness and Information" will help empower the home user as well as private sector employees and Federal workers to secure their portion of cyberspace. Roles and partnerships will be identified and described at all levels. Not every tool will be appropriate for every level, but, taken together, these tools will underpin all of the nation's efforts to secure cyberspace.

LEVEL 1:
THE HOME USER AND SMALL BUSINESS

The strategic goal is to empower the home user and small business person to protect their cyberspace and prevent it from being used to attack others. This goal can be achieved through the following:

- raising cybersecurity awareness of the home user and small business, including children and students;
- making it easier for home users and small businesses to keep current with anti-virus software, software patches, and firewalls, perhaps through activity by the Internet service providers;
- encouraging and helping facilitate the installation and use of firewalls on all broadband Internet connections, such as cable modems, DSL, satellite and wireless; and,
- bringing cybersecurity resources closer to the users through local organizations and educational courses.

Issues and Challenges

Too Small to Matter?

Many Americans think that those who would seek to damage us in cyberspace would certainly direct their attacks at major government departments and large corporations. They think cybersecurity is someone else's problem, not the concern of the home Internet user or the small business owner.

Unfortunately, such beliefs are inaccurate. Even the home user and small business can be damaged severely and, in some cases, can be used to severely damage others. See table to the right for some examples of what can, and does, happen.

Will It Happen to Me?

Unfortunately, Americans live in an environment in which cyber attacks of the types described in this Strategy are common. As more and more tools become available to automate these attacks, reaching each and every user becomes easier to do. For example, the "Honeynet Project" uses "dummy" systems attached to the Internet to measure actual computer attacks. According to the project's most recent results, a random computer on the Internet is scanned, meaning it is checked for its presence, setup or weaknesses, dozens of times a day. A common home user setup the project created was hacked five times in four days. Home users or businesses with larger systems are also a target. Systems are subjected to certain scans across the Internet an average of 17 times a day. In some cases, insecure servers have been hacked 15 minutes after plugging into the Internet.

Secure Internet Use

Using the Internet in a secure manner does not just happen. Rather it is the purposeful result of both awareness and the availability of services and tools which facilitate secure Internet use. It is often difficult for home users and small businesses to access secure Internet services. For example, many home users and small businesses do not use firewalls to protect their computers from unauthorized intrusions.

"Always-on-connections" to the Internet, such as broadband, digital service line (DSL), wireless and satellite services, are increasing in popularity. Such connections offer tremendous speed and efficiency. However, they also present unique challenges, because many users are not aware of the security implications of an "always-on-connection." For example, these connections generally mean that larger amounts of data can be sent at any time and the data can be sent continuously. These two factors can be exploited and used to attack other systems, possibly even resulting in nationally significant damage.

Facilitating and promoting more secure use of the Internet by home users and small business can be greatly advanced by the entire product chain that prepares the consumer for the Internet. The Internet service providers, hardware manufacturers, software vendors, retailers, and providers of security services can all facilitate this effort by making products and services available and easy to use.

CYBER ATTACKS ON THE HOME USER AND SMALL BUSINESS

What can happen	What it means
Hard Drive Crashing	A common problem caused by computer viruses on home and small business computers has been extensive damage to files, software, and operating systems that can leave the user with a blank screen and costly repair bills. Often, more importantly, the small business owner or home user may lose irreplaceable data, such as customer records or personal correspondence.
Identity Theft	Information stored on a home computer may provide a hacker with enough personal data that the thief could apply for a credit card or identification in the user's name.
Credit Theft	Rather than applying for a new credit card, a thief might just use credit card data on the hard drive of a home user or small business to buy products online and have them shipped to a drop site, such as a commercial "mail box" store.
Tunneling	When employees work at home and then transfer files to a computer at the office, there is a potential that someone could remotely gain access to the home PC and place a secret file in a document that ends up on the company system.
Extortion	For the small businesses, someone may access the customers names and credit card numbers and threaten to post that information on a Web site, unless the business owner pays up.
Zombies	Automatic programs search for systems that are connected to the Internet, but are unprotected, take them over without the owner's knowledge, and use them for malicious purposes.
Compromise of Private Information	Some viruses send private or confidential files from a user's hard drive to people in the user's email address book.

Table 1-1

Discussion of Strategy

Five Steps to Safety

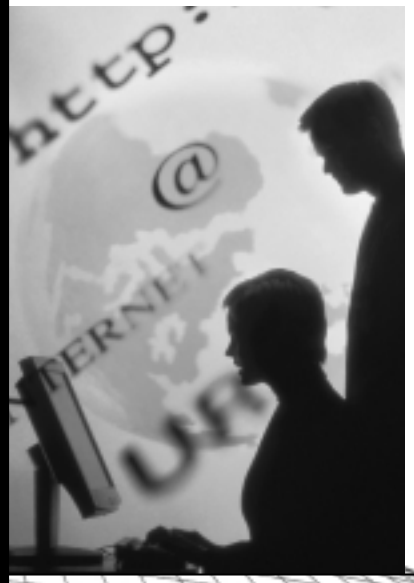
There are many places a homeowner, parent, or small business person can turn for help in avoiding security problems on the Internet. Before reviewing the helpful web sites cited below, consider these five simple steps:

1. Use a Tough Password: Hackers use software that is commonly available on the Internet to guess passwords and gain access to personal accounts and computers. It is important to use a strong password and change it on a regular basis. Strong passwords usually include:

- at least eight digits;
- a mix of upper and lower case letters;
- a random mix of letters and numbers (not just numbers at the end); and,
- keyboard symbols (#,$,&, *).

Home users should change their password at least once every six months, perhaps when the clocks change to daylight saving time and back to standard time.

2. Maintain an Updated Virus Protection Program: New viruses appear weekly and the new ones are the most frequent source of damage. The virus protection programs that come installed on the computer are quickly out of date, but they can be kept current by enrolling with the antivirus company for an update program. Many update programs now offer automatic notification of new data, so that the user does not need to remember to go to the antivirus site every week.



3. Update Patches: Many commonly used software programs (operating systems, web browsers, e-mail readers, and others) are regularly discovered to have security holes or flaws. The software companies issue the equivalent of "recall notices," but unlike a similar notice from a car company, it may not appear in the mail. Typically, a user has to go to the software company's web page to discover the problem and the solution. The solution is usually a small amount of additional software that can be downloaded over the Internet. These fixes, called "patches," are recommended for most home users and small businesses running uncomplicated systems. (In larger systems, the patch must be analyzed first to see if it will create conflicts with other programs.)

4. Filtering: Parents may want to consider managing their children's Internet use with software that allows them access to age-appropriate sites and materials. Many ISPs offer such software or filters, or they can be obtained from private vendors. In addition to filtering inappropriate sites, a parent may wish to limit the people from whom their child can receive e-mail. Most ISPs allow users to filter by listing the addresses from which they are willing to receive e-mail on all e-mail accounts they maintain, or just on their children's.

5. If you Have a Cable Modem, Digital Subscriber Line (DSL), Satellite or Other High Speed Connection: A high-speed connection that is always connected to the Internet (or more often than with dial up modems) makes the home user or small business an attractive target for the "bots" that search the Internet automatically for insecure connections. Even with updated virus software and current patches, smart "bots" can find a way to get into a system without the user knowing it. To prevent such covert entries, those with broadband connections (e.g., DSL, cable, satellite or wireless) should have additional software, known as a "firewall."

Firewalls can be easily configured to close the many doors to the Internet that all computers have, leaving open only the few that people typically use (e.g., for e-mail and web browsing). A user can specify what Internet programs are trusted to enter, and require all others to knock and be granted permission.

Where to go for General Cybersecurity Advice

An alliance of government agencies, corporations, and nongovernment organizations have joined to form the "National Cyber Security Alliance" to help home users, parents, and small businesses. Their web site is filled with helpful information and links to other sites with additional data. Go to: **www.StaySafeOnLine.info**.

For Small Businesses

Small business persons may want to seek cybersecurity ideas from local programs at nearby community colleges or chambers of commerce. On the national level, the Federal government's Small Business Administration (**www.sba.gov**) and the not-for-profit National Federation of Small Businesses (**www.nfib.com**) can also provide assistance.

In many larger cities, the National Infrastructure Protection Center partners with local businesses, the FBI, and academic experts in chapters of "Infragard", a grass roots public-private partnership for cybersecurity and against cybercrime, **www.infragard.net**.

In some metropolitan areas, the U.S. Secret Service sponsors a public-private partnership for cybersecurity related to financial institutions, credit cards, and cell phone theft. These groups are called the "Electronic Crimes Task Forces," **www.usss.gov/ectf.htm**.

In addition, the Computer Security Division of the National Institute of Standards and Technology maintains a computer security resources web page which provides helpful links to other centers of expertise where users can locate more alerts, software updates, and lists of the most common security threats, **www.csrc.nist.gov**.

For Parents and Teachers

In addition to the web sites already noted above that provide filters and teaching ideas, there are additional resources online that can help plan curricula, provide children with good advice, and help parents to decide what is safe:

The "CyberSmart School Program" is designed for teachers and provides lesson plans and professional development material. See **www.cybersmart.org**.

"NetSmartz" is designed to teach children directly about what to watch out for when surfing the net. See **www.netsmartz.org**.

"Get NetWise" is a resource for families trying to decide what they should consider about their children's web access. See **www.getnetwise.org**.

The Information Technology Association Foundation sponsors "Cybercitizen Awareness," which teaches teenagers about ethics online and the risks of cybercrime. Its site also provides material for teachers, parents, and smaller children. See **www.cybercitizenship.org**.

AGENDA

LEVEL 1: The Home User and Small Business

RECOMMENDATIONS

*Specific actions that government and nongovernment entities can take to promote cybersecurity.**

R1-1 Because automated hacking programs scan the Internet for unprotected broadband connections to exploit, those home users and small businesses planning to install a DSL or cable modem should consider installing firewall software first. (Some Internet service providers (ISPs), offer firewall software with DSL or cable modem set up.) Once firewall software is installed, it is important to regularly update it by going to the vendor's web site.

R1-2 Because new computer viruses are introduced every week, home users and small businesses should regularly ensure that they are running an up-to-date "antivirus system." (Some antivirus vendors offer automatic updates online. Some Internet service providers scan all incoming e-mail for viruses before the e-mail gets to the user's computer.)

R1-3 Because new viruses often come as e-mail, home users should use caution when opening e-mail from unknown senders, particularly those with attachments. To reduce the number of unknown senders, home users should consider using software that controls unsolicited advertisements, called "spam." (Some ISPs offer programs to block spam. Some ISPs also offer to block all incoming e-mail except from those friends and associates that the user selects.)

R1-4 Home users should also regularly update their personal computer's operating systems (such as Microsoft Windows, Linux) and major applications (software that browses the Internet or creates documents, charts, tables, etc.) for security enhancements by going to the vendors' web sites. (Some software vendors offer automatic updates online.)

R1-5 Internet service providers, antivirus software companies, and operating system/application software developers should consider joint efforts to make it easier for the home user and small business to obtain security software and updates automatically and in a timely manner, including warning messages to home users about updates and new software patches.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

PROGRAMS

Existing efforts in cybersecurity.

P1-1 Stay Safe Online web site: An alliance of government agencies, corporations, and nongovernment organizations have come together to form the National Cyber Security Alliance to help home users, parents, and small businesses. Their web site is filled with helpful information and links to other sites with additional data. Go to **www.StaySafeOnline.info**.

P1-2 FTC "Guide for E-Consumers," **www.ftc.gov/bcp/conline/pubs/alerts/glblalrt.htm**.

P1-3 FTC "How to Be Web Ready," **www.ftc.gov/bcp/conline/pubs/online/webready/index.htm**.

P1-4 FTC "How to Protect Kids' Privacy Online," **www.ftc.gov/bcp/conline/pubs/online/kidsprivacy.htm**.

P1-5 InfraGard: In many larger cities, the National Infrastructure Protection Center partners with local businesses, the FBI, and academic experts in chapters of InfraGard, a grass roots public-private partnership for cybersecurity and against cybercrime **www.Infragard.net**.

P1-6 The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) **www1.ifccfbi.gov/index.asp**.

P1-7 American Library Association, "The Librarian's Guide to Cyberspace for Parents and Kids," **www.ala.org/parentspage/greatsites/guide.html**.

P1-8 The FTC, U.S. Secret Service, the FBI, and others have formed the "Consumer Sentinel" to help consumers get the facts on frauds from Internet cons, prize promotions, work-at-home schemes, and telemarketing scams to identity theft and make it easy to file fraud complaints so they can be shared with law enforcement officials across the nation **www.consumer.gov/sentinel/**.

P1-9 DOJs Computer Crime Web site: information regarding a wide variety of computer crime and computer security issues, including a children's Cyberethics page and a link to invite DOJ experts to speak **www.cybercrime.gov**.

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D1-1 The biggest business in America is small business. Working through the SBA, many small businesses are able to obtain loans guaranteed by the Federal government. Increasingly, the cybersecurity of small business can impact its employees and the broader economy. Should SBA loans require an IT security checklist?

D1-2 How can parents and children create a useful dialogue about securing their families' cyberspace? Cybersecurity is an area where parents and children each bring their own experience and expertise. By sharing these experiences, families can improve the cybersecurity of their household and contribute to an overall increase in America's cybersecurity.

LEVEL 2: LARGE ENTERPRISES

The strategic goal is to encourage and empower large enterprises to establish secure systems. This goal can be achieved through a range of voluntary initiatives including:

- raising the level of responsibility;
- creating corporate security councils for cybersecurity, where appropriate;
- implementing A.C.T.I.O.N.S. (defined in the table, infra) and best practices; and,
- addressing the challenges of the borderless network, mainframe security, instant messaging and other technologies.

Issues and Challenges

The development of a resilient cyber infrastructure that supports the long-term economic development of the nation depends in large part on the security of large enterprises. Large enterprises do not operate in isolation. Rather, they provide a constant flow of data that helps to drive the U.S. economy. Resiliency enables the nation to protect, detect, respond, and recover from cyber-based attacks. Developing this essential economic attribute is a collective challenge that can only be achieved through the corporate actions of large enterprise operators.

Large enterprises can play a unique role in developing this resiliency by ensuring that security is an integral component of their individual architectures, network operations, and management. The massive networks that facilitate the transactions of the U.S. economy constitute both our strength and our vulnerability.

The economic consequences of cyber attacks on businesses do more than impact the short-term bottom line of a company. Rather such events can compromise intellectual property and sensitive research that can lead to long-term macroeconomic loss. Moreover, security breaches can place customer data at risk and erode confidence and trust in an enterprise and its affiliates. Cyber vulnerabilities can significantly damage large enterprises, if not remediated. Moreover, these same vulnerabilities can be exploited to harm other systems outside the enterprise and even infrastructures.

Cybersecurity is one of the most complex challenges facing large enterprises today. Technical and policy challenges, global interconnections, and Internet-based commerce complicate the provision and management of enterprisewide security. Cybersecurity is a moving and dynamic target. There is no one-size-fits-all solution, or special technology, that will make an enterprise secure. In fact, 100 percent security is not a possibility in today's interconnected environment.

Ultimately, addressing cybersecurity within an enterprise is more than a technical problem, it is a management challenge. The scope of the risks presented by cybersecurity can be effectively managed by engaging senior leadership and by involving the corporate board of directors. Cybersecurity may warrant close attention from the board of directors. Considering security only after an incident has occurred places the business, the customers, and even the country at risk. In contrast, effective governance of cybersecurity promotes growth, productivity, and shareholder confidence.

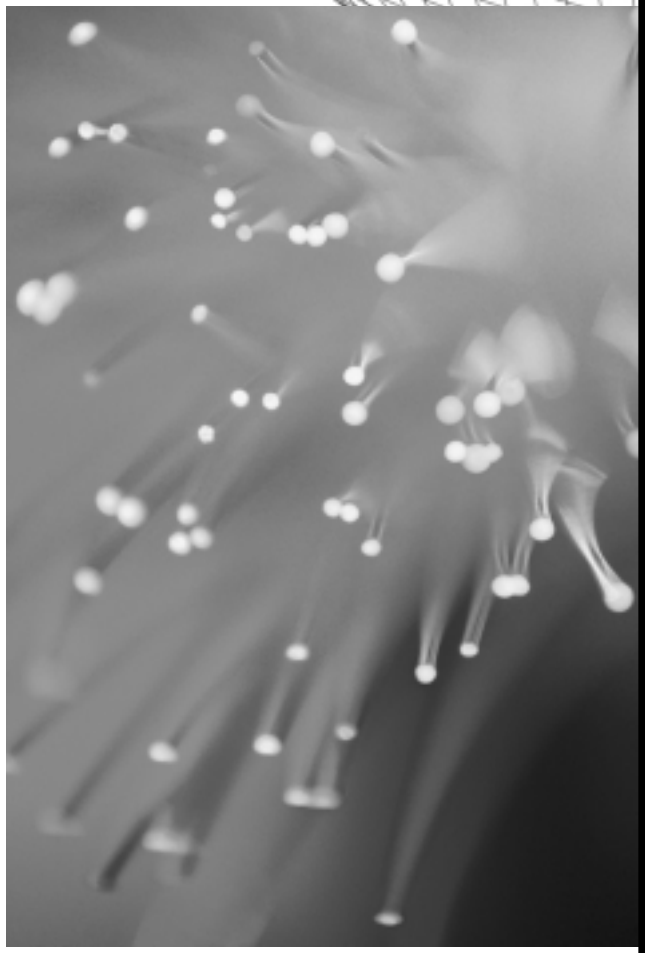
Discussion of Strategy

Raise the Level of Responsibility

The board of directors plays a vital role in the corporate system. Shareholders ultimately own corporations. Corporate boards are accountable to shareholders, and, in turn, managers are accountable to the board. Raising the responsibility for cybersecurity to the level of the board of directors can have significant enterprisewide results. The board can better understand its enterprise by asking a series of questions about the

Questions corporate boards, financial analysts and investors should ask:

1. What board members are responsible for IT security and risk management oversight? Do these members provide an annual report to the board?
2. Who is the senior most corporate official responsible for IT security and to whom is he or she directly accountable?
3. How often do the CEO and COO review IT security and the overall corporate risk management?
4. What internal IT security policies exist and do they involve annual training of all employees?
5. Are the security controls of the company's computer systems sufficient to prevent unauthorized access to files, alterations of data, loss or theft of trade secrets and assets?



sufficiency of the organization's security structure and controls. To better understand the scale, scope, and effectiveness of enterprise cybersecurity, some boards, through an appropriate board committee, require periodic reporting by management.

The U.S. Department of Commerce uses its Critical Infrastructure Assurance Office (CIAO) as its lead office to partner with the private sector to help promote the importance of information security management and assurance to senior managers and directors. The CIAO has been working with the Institute of Internal Auditors (IIA) to help raise awareness about critical infrastructure protection in the context of a large enterprise. The IIA teamed with the National Association of Corporate Directors, the American Institute of Certified Public Accountants, and the Information Systems Audit and Control Association to host a series of informative summits across the country. These highly successful events heightened the awareness of corporate directors and top managers of their key role in safeguarding the information assets of the organizations they oversee.

Towards a Corporate Security Council

Today's diffuse security threats require new thinking and approaches. For example, some large enterprises may want to consider creating a corporate security council consisting of key members of the company with security-related responsibilities. Corporate officials with risk management and security-related responsibilities could form the core of such a team. These officials may include:

- The Chief Operating Officer (COO);
- The Chief Information Officer (CIO);
- The Chief Technology Officer (CTO);
- The Chief Information Security Officer (CISO)/ Chief Security Officer (CSO);
- The Chief Risk Officer (CRO);
- The Privacy Officer; and,
- The official responsible for physical security.

These officials can coordinate preparedness plans to ensure that cybersecurity is factored into the operations of the enterprise. Because a failure in cybersecurity can compromise intellectual property, customer data, and business operations, it is important that the key decision makers and technical officials are brought together. Furthermore, they can advise the CEO in a crisis and coordinate the execution of their contingency and continuity plans in response to cybersecurity incidents. The resiliency of large enterprises contributes directly to resiliency of the macro economy, and ultimately, the nation.

A.C.T.I.O.N.S. and Best Practices

There are a wide range of A.C.T.I.O.N.S. that can be undertaken to facilitate the integrity, reliability, availability, and confidentiality of the enterprise. (Figure L2-1)

A.C.T.I.O.N.S. AND BEST PRACTICES

Authentication	Implement processes and procedures to authenticate, or verify, the users of the network. This may include techniques such as PKI using smart cards, secure tokens, biometrics, or a combination of efforts.
Configuration management	Plan enterprise architecture and deployment with security in mind. Manage configurations to know exactly what hardware, operating systems and software are in use, including specific versions and patches applied; create robust access and software change controls, segregate responsibilities; implement best practices; and, do not use default security settings.
Training	Train all employees on the need for IT security and ensure that security is factored into developing business operations. Foster an enterprise culture of safety and security.
Incident response	Develop an enterprise capability for responding to incidents, mitigating damage, recovering systems, investigating and capturing forensic evidence, and working with law enforcement.
Organization network	Organize enterprise security management, IT management, and risk management functions to promote efficient exchange of information and leverage corporate knowledge.
Network management	Create a regular process to assess, remediate, and monitor the vulnerabilities of the network; consider developing automated processes for vulnerability reporting, patching, and detecting insider threats. Internal and external IT security audits can also supplement these efforts.
Smart procurement	Ensure that security is embedded in the business operations and the systems that support them. Embedding security is easier than "bolting it on" after the fact.

Figure L2-1

The Borderless Network

One of the most dramatic challenges to enterprise security is the borderless corporate network. The rapid adoption of networking and business-to-business (B2B) commerce has eroded the once well-defined borders of corporate networks. Today's enterprises are so interconnected that when enterprises take on joint ventures they may end up with virtual insiders. Virtual insiders are the people connected to a network that the owner does not know are there. These connections are not recorded in the enterprise management plan and can often result when a contractor grants access to a subcontractor. Ubiquitous connectivity is driving fundamental changes in the approaches to enterprise security management. These changes are, in turn, requiring new research, tools, and approaches.

Mainframe Computers

Mainframe computers continue to play important roles in large enterprises. However, security policies and practices tend to focus on desktop computers, network servers, network devices, the Internet, and pervasive computing devices – to the exclusion of mainframe computers. Mainframe security personnel have been redeployed or recruited toward new opportunities. Advances in mainframe technology and connection to the Internet have created new risks and vulnerabilities rendering existing mainframe security policies and practices obsolete. Furthermore, the frequency and rigor of qualified mainframe audits have deteriorated to the point they are no longer capable of identifying these threats. Organizations and government agencies must refresh their security polices, practices and technologies as vigorously as elsewhere or risk exploitation from new threats.

Instant Messaging

Instant messaging (IM) programs present another point of vulnerability to large enterprise systems. For example, IM programs can by-pass firewalls and antiviral scanners allowing malicious code, unauthorized intruders, and valuable data to covertly move in and out of enterprise systems. Enterprises should adjust their computer security polices to appropriately account for the risk presented by IM programs.

Insider Threats

Approximately 70 percent of all cyber attacks on enterprise systems are believed to be perpetrated by trusted "insiders." Insiders are trusted people with legitimate access rights to enterprise information systems and networks. Such trusted individuals can pose a significant threat to the enterprise and beyond. The insider threat can arise from the intentional malice of a disgruntled employee or accidentally from the poor security practices of a careless or unaware employee. Whether the threat is intentional or accidental, the results are often the same—damage, disruption, and loss of data. Effectively mitigating the insider threat requires policies, practices and continued training. Three common policy areas which can reduce insider threat include: (1) access controls, (2) segregation of duties, and (3) effective policy enforcement.

- Poor access controls enable an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage.
- Segregation of duties is important in assuring the integrity of an enterprise's information system. No one person should have complete control of any system. Failing to properly segregate the computer duties of an organization's staff can dramatically increase the risk of errors or fraud.
- Effective enforcement of an enterprise security policy can be challenging and requires regular auditing. New automated software is beginning to emerge which can facilitate efficient enforcement of enterprise security. These programs allow the input of policy in human terms, translation to machine code, and then monitoring at the packet level of all data transactions within, and outbound from, the network. Such software can detect and stop inappropriate use of networks and cyber-based resources.

AGENDA

LEVEL 2: Large Enterprises

RECOMMENDATIONS

*Specific actions that government and nongovernment entities can take to promote cybersecurity.**

R2-1 CEOs should consider forming enterprisewide corporate security councils to integrate cybersecurity, privacy, physical security, and operational considerations.

R2-2 CEOs should consider regular independent Information Technology (IT) security audits, remediation programs, and reviews of best practices implementation.

R2-3 Corporate boards should consider forming board committees on IT security and should ensure that the recommendations of the chief information security official in the corporation are regularly reviewed by the CEO.

R2-4 Corporate IT continuity plans should be regularly reviewed and exercised and should consider site and staff alternatives. Consideration should be given to diversity in IT service providers as a way of mitigating risks.

R2-5 Corporations should consider active involvement in industrywide programs to: (a) develop IT security best practices and procurement standards for like companies; (b) share information on IT security through an appropriate information sharing and analysis center (ISAC); (c) raise cybersecurity awareness and public policy issues; and, (d) work with the insurance industry on ways to expand the availability and utilization of insurance for managing cyber risk.

R2-6 Corporations should consider joining in a public-private partnership to establish an awards program for those in industry making significant contributions to cybersecurity.

R2-7 (1) Enterprises should review mainframe security software and procedures to ensure that effective technology and procedural measures are being utilized, (2) IT vendors and enterprises employing mainframes servers should consider developing a partnership to review and update best practices of mainframe IT security and to ensure that there continues to be an adequate trained cadre of mainframe specialists; and, (3) IT security audits should include comprehensive evaluations of mainframes.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

PROGRAMS

Existing efforts in cybersecurity.

P2-1 CIAO and the Institute of Internal Auditors have been working to train and raise awareness about the importance of understanding IT security in the context of the overall enterprise mission **www.iia.org**.

P2-2 The National Threat Assessment Center (NTAC) with the CERT/Coordination Center is presently conducting a study on this critical topic. Using their experience from previous studies—the Exceptional Case Study Project and the Safe School Initiative—NTAC hopes to build a more complete understanding of this threat to enterprise IT security. For more information on this topic, look in detail at the full Strategy or view the NTAC web site at **www.survey.cert.org/Insider Threat** to learn how you can participate, anonymously, in the study.

P2-3 The Internet Security Alliance has recently issued a "*Common Sense Guide for Senior Managers*," which includes the organization's top ten recommended information security practices **www.isalliance.org.**

P2-4 Many critical infrastructure industries have formed information sharing and analysis centers (ISACs) in order to disseminate cybersecurity information to their respective sectors.

P2-5 In many larger cities, the National Infrastructure Protection Center partners with local businesses, the FBI, and academic experts in chapters of InfraGard, a grass roots public-private partnership for cybersecurity and against cybercrime **www.infragard.net.**

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D2-1 Cybersecurity is a constant process which requires regular assessments and remediation. Accordingly, cybersecurity can be enhanced with regular IT security audits. How often should large enterprises have cybersecurity audits performed by outside auditors?

D2-2 Cybersecurity is an integral component of a company's operations. When a company makes cybersecurity a management issue, it can better protect its intellectual property and its business operations. What should financial analysts and investors ask companies about their security programs before investing?

D2-3 How can large enterprises facilitate the identification and implementation of best practices for cybersecurity?

D2-4 Should the National Security Telecommunications Advisory Committee and the National Infrastructure Assurance Council examine the need and possible benefits of establishing an independent organization, similar to the accounting profession, which would develop standards, guidance, and auditing procedures for IT security enterprises?

LEVEL 3: THE FEDERAL GOVERNMENT

The Federal government's strategic goal is to significantly improve the cybersecurity[1] of Federal information and information technology. To achieve this goal, each agency will be expected to create and implement the following formal three-step process to achieve greater security:

- step one — identify and document enterprise architectures;
- step two — continuously assess threats and vulnerabilities, and understand the risks they pose to agency operations and assets; and,
- step three — implement security controls and remediation efforts to reduce and manage those risks.

In addition, to assist the individual agencies in implementing the foregoing three-step process, the following overarching structures and processes will be implemented under the Federal government IT security program through the following actions:

- exercise budget and security oversight (OMB); to hold government agencies accountable for systems security;
- explore greater use of cross-government acquisition and centralized management;
- conduct overarching reviews by the Executive branch Information Systems Security Committee to identify, recommend, and coordinate Federal security enhancements;
- establish an Office of Information Security Support Services within the Federal government;
- develop a Federal response plan to manage cyber incidents and prepare for contingencies; and,
- explore whether specific criteria for independent security reviews and reviewers are necessary and whether contractor certification is necessary.

[1] *Note: The term "cybersecurity" used in the Federal government section of this document is synonymous with the term "computer security" used in OMB guidance.*

Issues and Challenges

The security of the Federal government is the collective responsibility of its departments and agencies. Accepting anything less than excellence in Federal computer security places the nation and the American people at risk.

Historically, the Federal government did not consider information security systemically; instead, it often merely "tacked on" security as an afterthought—reacting to threats, vulnerabilities, and attacks as they arose, rather than anticipating and attempting to avoid problems.

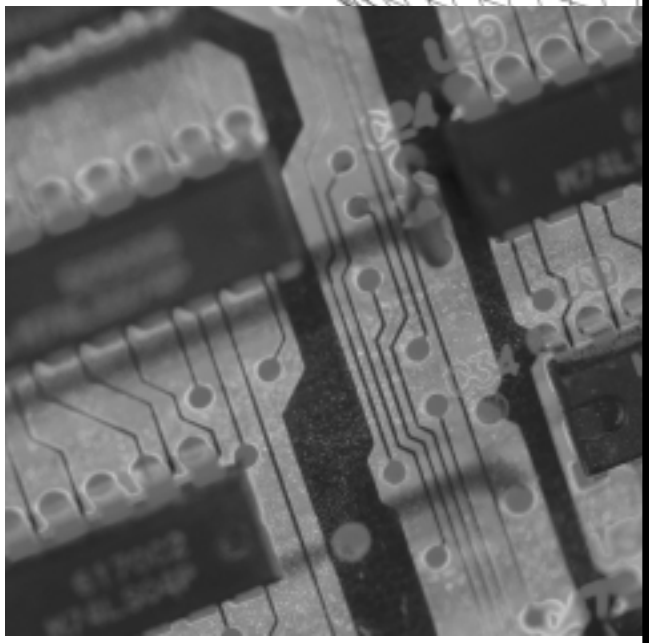
To overcome this deficiency, OMB established a governmentwide IT security program, as required by law, to set IT security policies and perform oversight of Federal agency compliance with security requirements. This program is based on a cost-effective, risk-based approach. Agencies must ensure that security is integrated within every investment. This approach is designed to enable Federal government business operations, not to unnecessarily impede those functions.

Federal Government IT Security Remediation Process

A key step to ensure the security of Federal information technology is to understand the current state of the effectiveness of security and privacy controls in individual systems. Once identified, it is equally important to maintain that understanding through a continuing cycle of risk assessment. This approach has long been suggested by the General Accounting Office, is reflected in OMB security policies, and is featured in the Government Information Security Reform Act of 2000 (GISRA).

OMB is responsible for the development and oversight of the implementation of governmentwide policies, principles, standards, and guidelines for Federal government computer security programs. Within a statutory framework, OMB issues security policies and ensures that security is appropriately integrated with capital planning and budget guidance. Oversight is achieved largely in the following ways: via the budget and capital planning process, independent program reviews, annual agency program reviews, independent Inspector General (IG) evaluations, agency reports to OMB, agency security corrective action plans, and an annual OMB report to Congress.

Through the implementation of GISRA, Federal agencies are required to conduct annual security reviews of all programs and systems, and IGs



perform annual independent evaluations of an agency's security program and a subset of systems. These reviews and evaluations, along with other applicable security reviews, identify an agency's security performance gaps. To ensure that those gaps are addressed, agencies are required to develop corrective action plans for every system and program where a weakness was found. Corrective action plans for agency systems are tied directly to each agency's funding request for the system—OMB funding approval for systems is contingent upon correction of outstanding security weaknesses. Additionally, agencies must ensure that security has been incorporated and security costs reported for every IT investment through the Federal capital planning process. OMB policy stipulates that specific lifecycle security costs be identified, built into, and funded as part of each

system investment. Failure to do so results in disapproval of funding for the entire system. On a quarterly basis, agencies report their progress in closing their security performance gaps. Annually, OMB reports the results of agency security reviews and IG evaluations to Congress.

The annual reviews identify weaknesses and vulnerabilities and, for the first time, across the Federal government, there is a detailed understanding of IT security performance gaps. More importantly, through the development and use of corrective action plans, the Federal government has a uniform process to track progress in fixing those weaknesses.

The annual status reports focus on management-level issues to ensure that security is viewed as an essential management function. OMB agrees with GAO, agency IGs, and other experts that a sound management foundation is essential to ensure that important, but lower-level, technical security details are adequately addressed. Corrective action plans and quarterly updates are the next step for Federal agencies to reflect the status of corrective actions for specific agency programs and systems. These corrective action plans include an identification of all management, operational, and technical security weaknesses, the estimated resources needed to correct the weaknesses, the projected timeline for corrective action, and whether corrections are on track.

Current Gaps and Weaknesses

OMB's first report to Congress on government information security reform in February 2002 identified six common governmentwide security performance gaps.

For the most part, these gaps are not new or surprising. OMB, along with GAO, and agency IGs, have found them to be problems for at least six years. The evaluation and reporting requirements of GISRA have given OMB and Federal agencies an opportunity to develop a comprehensive, cross-government baseline of agency IT security performance that has not been previously available. These weaknesses include:

1. *Lack of senior management attention.*
   Senior leaders must consistently establish and maintain control over the security of the operations and assets for which they are responsible. As GISRA recognizes, security is a management function which must be embraced by each Federal agency and agency head.
2. *Lack of performance measurement.*
   Agencies must be able to evaluate the performance of officials charged with implementing specific requirements of GISRA. To evaluate agency actions, agencies must measure job and program performance, i.e., how senior leaders evaluate whether responsible officials at all levels are doing their jobs. They must be able to evaluate the performance of officials charged with securing agency operations and assets. Virtually every agency response regarding performance implies that there is inadequate accountability for job and program performance related to IT security.
3. *Poor security education and awareness.*
   Agencies must improve security education and awareness. General users, IT professionals, and security professionals need to have the knowledge to do their jobs effectively before they can be held accountable.
4. *Failure to fully fund and integrate security into capital planning and investment control.*
   Security must be built into and funded within each system and program through effective capital planning and investment control. As OMB has done for the past two years in budget guidance, Federal agencies were instructed to report on security funding to underscore this fundamental point. Systems that do not integrate security into their IT capital asset plans will not be funded.
5. *Ensuring that contractor services are adequately secure.*
   Agencies must ensure that contractor services are adequately secure because most Federal IT projects are developed and many operated by contractors. Therefore, IT contracts, including those for telecommunications, need to include adequate security requirements. Many agencies reported no security controls in contracts or no verification that contractors fulfill any requirements that may be in place. Additionally, the OMB report discusses pervasive security flaws found in many of today's commercial software products. These flaws go well beyond security to the very performance of the products themselves, and it is time to address this problem at a national level.
6. *Failure to detect, report, and share information on vulnerabilities.*
   Far too many agencies have virtually no meaningful system to test or monitor system activity; therefore they are unable to detect intrusions, suspected intrusions, or virus infections. This places individual agency systems and operations at great risk since response depends on detection. Perhaps most significant is not detecting and reporting IT security problems could cause cascading harm. America's vastly inter-networked environment also means shared risk with the best security being only as strong as the weakest link.

Early warning for the entire Federal community starts first with detection by individual agencies, not incident response centers at the FBI, GSA, DOD, or elsewhere. The latter can only know what is reported to them, reporting can only come from detection, and guidance for corrective action depends upon both. This need is thus not a technical one, but a management one. Additionally, it is critical that agencies and their components report all incidents in a timely manner to GSA's Federal Computer Incident Response Center and appropriate law enforcement authorities, such as the FBI's National Infrastructure Protection Center, as required by GISRA.

Additional issues and challenges have also been identified:

Authentication: Key to Cybersecurity

Intruders gaining access to systems by pretending to be the authorized user can do immense harm. As described in NIST's "*Introduction to Computer Security*"—The NIST Handbook (located at **www.csrc.nist.gov/**), there are three basic means to ensure the identification and authentication of users—applying something the user knows (password), applying something the user has (token or smart card), and applying something the user is (biometric information). The weakest and most commonly used method of identification and authentication is applying something a user knows. Why is it the weakest? Because would-be intruders (and auditors) often successfully discern passwords through both pretext conversations with unsuspecting users and relatively simple technical means.

If an intruder were to obtain the password of an agency employee, he would gain the same trusted privileges as the employee and could operate behind the firewall, use and interfere with system resources, and gain real-time access to sensitive data. What is more, the intruder might also have access to other systems in the domain.

If the victim employee had administrator or super-user privileges, the intruder would likewise acquire those privileges and could have unlimited access to the entire network and the information on it. What is worse, the intruder could acquire valuable information and an understanding of system weaknesses, escape without detection, perhaps share what they have learned with others, and return another day to inflict even greater damage.

Inconsistent Contingency Planning

Among the lessons learned from security reviews following the events of September 11, was that Federal agencies had vastly inconsistent, and in most cases incomplete, contingency capabilities for their communications and other systems. Contingency planning is a key element of cybersecurity. Without adequate contingency planning and training, agencies may not be able to effectively handle disruptions in service and ensure business continuity. Continuity plans cannot simply be written and placed on the shelf. These plans must be tested on a regular basis to ensure that agency employees are fully aware of their roles and responsibilities.

Discussion of the Strategy

Agency-Specific Measures

In order to fully realize the intent of GISRA, the Federal government must have a comprehensive and cross-cutting approach to improving cybersecurity. Clearly, cybersecurity is not a "one-size-fits-all" solution. However, there are three elements that are central to attaining and maintaining robust cyber security for the Federal government. These include:

- identifying and documenting enterprise architectures;
- continuously assessing threats and vulnerabilities, and understanding the risks they pose to agency operations and assets; and,
- implementing security controls and remediation efforts to reduce and manage those risks.

Step One — Identify and Document Enterprise Architectures. As a matter of OMB policy, each agency must identify and document their enterprise architecture, including developing an authoritative inventory of all operations and assets, and all agencies IT systems, critical business processes, and their inter-relationships with other organizations. This will produce a governmentwide view of critical security needs. The Federal government is now integrating OMB and Federal CIO Council governmentwide enterprise architecture activities and the Critical Infrastructure Assurance Office's Project Matrix efforts. The integration is intended to better identify and document agency and cross-government core processes, areas of unnecessary duplication, and areas where planned redundancy is lacking. Modeling and evaluating potential implications of threats and vulnerabilities on cross-agency business processes will also benefit from the integration efforts.

Step Two — Continuously Assess Threats and Vulnerabilities, and Understand the Risks they Pose to Agency Operations and Assets. Commercial automated auditing and reporting mechanisms are now available to validate the effectiveness of the security controls across a system and are essential to continuously understand risks to those systems. Some, but not all, civilian agencies have taken steps to increase the use of these automated tools. More agencies need to do so. Therefore, the Federal government will drive the greatly expanded use of effective automated tools to detect intrusions, conduct periodic vulnerability assessments, actively manage and preempt threats, and continuously audit the security posture of information technology systems. (See recommendation R3-5.)

As agencies expand their use of automated tools, the Federal government will consider whether benefits derive from consolidated acquisition, operation, and management of those tools. One possible approach, but certainly not the only one, could be to centrally deploy and manage them from FedCIRC. Such consolidation could standardize and automate vulnerability identification and reporting—one of the six significant weaknesses identified in OMB's February 2002 security report to Congress.

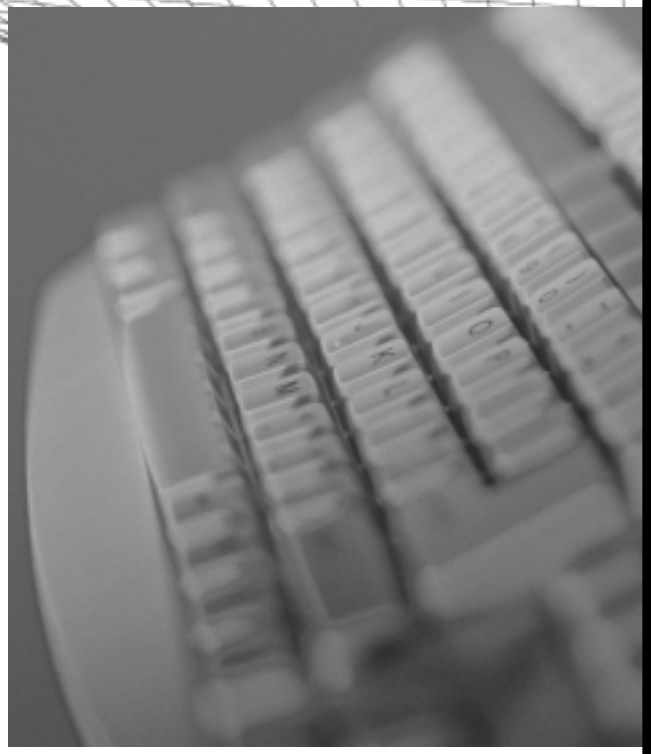
Automated tools on agency networks could continuously assess system vulnerabilities, collect and analyze firewall and intrusion detection audit logs, audit configuration and security policy controls, and automatically report the results to FedCIRC. Automated tools can be helpful in analyzing data, providing forward-looking assessments, and alerting agencies of unacceptable risks to their operations.

At the same time however, it is important that individual agencies and program officials within them continue to take responsibility and be held accountable for the security of the operations and assets under their control. Separating responsibility and accountability sends the incorrect signal that security is not their job—it is. Thus any centralization will be carefully considered before being adopted. (See recommendation R3-3)

Step Three — Implement Security Controls And Remediation Efforts To Reduce or Manage Those Risks. The implementation of security controls that maintain risk at an acceptable level and test the controls to ensure that they continue to be effective can often be accomplished in a relatively brief amount of time. However, the remediation of vulnerabilities is a much more complex challenge. Software is constantly changing and each new upgrade can introduce new vulnerabilities. As a result, vulnerabilities need to be assessed continuously. Remediation often involves "patching," or installing pieces of software or code that are used to update the main program. The remediation of Federal systems must be planned in a consistent fashion. In addition, the Federal government should explore more secure network protocols as they develop and assess how their adoption and implementation could benefit agency operations. When it is shown that such secure protocols can have a cost-effective benefit on agency operations, the Federal government should lead in adopting and implementing them.

Identifying and Authenticating Users and Maintaining Authorization

Through the electronic government e-Authentication initiative and other means, the Federal government is promoting a continuing chain of security for all Federal employees and processes, including the use where appropriate of biometric smart cards for access to buildings and computers, and authentication from the moment of computer log on. The benefits of such an approach are clear. To establish and maintain secure system operations, organizations must ensure that the people on the system are who they say they are and are doing only what they are authorized to do.



Identifying and authenticating each system user is the first link in the system security chain, and it must take place whenever system access is initiated. Many authentication procedures used today are inadequate and, even correctly configured passwords can often be obtained from users. However, as GAO and others frequently report, passwords are not being changed from the system default, are often incorrectly configured, and are rarely updated.

By promoting multi-layered identification and authentication—the combined use of strong passwords, smart tokens, and biometrics—the Federal government will eliminate many significant security problems that it has today. Through the ongoing e-Authentication initiative, the Federal government will review the need for stronger access control and authentication; explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms; and, consequently, further promote consistency and interoperability.

System Configuration Management

Using the Board's Executive branch Information Systems Security Committee and the governmentwide architecture development activities, OMB is exploring ways to promote greater uniformity of systems throughout the Federal enterprise, and to simplify and unify security processes to increase efficiency and effectiveness.

Through the budget process, the Federal government will drive agency investments in commercially available automated tools to assist them in ensuring the accurate maintenance of their architectures and system configuration. As discussed in the Federal CIO Council's "*Practical Guide to Federal Enterprise Architecture*," configuration management is critical to an architecture maintenance program. See the CIO Council's "Guide" at **www.itpolicy.gsa.gov/mke/archplus/ea_guide.doc**.

The guide also describes the need for periodic configuration audits as an architecture control feature. Automated tools are now widely available commercially to perform such audits. Configuration control has incidental and important benefits to security, i.e., controlling system configuration permits agencies to more effectively and efficiently enforce policies and permissions and more easily install antivirus definitions and other software updates and patches across an entire system or network.

The National Information Assurance Partnership (NIAP)

NIAP is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under the Computer Security Act of 1987.

The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the nation's critical information infrastructure. More information on the partnership can be found at www.niap.nist.gov/.

Improved Security in Government Outsourcing and Procurement

Through a joint effort of OMB's Office of Federal Procurement Policy, the Federal Acquisition Regulations Council, and the Executive branch Information Systems Security Committee, the Federal government is identifying ways to improve security in agency contracts and evaluating the overall Federal procurement process as it relates to security. Agencies maintaining the security of outsourced operations was one of the key weaknesses identified in OMB's February 2002 security report to Congress.

Additionally, the Federal government is conducting a comprehensive review of the NIAP, to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. This review will include lessons-learned from implementation of the Department of Defense's July 2002 policy requiring the acquisition of products reviewed under the NIAP or similar evaluation processes. That policy stipulates that if an evaluated product of the type being sought is available for use, then the DOD component must procure such evaluated product. If no evaluated product is currently available, the component must require prospective vendors to submit their product for evaluation to be further considered.

Following this program review, the government will evaluate the cost-effectiveness of expanding the program to cover all Federal agencies. If this proves workable, it could both improve government security and leverage the government's significant purchasing power to influence the market and begin to improve the security of all consumer information technology products. The Federal government recognizes that past efforts such as this have failed, but believes that the heightened level of government and consumer concerns over significant flaws in information technology products warrants renewed efforts.

Framework for the Strategy

Hold Agencies Accountable

Since the beginning of his Administration, the President has called for better management of the Federal government. Beginning with his Budget Blueprint in February 2001, continuing in the FY 2002 and 2003 budgets, and in his Management Reform Agenda, the President has repeatedly spelled out a clear agenda for government reform. The President has ordered the pursuit of five governmentwide initiatives that together will help government achieve better results. See **www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf**. Because much of what is required to develop and sustain an effective security program is a solid management foundation, the Federal government is using the President's Management Agenda to build that foundation and drive the reform of its security program.

One of the management agenda's initiatives—expanded E-Government—harnesses the power of information technology and the Internet to make government more productive. The *National Strategy to Secure Cyberspace* complements these efforts by making sure that the E-Government initiative ("E-Gov"), and the infrastructure it relies upon, are secure. The Federal government will then be better able actively to anticipate threats and vulnerabilities, preempt them where possible, and survive them when preemption is not possible. In this way, the Federal government will set an example for all owners and operators of the nation's cyber infrastructure.

To achieve this standard of performance, good intentions and good beginnings are not the measure of success. Rather, the government will require demonstrated performance and results. In order to ensure accountability and measure performance in cyber security, the Administration will do three things:

- *Analyze Empirical Evidence of Agency Performance to Evaluate Compliance.* GISRA required the Federal agencies to perform an annual independent evaluation of their information security program and practices. The results of these evaluations are reported to OMB. These reports include an accounting of all security weaknesses in agency systems and programs and a detailed corrective action plan with milestones and timelines. These reports are tied to the budget process and agency information technology funding requests to OMB must account for the lifecycle costs for security or they will not be approved. OMB uses this data to score the agencies' security performance. The first round of security reporting is reflected in OMB's February 2002 security report to Congress. See **www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf**.
- *Chart Agencies Progress Using the Management "Scorecard."* For each of the President's Management Agenda initiatives, OMB has adopted an Executive branch management "scorecard"—a simple "traffic light" grading system common today in well-run businesses. Green indicates success, and yellow shows mixed results. Within the E-Gov "scorecard," OMB measures agency performance with respect to security. See **www.whitehouse.gov/omb/memoranda/m02-02.html**.
- *Base Agency Funding Decisions on Demonstrated Cybersecurity Performance.* Over the next three years the Federal government will likely spend approximately $20 billion on IT security—including research and development. OMB will continue to use both the "scorecard" and the GISRA security reporting to inform budget decisions for agency requests for information technology. OMB policy is clear: requests for information technology will not be funded or resources will be reallocated if the agency has shown poor security performance or if it has not included security requirements in the life-cycle costs for each investment. See OMB's security investment policy, **www.whitehouse.gov/omb/memoranda/m00-07.html**.

These measures will help to ensure that each agency does its part to improve and maintain the overall Federal government security posture by developing and maintaining a solid security management foundation upon which operational and technical security controls are built. This management foundation includes assigning clear and unambiguous authority and responsibility for security, holding officials accountable for fulfilling those responsibilities, and integrating security requirements into budget and capital planning processes.

Establish an Office of Information Security Support Services

The "build once, use many" approach demands a central organization to manage and finance some of the initiatives. Moreover, the increasing complexity of information technology security is placing significant pressure on many (especially small) agencies to effectively address their security requirements. For the civilian agencies, an office in the proposed Department of Homeland Security could perform this operational support function. Operating under OMB oversight, this office could include resources from other agencies and could assist the agencies, OMB, NIST, the CIAO, and others in meeting their responsibilities. (See recommendation R3-9.)

Federal Cyber Incident Response Plan

The Incident Response Committee of the President's Critical Infrastructure Protection Board is developing a cyber annex to the Federal Response Plan (FRP) maintained by FEMA (**www.fema.gov/rrr/frp/frpintro.shtm**). The FRP establishes a process and structure for the systematic, coordinated, and effective delivery of Federal assistance to address the consequences of any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S.C. 5121, *et. seq.*). The cyber annex will identify lead agency roles, authorities, and policy governing Federal cyber response in the event of a large-scale cyber threat or attack. The annex will have a supplement with a comprehensive contingency plan detailing the Federal government's response to large-scale cyber incidents.

A valuable by-product of the foregoing effort will be to evolve incident response capabilities toward greater efficiency and improved coordination. An essential component of this enhanced capability is greatly improved analysis and warning, including moving from a retrospective view to a forward-looking one. The Federal government is also working to consolidate, and make uniform, agencies contingency and disaster recovery planning for their telecommunications networks and information systems.

Security Preparedness Exercise

To test the civilian agencies security preparedness and contingency planning, the Federal government is considering the use of a scenario based exercise to evaluate the impact of a threat on a selected cross-government business process. One such possibility could include governmentwide cybersecurity exercises. This approach is similar to that employed in 1998 by the Department of Defense in an effort known as "Eligible Receiver" and would be developed with the cooperation of each participating agency. The exercise would include most security disciplines—including physical, operations, information, and systems. Among other things, it would prove or disprove the notion that today's agency-specific exercises and isolated tests on individual systems do little to reveal how low probability events result in high consequences on interconnected systems and processes. Weaknesses discovered will be included in agency GISRA corrective action plans. (See recommendation R3-8.)

Explore Creation of a Separate Federal Telecommunications and Information Systems Infrastructure

Federal policy currently stipulates that each agency must plan and provide for the continuity of its operations including communications. Such planning and service provision should be consistent across the government, and departments considering creating new capabilities should examine cross-agency sharing arrangements.

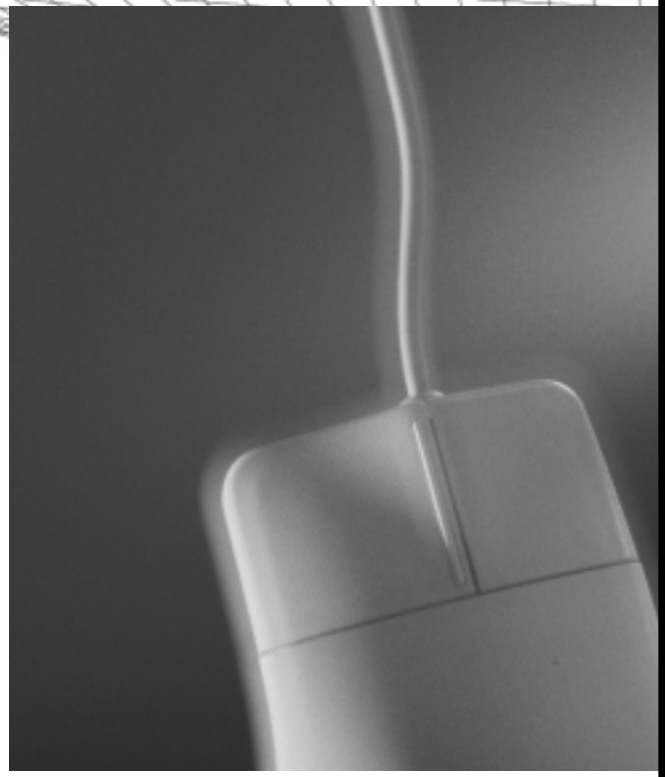
The Federal government will continue to assess the technical viability and cost effectiveness of various options that provide for the continuity of operations during service outages such as VPNs, "private line networks," and others. (See recommendation R3-6.)

Consider Developing Specific Criteria for Independent Security Reviews and Reviewers and Certification

With the growing emphasis on security comes the corresponding need for expert independent verification and validation of agency security programs and practices. GISRA and OMB's implementing guidance require that agencies' program officials and CIOs review at least annually the status of their programs. Few agencies have available personnel resources to conduct such reviews, and thus they frequently contract for such services.

Agencies and OMB have found that contractor security expertise varies widely from the truly expert to less than acceptable. Moreover, many independent verification and validation contractors are also in the business of providing security program implementation services; thus, their program reviews may be biased towards their preferred way of implementing security. Indeed, last year, OMB learned that some security service providers were also contracted by the same agency to perform annual GISRA program reviews. Even the perception of a conflict of interest should be avoided when evaluating the security of an agency network.

The Federal government will explore whether private sector security service providers to the Federal government should be certified as meeting certain minimum capabilities including the extent to which they are adequately independent. The national security community has begun such certifications for security service providers working in that sensitive



environment and lessons learned from their experience will be applied in considering the cost effectiveness of this approach for other areas of the Federal government.

Among the possible elements of such an approach could be limiting contract awards to service providers that meet specific published criteria that address both the level of security expertise (including a thorough understanding of all government requirements) and their relative independence. To ensure independence, agencies could be prohibited from employing their existing (or recent past) security services contractors as their security program reviewer.

None of the foregoing should be viewed as diminishing the role of agency Inspectors General under GISRA. OMB continues to see the IGs as a linchpin to agency security performance improvement. In fact, there are direct benefits to the IGs from implementing this plan—they would

have an additional source of independent and expert information upon which they could also rely. (See recommendation R3-2.)

Overarching Reviews by the Board's Executive Branch Information Systems Security Committee

In addition to the efforts described earlier, the OMB-chaired Committee is reviewing a number of security issues that will promote greater benefits for securing agency business operations. To view the impact and effects of security policies on agency programs and business operations, this Committee includes officials from across a number of communities within the Federal government, including Chief Information Officers, Chief Financial Officers, Inspectors General, Procurement Executives, small agencies, operational program officials (business lines), human resources officials, and budget officials.

Among the Committee's current and planned activities are a gap analysis of current policies and processes, an evaluation of the viability of a governmentwide common methodology for grading risks, and a review of the desirability of developing uniform security practices or benchmarks for similar operations, assets, and systems. The latter two efforts reflect our "build once, use many" approach.

Gap Analysis of Current Policies and Processes

This review is addressing whether there are gaps in the coverage of current IT security policies, standards, and guidance for non-national security applications: Do they meet the needs of the departments and agencies with respect to the level of detail and coverage and adequately assist agencies improving security performance? The Committee is also examining whether existing policy development processes are efficient, effective, consider input from all relevant agencies and organizations, and produce results in a timely manner. Where improvement is needed the Committee is providing appropriate recommendations.

Grading Risks

This review is examining the current risk assessment practices of agencies and other organizations and will determine whether a uniform scheme under which all agencies grade risks is viable and desirable. The group has begun assessing whether a common methodology across the government enterprise (e.g., including specific metrics for identifying high, medium and basic risk exposures) would reduce complexity, simplify the use of risk-based security controls, and facilitate interoperability and information sharing across agencies.

In reviewing this issue, the Committee is proving or disproving several assumptions. First, all agency operations and assets require some level of security. Second, effective security demands an understanding of the acceptable level of risk. Third, the business requirements to share information within and across agencies, with industry, and with the public (especially in light of the September 11 terrorist attacks) has increased, and is complicated by differing approaches to grading risk. Fourth, a uniform risk-grading process will assist agencies in applying corresponding security controls. Fifth, a uniform risk-grading process will assist developing corresponding security requirements.

Uniform Security Practices or Benchmarks for Similar Operations, Assets, and Systems

The Committee will examine the viability of developing, and the potential benefits derived from, uniform security practices that apply to high, medium, and basic risk applications as determined in the grading risk activity described above. The group will explore whether implementing, maintaining, and monitoring security for operations that are similar across the departments and agencies will reduce costs and improve the security of such similar operations.

Several assumptions will also be tested in this area. First, many agency programs and IT operations are essentially the same (e.g., e-mail and web servers, financial systems, general support systems or networks) and so too are the associated security requirements. Second, uniform security practices that consolidate in one place all applicable security policies and technical guidance would simplify and reduce costs for achieving the adequate level of security for similar activities. Third, uniform security practices are viable once uniform risk grading is in place.

Cross-government Steps

One of the goals for many of these efforts is to unify and simplify security programs and processes and build security consistency across the government. This "build once, use many" approach for governmentwide security is consistent with the approach used for E-Gov initiatives and OMB's guidance to the agencies for preparing their FY 2004 budget requests. That guidance states that OMB "will give priority consideration to IT investments that leverage technology purchases across multiple entities." For more on OMB's FY 2004 budget guidance, see **www.whitehouse.gov/omb/circulars/a11/01toc.html**.

INFORMATION INTEGRATION AND INFORMATION TECHNOLOGY FOR HOMELAND SECURITY

A key goal to protect our nation's infrastructure is to ensure that there is a national environment—addressing people, process, and technology—that enables the integration of essential information for combating terrorism among Federal, State, local, and private sector entities. We must put in place mechanisms that provide the right information to the right people all the time. With the use of information technology, homeland security officials throughout the United States will have complete and common awareness of threats and vulnerabilities, as well as knowledge of the personnel and resources available to mitigate those threats. Officials will receive the information they need from all levels of government and the private sector so that they can anticipate threats and respond rapidly and effectively. This information integration will better enable officials to protect the physical and cyber infrastructure, secure our country's borders, prevent biological or chemical attacks, and provide an effective first response to a terrorist or natural disaster incident.

Major Strategic Goals

- Create collaborative partnerships with State and local government and the private sector
- Ensure adoption of leading-edge information technologies as offensive weapons in the prevention and detection of terrorism
- Drive national and international information integration and information delivery standards
- Develop innovative service delivery models and business models that enable government to use information held outside the government arena

Immediate Objectives

- Lead the integration of information essential to homeland security across Federal agencies (horizontal integration)
- Drive the integration of information essential to homeland security among and between Federal, State, and local government, and the private sector (vertical integration)
- Guide the enablement of the *National Strategy for Homeland Security* through appropriate use of information technology capabilities, products, and services

Major Risks to be Addressed

- Maintaining privacy while enhancing security
- Aligning policy and laws with desired outcomes
- Leveraging cultural beliefs and diversity to achieve collaborative change
- Consolidating redundant or duplicative efforts
- Overcoming political and cultural barriers
- Ensuring appropriate security measures for new technology

To guide information integration, the President proposed the Information Integration Program Office (IIPO) within the Critical Infrastructure Assurance Office in the Department of Commerce. If created, this office would migrate to the proposed Department of Homeland Security. The office is intended to coordinate the sharing of essential information nationwide. The most important function of this office would be to design and help implement a national enterprise architecture to guide investment in and use of information technology. Such an architecture would define the information integration requirements needed to detect, prevent, monitor, and respond to terrorist threats and incidents within the nation and around the world, while improving both the time of response and the quality of decisions.

Major Efforts in a Proposed Information Integration Strategy

- Development of a business-driven Homeland Security Enterprise Architecture
- Implementation of a National Homeland Security Portal (World Wide Web site)
- Consolidation of Federal "Watch-out" lists
- Multi-State Sharing of Law Enforcement Information
- Establishment of a digital National Homeland Security Information clearing-house
- Application of digital Intelligent Agents to the prevention and detection of terrorism

AGENDA

LEVEL 3: CRITICAL SECTORS – The Federal Government

RECOMMENDATIONS

Specific actions that government and nongovernment entities can take to promote cybersecurity.

R3-1 In order to enhance the procurement of more secure IT products, the Federal government, by 4Q FY03, will complete a comprehensive program performance review of the National Information Assurance Program (NIAP) to determine the extent to which NIAP is cost effective and targets a clearly identified security gap; whether it has defined goals to close the gap; whether it is achieving those goals; and the extent to which program improvements, streamlining, or expansion are appropriate and cost effective.

R3-2 The Federal government, by 3Q FY03, will assess whether private sector security service providers to the Federal government should be certified as meeting certain minimum capabilities.

R3-3 The Federal government, by 3Q FY03, using the E-Government model, will explore the benefits (including reducing resource pressures on small agencies) of greater cross-government acquisition, operation, and maintenance of security tools and services.

R3-4 Through the ongoing E-Authentication initiative, the Federal government, by 2Q FY03, will explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms to further promote consistency and interoperability.

R3-5 Federal departments should continue to expand the use of automated, enterprisewide security assessment and security policy enforcement tools and actively deploy threat management tools to preempt attacks. By 2Q FY03, the Federal government will determine whether specific actions are necessary (e.g., through the policy or budget processes) to promote the greater use of these tools.

R3-6 The Federal government will continue to assess the technical viability and cost effectiveness of various options that provide for the continuity of operations during service outages, such as VPNs, "private line" networks, and others.

R3-7 The Federal government should lead in the adoption of secure network protocols. The Federal government will review new secure network protocols as they are published to determine whether they fill a security gap and whether their adoption would have a cost-effective impact on the operations and security of the Federal government.

R3-8 By the end of 2Q FY03, the Federal government will consider the cost effectiveness of a scenario-based security and contingency preparedness exercise for a selected cross-government business process. Should such an exercise take place any security weaknesses shall be included as part of agencies' GISRA corrective action plans.

R3-9 OMB, in conjunction with the CIO council,will determine on a case by case basis whether to employ a lead agency concept for governmentwide security measures. The alternatives will generally include GSA, NIST, the proposed Department of Homeland Security, and the Department of Defense.

PROGRAMS

Existing efforts in cybersecurity.

P3-1 National Security Agency **www.nsa.gov/isso/index.html**

P3-2 National Infrastructure Assurance Partnership **www.niap.nist.gov/**

P3-3 OMB security program/budget process /GISRA reporting **www.whitehouse.gov/omb/inforeg/infopoltech.html**

P3-4 E-Government initiative **www.egov.gov/**

P3-5 Enterprise architecture Project Matrix **www.ciao.gov/Federal/**

P3-6 NIST Computer Security Resource Center **www.csrc.nist.gov/**

P3-7 Federal CIO Council **www.cio.gov**

P3-8 The General Services Administration's PKI bridge and Federal Telecommunications System security levels **www.gsa.gov**, Federal Computer Incident Response Center **www.fedcirc.gov**

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D3-1 Should Federal agencies be required to comply with a maximum time limit for the implementation of patches for known vulnerabilities?

D3-2 Should the CIAO or CISO be different than the CIO?

D3-3 How should civilian agencies expand use of PKIs for specific situations?

LEVEL 3: STATE AND LOCAL GOVERNMENTS

State and local governments have set strategic goals for achieving and maintaining the ability to protect critical information infrastructures from natural events and intentional acts that would significantly diminish State and local governments capacity to maintain order and to deliver essential public services.

Issues and Challenges

States provide services that make up the "public safety net" for millions of Americans and their families. Services include essential social support activities as well as critical public safety functions, such as law enforcement and emergency response services. States also own and operate critical infrastructure systems, such as electric power and transmission, transportation, and water systems. They play a catalytic role in bringing together the different stakeholders that deliver critical services within their State to prepare for, respond to, manage, and recover from a crisis. Delivering critical services unique to their roles and responsibilities within our Federalist system makes State government a critical infrastructure sector in its own right.

Many of these critical functions carried out by States are inexorably tied to IT—including making payments to welfare recipients, supporting law enforcement with electronic access to criminal records, and operating State-owned utility and transportation services. Preventing cyber attacks and responding quickly when they do occur, ensures that these 24/7 systems remain available and in place to provide important services that the public needs and expects.

Information technology systems have the potential for bringing unprecedented efficiency and responsiveness from State governments for their residents. Citizen confidence in the integrity of these systems and the data collected and maintained by them is essential for expanded use and capture of these potential benefits.

Discussion of Strategy

With an increasing dependence on integrated systems, State, local, and Federal agencies have to collectively combat cyber attacks. Sharing information to protect systems is an important foundation for ensuring government continuity. States have adopted several mechanisms that assist in sharing information on cyber attacks and in reporting incidents. These mechanisms are continually being modified and improved as new policy emerges and as technological solutions become available. In addition, States are exploring options for improving information sharing both internally and externally. These options include enacting legislation that provides additional funding and training for cybersecurity and forming partnerships across State, local, and Federal governments to manage cyber threats.

Some mechanisms that many States are using to address cyberspace security include:

- *Governance Structure.* Many States have an IT security governance structure that guides and enacts cybersecurity policy for the State. Functions may include making policy recommendations to the Governor or establishing a restoration priority list of agencies if multiple agencies are disabled concurrently. In many cases, the cybersecurity board includes all branches of government and affected agencies. Additionally, some States are including local governments in the governance structure, recognizing that local and State systems may be interconnected.
- *Establishment of the Roles of the State Chief Information Officer (CIO) and Chief Information Security Officer (CISO).* CIOs and CISOs oversee security policy and the implementation and maintenance of critical information systems.
- *State Homeland Security Initiatives.* Homeland Security Directors recognize that the States' cyber systems are at high risk for terrorist threats. With this in mind, States are shoring up network infrastructure and implementing authentication and authorization processes for State information systems. State policymakers and technologists are making outreach efforts to the public to educate them on how to protect their own information systems at home.

Gap Analysis

States representative groups have identified additional mechanisms needed to foster intergovernmental and industry partnerships:

- **Create a State CIO advisory group to the President's Critical Infrastructure Protection Board.**
- **Initiate an intergovernmental, cross-disciplinary architecture design guidance effort to support national information sharing.**
- **Increase information sharing efforts such as the Interstate ISAC.**
- **Initiate an ongoing intergovernmental effort to develop and deliver cybersecurity tools and training to State and local governments, in cooperation with NIST.**
- **Implement a concerted outreach effort to both citizens and businesses in regions where access to cybersecurity knowledge and tools is limited.**
- **Assure the inclusion of local government representation on State cybersecurity boards so that local interests and needs are represented.**
- **Leverage learning from private industry security providers on best practices, trends, lessons learned, and new technology.**
- **Find ways to bridge the information "stovepipes" at all levels of government.**
- **Address States information sharing concerns.**

Law Enforcement

State and local governments play an important role in the emergency law enforcement sector. Emergency Law Enforcement Services (ELES), as a critical infrastructure sector, is included within the emergency services sector. The continued operation of the ELES sector during a time of crisis is essential to the rule of law, the protection of the general welfare, the preservation of civil liberties and privacy rights, and consequence management.

More than 18,000 Federal, State, and local agencies comprise the ELES sector. Responses from more than 1,500 of these agencies to a sector-commissioned information systems vulnerability survey reveal that these organizations have become increasingly reliant on information and communications systems to perform their critical missions. The threat against such systems continues to grow. Sector agencies also depend on other critical infrastructures, such as energy and telecommunications, which are also vulnerable to both cyber and physical disruption.

This ELES sector critical infrastructure protection plan presents the sector's initial strategy for ensuring its continuing ability to perform critical emergency law enforcement functions. The plan represents the combined efforts of the National Infrastructure Protection Center (NIPC), the designated lead agency for the ELES sector, and the ELES Forum, a group of senior law enforcement executives from State, local, and non-FBI Federal agencies. The Forum was created to support the development of the ELES plan, to be national advocates for emergency law enforcement issues, and to conduct liaison activities with the ELES community.

The plan presents the sector's framework for identifying its most critical assets, assessing their vulnerability to attack, and developing remediation and mitigation plans. The plan also provides information on the National Infrastructure Protection Center's (NIPC) threat alert and notification system and on various infrastructure and information security-related training programs. A companion *Guide for State and Local Law Enforcement Agencies* provides tools that sector agencies can use when implementing the activities suggested in the plan.

The guide serves as the sector baseline infrastructure protection education and awareness program document. Each law enforcement agency operates independently and is responsible for its own critical infrastructure protection. Therefore, the success of any sectorwide program depends on the voluntary efforts of each of these organizations to undertake the activities suggested in the plan. At the national level, the ELES sector leadership will continue to serve as the sector representative in cross-sector planning and implementation activities.

AGENDA
LEVEL 3: CRITICAL SECTORS — State and Local Governments

RECOMMENDATIONS

*Specific actions that government and nongovernment entities can take to promote cybersecurity.**

R3-10 State and local governments should consider establishing IT security programs for their departments and agencies, including awareness, audits, and standards. State, county, and city associations should consider providing assistance, materials, and model programs.

R3-11 State and local governments should consider participating in the established information sharing and analysis centers (ISACs) with similar governments.

R3-12 State and local governments should consider expanding training programs in computer crime for law enforcement officials, including judges, prosecutors, and police. The Federal government could assist in coordinating such training and explore whether funding assistance is feasible.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

PROGRAMS

Existing efforts in cybersecurity.

P3-9 The National Association of State Chief Information Security Officers **www.nascio.org/**. NASCIO published a report entitled, "*Public-Sector Information Security: A call to Action for Public Sector CIOs*."

P3-10 The National Governors Association **www.nga.org/**.

P3-11 The National League of Cities **www.nlc.org/nlc_org/site/**.

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D3-4 How can Federal, State, and local governments enhance coordination and crisis management for cybersecurity?

D3-5 What special legal or policy challenges might States face in developing an interstate ISAC?

LEVEL 3: HIGHER EDUCATION

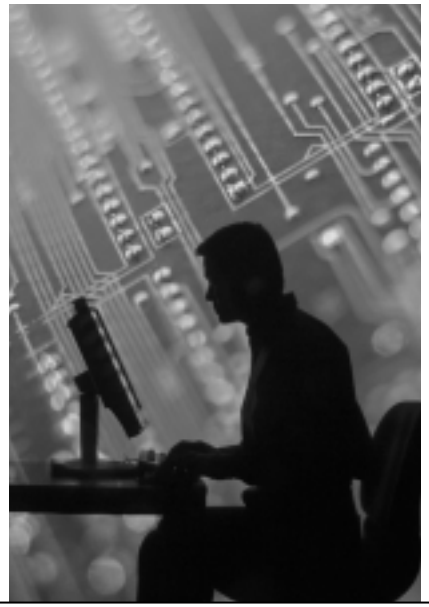
Institutions of Higher Education (IHEs)—universities, four-year colleges, community colleges—in the United States have set goals to adopt and implement a level of information system and network security to protect sensitive information, and to prevent its systems from being used for attacks on others. To achieve that goal, IHEs have identified the following framework for action:

- make IT security a priority in higher education;
- revise institutional security policy and improve the use of existing security tools;
- improve security for future research and education networks;
- improve collaboration between higher education, industry, and government; and,
- integrate work in higher education with the national effort to strengthen critical infrastructure.

Issues and Challenges

As recent experience has shown, many insecure computer systems traceable to the campus networks of higher education have been collectively exploited by hackers as a platform from which to launch denial-of-service attacks and other threats to unrelated systems on the Internet. Such attacks harm not only the targeted systems, but also the owners of those systems and those who desire to use their services.

IHEs are subject to such exploitation for two reasons: (1) they possess vast amounts of computing power; and, (2) they allow relatively open access to those resources. The computing power owned by IHEs is extensive, covering over 3,000 schools, many with research and significant central computing facilities. Research and education institutions represent approximately 15 percent of all the advertised domains on the Internet. To the extent that IHEs systems can be penetrated and "hijacked" for the purpose of launching cyber attacks against third-party systems (the "zombie" phenomenon). They unwittingly place other sectors at risk.



IHEs also hold much information for and about students and staff that is either private or confidential. Sensitive information (such as patient information and medical records, student information, personnel records, and sensitive research data) is maintained within university system databases. Such information must be protected and kept private. Moreover, vulnerabilities in one trusted network create vulnerabilities in many networks. Accordingly, IHEs must consider the broader implications of their cybersecurity.

While IHEs must maintain privacy of information and prevent malicious use of their systems, they also must provide an environment in which students can learn, and research can be conducted efficiently. These two needs do not necessarily conflict, but must both be considered as IHEs identify their strategy for securing their part of cyberspace.

Discussion of Strategy

IHEs' Action Plan–Steps Completed and Those to be Taken

The higher education community, collectively, has been actively engaged in efforts to organize its members and coordinate action to enhance cybersecurity on America's campuses. Most notably, through EDUCAUSE, the community has raised the issue of the National Strategy's development with top leaders of higher education, including the American Council on Education and the Higher Education IT Alliance. Significantly, through this effort, top university presidents have adopted a 5-point Framework for Action that commits them to give IT security high priority and to adopt the policies and measures necessary to realize greater system security.

Task Force on Computer and Network Security

In July 2000, EDUCAUSE and Internet2 established the Task Force on Computer and Network Security (www.educause.edu/security). The Task Force represents just one effort by the higher education community to take an active role in identifying vulnerabilities and the flaws that create them, and developing and implementing solutions on their campuses. By doing so, the Task Force seeks to reduce significantly the direct threat that higher education systems confront and the indirect threat that exists to others.

The Task Force works with partner associations and well-known security specialists to develop short-term actions and intermediate and long-term projects to address these problems in higher education. Among its recommendations are the following:

- **Near Term: All campus network and technology leaders should find and fix the ten most common security holes on their campus by adopting the advice and methodology of the SANS Institute.**
- **Intermediate: The Task Force will seek out and publicize improved procedures and policies to find, fix, and prevent security flaws on campus, as well as means to measure and compare progress.**
- **Long Term: Research next-generation security issues that will help to engineer new services in a secure fashion and provide systemic remedies to some of today's problems (e.g., Internet2 PKI labs and the Higher Education PKI joint project of Internet2).**

America's colleges and universities have also adopted an agenda of further activities to address the challenges of IT security and information assurance. For example, along with the National Science Foundation (NSF), EDUCAUSE is organizing a series of four workshops.

The first of these workshops will bring together leaders in higher education to establish principles for a security strategy that can also support higher education's mission. Representatives from the university research community will also meet to identify the problems, issues, and solutions associated with securing faculty and student research activities.

RECOMMENDATIONS

*Specific actions that government and nongovernment entities can take to promote cybersecurity.**

R3-13 Each college and university should consider establishing a point-of-contact, reachable at all times, to Internet service providers (ISPs) and law enforcement officials in the event that the school's IT systems are discovered to be launching cyber attacks.

R3-14 Colleges and universities should consider establishing together: (a) one or more information sharing and analysis centers (ISACs) to deal with cyber attacks and vulnerabilities; (b) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (c) one or more set of best practices for IT security; and, (d) model user awareness programs and materials.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

PROGRAMS

Existing efforts in cybersecurity.

P3-12 EDUCAUSE and Internet2 established the Task Force on Computer and Network Security **www.educause.edu/security**.

P3-13 EDUCAUSE Workshop series with National Science Foundation.

P3-14 EDUCAUSE Outreach and awareness program to leaders and associations in higher education.

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D3-6 What are the merits of adopting a model set of authorities for IHE CIOs, the academic institution, and the nation? (An example of such authorization can be found at **www.indiana.edu**.

D3-7 Should consideration be given to tying State or Federal funding to IHEs to compliance with certain cybersecurity benchmarks?

D3-8 Should an ISAC for the higher education community be established? If so, how? What other steps could be taken to improve methods of information sharing among IHEs at all levels?

D3-9 Should IHEs adopt the NIST Information Technology Security Assessment Framework ("NIST 3") as a standard for information system security compliance?

LEVEL 3: PRIVATE SECTOR

The private sector plays a central role in securing cyberspace because it owns and operates the vast majority of the nation's infrastructures and the cyber systems on which they depend. Several critical infrastructure sectors have undertaken substantial efforts to coordinate the development of infrastructure protection plans. During these processes, sectors identified for themselves the strategic goal of securing the critical information infrastructures that they own and operate. The sector plans have provided an invaluable insight into the scale, scope and character of the challenges facing the United States.

CRITICAL INFRASTRUCTURE SECTORS CONTRIBUTORS	SECTOR COORDINATORS/ CONTRIBUTORS
Banking & Finance	American Banking Association, Securities Industry Association, BITS, the Financial Services Information Sharing and Analysis Center board, and the Independent Community Bankers of America
Electric	North American Electric Reliability Council
Oil & Natural Gas	National Petroleum Council
Water	The Association of Metropolitan Water Agencies, with support from the American Water Works Association, the National Association of Water Companies, and the AWWA Research Foundation.
Transportation (Rail)	Association of American Railroads
Information & Communications	Cellular Telecommunications and Internet Association, Information Technology Association of America, Telecommunications Industry Association, and United States Telecom Association
Chemicals	Chemicals Sector Cyber-Security Information Sharing Forum
These Plans can be found at **www.pcis.org** or **www.ciao.gov**	

The sector plans provide a specific overview of the challenges facing the different industry sectors and the steps they are taking to meet these challenges. Moreover, the industry planning efforts advance cyberspace security by creating a process where sectors can begin to identify their unique security issues for resolution; and the planning efforts also facilitate the prioritization of infrastructure protection issues which may need to be addressed through a public-private partnership.

Issues and Challenges

Cyberspace security is a shared responsibility. No single industry is responsible for its security and no government entity can protect it. At the request of the Bush Administration, American infrastructure sectors have undertaken an unprecedented effort to develop infrastructure protection plans that address cyber and physical security. The various sector strategies describe the actions that each industry sector is taking to assure its critical operations will not be disrupted or compromised by cyber attacks or physical incidents. The private sector plans are intended to foster greater infrastructure security and complement Federal planning efforts. Together these plans lay a foundation for a truly national strategy.

The Partnership for Critical Infrastructure Security (PCIS), a nonprofit organization of critical infrastructure companies, was formed to address the complex set of issues related to infrastructure protection. The Partnership is a collaborative effort of over 60 member companies and associations and 13 Federal government agencies in 8 critical infrastructure sectors.

The mission of the Partnership is to coordinate cross-sector initiatives and complement public-private efforts to promote the assurance of reliable provisions of critical infrastructure services in the face of emerging risks to economic and national security. Accordingly, the Partnership focuses on issues that the sectors have in common.

The PCIS and the CIAO have reviewed the sector plans listed in the table to the left and summarized the common issues and concerns identified by the sectors. The PCIS/CIAO analysis is available on the PCIS web site (**www.pcis.org**).

The companies which own and operate the critical infrastructures share six common challenges which must be addressed to enhance infrastructure protection efforts. These challenges include a wide range of issues such as infrastructure interdependencies, research and development, education and workforce development, information sharing and analysis, public policy issues, and international challenges.

Infrastructure Interdependencies

During the past decade American infrastructures have integrated information technology (IT) and cyberspace into almost every aspect of their operations.

The rapid integration of IT has yielded profound efficiencies, promoted innovation, and increased service reliability. Once distinct infrastructures, which were isolated by closed proprietary systems, are now tightly integrated with one another. This integration has created many new and complex interdependencies. In many cases, these interdependencies are not well understood.

Industry is working jointly with government to develop an understanding of the complex connections between organizations in a sector, among sectors, and with the government. In particular, there is concern about cascading effects from one critical infrastructure sector to others. Developing tools and methodologies to perform cyber risk modeling is essential to both eliminating vulnerabilities and fostering the appropriate risk-transfer mechanisms. Efforts are beginning in the insurance and reinsurance communities to support these endeavors (To read more about insurance sector efforts see **www.pcis.org** or **www.ciao.gov**.)

Research and Development

Cybersecurity research and development (R&D) is another challenge sectors are addressing. Within sectors there are specific technical R&D challenges unique to each industry. These unique challenges are explained by each of the industries and can be found in their respective sector plans. Other R&D challenges are much more cross cutting and include issues such as vulnerability assessments guidelines and best practices for contingency planning.

Education and Workforce Development

Improving cybersecurity in the infrastructures depends on people. Senior management, technical personnel, and the employees in general all play important roles. As senior management develops an increased awareness of cybersecurity risks, they can set policy that promotes infrastructure security. However, in order to implement the management policy infrastructures need to be able to hire well-trained technical people. Accessing the right technical people depends largely on educating and training. Finally, the security of sector depends on the average employee complying with the enterprise computer security policies. These three factors play a crucial role in improving cybersecurity in all of the infrastructures.

Information Sharing and Analysis

Industry and government are working together to improve information sharing and analysis efforts. Currently, the independent critical sectors are establishing mechanisms to share security information among their constituencies. Moreover, several continue to develop additional means through which they can share threat, vulnerability, countermeasure, and best practices information beyond their individual industries, across sectors, and with government.

Public Policy and Legal Challenges

During their own planning efforts, sectors have identified a variety of public policy and in some instance legal challenges that may impede their efforts in infrastructure protection and cybersecurity. The PCIS provides a more detailed discussion of private sector concerns in its analysis.

International Issues

Cyberspace security is an international challenge that is not bounded by any physical national boundary. The operations of multiple sectors cross international boundaries. As a result, global infrastructure sectors are initiating efforts to promote the availability, integrity, and reliability of their common information systems.

Discussion of Strategy

Fostering a Stronger Public-Private Partnership

A successful public-private partnership requires trust. Trust cannot be legislated or mandated. Rather it is built over a period of time. The Federal government will continue to explore a variety of efforts to enhance and expand its partnership with the critical infrastructure sectors including improving coordination with the industry-led efforts for information sharing about cybersecurity.

Information Sharing and Analysis Centers

Information sharing and analysis centers (ISACs) play an increasingly critical role in homeland and cybersecurity. An ISAC is typically an industry-led mechanism for gathering, analyzing, sanitizing, and disseminating sector-specific security information. ISACs are designed by the various sectors to meet their respective needs and are financed by their members. (The telecommunications ISAC located at the National Communications System is funded by the government.) ISACs work closely with the Federal government through the National Infrastructure Protection Center (NIPC) to exchange data about threats and vulnerabilities; and through the CIAO for coordination and planning efforts. The President's proposed Department of Homeland Security would combine the NIPC, CIAO, and other Federal cyber centers to streamline information sharing and enhance infrastructure analysis.

Establishing an ISAC requires tremendous cooperation within the sector and the establishment of a clear business model. While each ISAC is different, new and established ISACs must overcome a variety of challenges. These challenges include improving business participation in the ISAC; enhancing the timeliness and effectiveness of threat information; and overcoming information sharing challenges. Several of the critical infrastructure sectors have either created or are now planning the development of their industry-specific ISACs.

ISACs are developing and maturing across the various sectors including telecommunications, financial services, information technology, water, transportation, electric power, oil and gas, chemicals, food, State government, and more. Because they draw on the technical expertise of a given sector, the ISACs can facilitate the management and resolution of cybersecurity incidents.

In order to respond to future challenges, ISACs may need to be linked to government warning-and-analysis centers. As a result there are efforts underway to explore the benefits of linking ISACs to each other and to critical government centers. This could facilitate the timely flow of critical infrastructure information and enhance crisis management efforts.

As ISACs mature, so too will the national ability to respond and manage cyber incidents and attacks. In addition, the Federal government and ISACs could explore the challenges associated with infrastructure analysis and identify the methodologies and tools that might be needed to visualize and understand vulnerabilities, attacks, and remediation.

If requested, the Federal government could, through the ISACs, provide technical assistance to develop contingency and crisis management plans for critical infrastructures. In addition, Federal, State, and local governments could examine ways to coordinate response and recovery activities for significant disruptions that require actions beyond the capabilities or purview of individual companies.

AGENDA
LEVEL 3: CRITICAL SECTORS — Private Sectors

RECOMMENDATIONS

*Specific actions that government and nongovernment entities can take to promote cybersecurity.**

R3-15 Each sector group should consider establishing an information sharing and analysis center (ISAC) that should cooperate with other ISACs. The Federal government will explore linking the ISACs with appropriate cybersecurity warning-and-analysis centers upon request, and could facilitate the provision of information related to critical infrastructure protection when necessary.

R3-16 Each sector group should consider conducting a technology and R&D gap analysis, in conjunction with OSTP efforts to prioritize Federal cybersecurity research to address identified gaps. The sectors and OSTP should coordinate on the conduct of such research.

R3-17 Each critical infrastructure sector group should consider developing best practices for cybersecurity and, where appropriate, guidelines for the procurement of secure IT products and services.

R3-18 Each sector group should consider working together on sector specific information security awareness campaigns.

R3-19 Each sector should consider establishing mutual assistance programs for cybersecurity emergencies. The Department of Justice and the Federal Trade Commission should work with the sectors in addressing any barriers to such cooperation.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

PROGRAMS

Existing efforts in cybersecurity.

P3-15 The Partnership for Critical Infrastructure Security, **www.pcis.org.**

LEVEL 4: NATIONAL PRIORITIES

The overall strategic goal in implementing the national priorities is establishing foundations for securing cyberspace. The three foundations central to cybersecurity include the following:

- securing shared systems;
- fostering a reinforcing economic and social framework; and,
- developing national plans and policy.

Establishing these foundations will require a clearly defined set of efforts. These efforts are national in scope and underpin the approaches that are being taken by constituents at each level of the Strategy. For example, additional research to make current infrastructure more secure or to invent new methods for securing information will benefit everyone, from the home user, to industry, to government. This section summarizes the Strategy for what the nation is doing in seventeen areas critical to cybersecurity.

The following pages lay out the major issues and strategic steps that the nation should take in each of these areas. The issues are national in scope, and success in addressing these areas will require efforts at all audience levels.

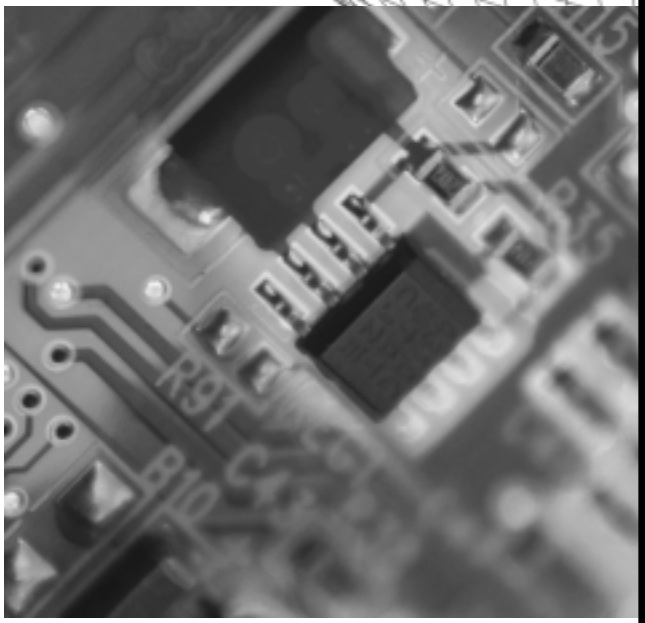
Securing Shared Systems

Making basic elements of cyberspace more secure and reliable will benefit users at all levels. Ideally, the nation can find ways to make computing, and especially operating systems, more secure, to make networks that connect them secure, and to ensure that new additions are equally secure. One improvement in security of common systems equates to millions of improvements for individual users. Where vulnerabilities persist, efficient means must exist to correct them. The strategic goal of securing shared systems is to greatly enhance individual security by securing the systems that affect users at all levels.

Securing the Mechanisms of the Internet

When the Internet was first developed, its creators did not imagine all of the commercial, national security, and emergency preparedness purposes it would eventually acquire. They did not realize how quickly and how much the Internet would grow over time. Thus, when the Internet was built, features like security, which are vital today, were not part of its foundation.

Key foundations for cybersecurity	Areas of effort to develop foundation
Securing shared systems	Securing the mechanisms of the Internet Supervisory control and data acquisition systems Research Highly secure and trustworthy computing Securing emerging systems Vulnerability remediation
Fostering a reinforcing economic and social framework	Awareness Training and education Certification Information sharing Cybercrime Market forces Privacy
Developing national plans and policy	Analysis and warning Continuity of operations, reconstitution, and recovery National security Interdependency and physical security



The Internet was built to be redundant and though security has been added on over time, security was never incorporated as a fundamental feature and gaps remain in its implementation. In addition, the methods and rules that the Internet uses for communication, and the devices that support the transfer of information, were not designed to support the growing volume of data that flows through the Internet.

The development and implementation of the mechanisms for securing the Internet are responsibilities shared by its owners, operators and users. This effort cannot be accomplished by any one entity or group. Rather, securing the mechanisms of the Internet will require a partnership. Private industry is leading the effort to ensure that the core functions of the Internet develop in a secure manner and, as appropriate, the Federal government will continue to support these efforts.

The strategic goal for securing the mechanisms of the Internet is to foster the development of secure and robust mechanisms that will enable the Internet to support the nation's needs now and in the future. Securing the mechanisms of the Internet includes:

- improving the security and resilience of key Internet protocols;
- increasing router security;
- adopting best security standards, practices, and criteria—"code of good conduct"; and,
- establishing a public-private partnership to identify and address fundamental technology needs for the Internet.

Supervisory Control and Data Acquisition (SCADA) Systems

Many industries in America have radically transformed the way they control and monitor equipment over the last 20 years. In the past, workers controlled many systems manually, which required traveling to the equipment site. Today, many of these same systems are controlled remotely over cyber networks. In many cases, this information is using the Internet to travel from one point to the other.

The ability of companies to make these systems secure is limited in two ways. First, adding security requires investment that companies may not be willing to make. Second, technological limitations exist. SCADA systems are often small and self contained. They may have limited power supplies. Moreover, they operate in real time. This means that security measures that might slow down system performance, or require additional power to operate, could be difficult to implement.

The strategic goal is to empower Digital Control System (DCS)/Supervisory Control and Data Acquisition (SCADA) users to protect their cyberspace and prevent it from being used to disrupt the nation's critical infrastructure. The following will help to achieve this goal:

- raising the level of awareness among industry vendors and users to the vulnerabilities in DCS/SCADA systems, and the consequences of exploitation of those vulnerabilities;
- developing and deploying training and certification programs on topics such as: basic data security, DCS/SCADA-oriented security, secure software, secure hardware;
- promoting standards efforts, security policy creation, and means of enforcement of these standards and security policies;
- providing a test bed environment to study security problems and proposed solutions;
- performing research and development in the areas of extremely low latency link encryptors/authenticators, key management, and network status/state-of-health monitoring; and,
- developing a government/industry partnership to identify the most critical DCS/SCADA-related sites and to develop a plan for short-term cybersecurity improvements to those sites.

Research

As the nation's reliance on cyberspace continues to grow, Federal investment in research for the next generation of technologies to maintain and secure cyberspace must keep pace with an increasing number of vulnerabilities. Flexibility and nimbleness are important in ensuring that the research and development process can keep pace with the revolutionary technology environment in the years ahead. The proper balance between fiscal restraints and responsiveness to the vulnerabilities in the nation's critical infrastructures may require greater levels of funding in the future. The nation will prioritize and provide resources as necessary to advance the research to secure cyberspace.

A new generation of enabling technologies will serve to "modernize" the Internet for rapidly growing traffic volumes, expanded e-commerce, and the advanced applications that will be possible only when next-generation networks are widely available. As a result, national research efforts must be prioritized to support the transition of cyberspace into a secure, high-speed knowledge and communications infrastructure for the 21st century.

Vital research is required for this effort. For example, new technology must be developed that can create an encryption and authentication capability for digital control systems. The nation must prioritize its cyberspace security research efforts across all sectors and funding sources.

The strategic goal of the national cyberspace security R&D agenda is to coordinate the development of technologies to counter threats, reduce vulnerabilities, and foster a resilient, secure cyberspace for the future. This goal is accomplished by:

- developing an annual cyberspace security R&D agenda to meet near-, medium-, and long-term objectives;
- leading a vigorous program of Federal R&D in cybersecurity that rapidly identifies, develops, and facilitates the fielding of technologies and tools for countering threats and vulnerabilities;
- fostering a close partnership with the private sector, academia, and the international community to ensure that no key technologies are missed, and new security technologies are quickly adopted; and,
- ensuring Federal cybersecurity R&D funding in FY04 is consistent with the national R&D agenda priorities.

Highly Secure and Trustworthy Computing

One day in the future, working with a computer, the Internet or any other cyber system may become as dependable as turning on the lights or the water. It may become something that can be taken for granted and left in the background. Today, however, it is common to have computers crash and to have systems be unavailable for long periods of time. Data is often lost or recovered only with great difficulty. Systems become overloaded or fail because a component has gone bad.

The strategic goal is to ensure that future components of the cyber infrastructure are built to be inherently secure and dependable for their users. This goal is accomplished by:

- conducting additional research to develop highly secure and

reliable systems;

- fostering software development practices and quality assurance testing that produce and maintain secure and reliable products;
- developing improved capabilities for detecting malicious code in software; and,
- reshaping Federal purchasing standards to insist on security and adhere to them strictly.

Securing Emerging Systems

As new technologies are developed they introduce the potential for new security vulnerabilities. Wireless local area networks are an example of this. Though care was taken in developing these systems, their implementation in an operating environment has highlighted some of their weaknesses. Today, a person driving in a car around a city can log onto numerous networks without the knowledge of their owners. The intruder could steal information or launch attacks on those systems if he or she desires. With the addition of security mechanisms (such as password access requirements, address filtering, encryption, or using a virtual-private-network) these systems are much less susceptible to attack. Too often, however, such additions are not made due to complexity, cost, or time associated with setting them up. Intrusion is possible even when the manufacturer's security mechanisms are installed because the encryption can be broken. As new systems enter the market and become widespread, care must be taken to ensure that their security is adequate.

New technologies can produce unforeseen consequences for security. The emergence of optical computing and intelligent agents, as well as in the longer term, developments in areas such as nanotechnology and quantum computing, amongst others, could reshape cyberspace and its security. The nation must be at the leading edge in understanding these technologies and their implications for security.

The strategic goal is to address vulnerabilities that emerging technologies are introducing in cyberspace and determine how to eliminate, mitigate or manage the potential risk of these vulnerabilities. Achieving this goal is possible through efforts such as:

- improving the security of emerging technologies, such as wireless local area networks (WLANs), by increasing awareness and ease of use, evolving a new generation of secure wireless technologies, and addressing the security issues related to ad hoc networks and grid computing; and,
- examining, on a continuing basis, the security of emerging technologies.

Vulnerability Remediation

New vulnerabilities emerge daily as use of software reveals flaws that criminals can exploit for malicious activity. Currently, approximately 3,500 vulnerabilities are reported annually. Corrections are usually completed by the manufacturer in the form of a patch and made available for distribution to fix the flaws.

Many known flaws remain uncorrected for long periods of time. For example, the top ten known vulnerabilities may account for the majority of the reported incidents of cyber attacks. This happens for multiple reasons. Many system administrators may lack adequate training or may not have time to examine every new patch to see if it applies to their system. The software to be patched may affect a complex set of interconnected systems that take a long time to test before a patch can be installed with confidence. If the systems are critical, it may be difficult to shut them down to install the patch.

The strategic goal is to significantly improve the speed, coverage, and effectiveness of remediation in the near term by improving tools and practices, and in the longer term by reducing vulnerabilities at the source. This goal can be accomplished through the following strategic steps:

- identifying and promoting adoption of company and agency best practices for vulnerability remediation;
- creating a neutral clearinghouse to promote faster identification of the impact of patches on common applications, possibly including test results;
- researching and encouraging improved disclosures of the impact of patches to speed implementation;
- developing and implementing improved coding techniques and quality assurance criteria to reduce the number of vulnerabilities created; and,
- increasing the percentage of software that is shipped in a secure initial configuration.

Fostering a Reinforcing Economic and Social Framework

To enhance and maintain the security of cyber systems, the laws and customs of the society in which those systems exist must reinforce security in a sustainable way. Mechanisms that help reinforce security are laws addressing cybercrime, rules and bodies facilitating the sharing of information, and organizations training and educating a security workforce. Adherence to fundamental principles, such as recognition of the role of market forces and the importance and centrality of maintaining privacy, help sustain the other enforcing mechanisms. The Strategy aims to foster a social and economic framework that accepts and reinforces security in a natural and sustainable way.

Awareness

In many cases, solutions to cybersecurity issues exist, but the people that need them do not know they exist or do not know how or where to find them. In other cases, people may not even be aware of the need to make a network element secure. A small business, for example, may not realize that the configuration of its web server uses a default password that allows anyone to gain control of the system. Education and outreach play an important role in making users and operators of cyberspace sensitive to security needs. These activities are an important part of the solution for almost all of the issues discussed in this Strategy, from securing digital control systems in industry, to securing the cable modem at home.

The strategic goal for awareness is to stimulate actions to secure cyberspace by creating an understanding at all audience levels of both cybersecurity issues and solutions. This can be accomplished by doing the following:

- building upon and expanding existing efforts to direct the attention of key corporate decision makers (e.g., CEOs and members of boards of directors) to the business case for securing their companies information systems;
- implementing plans to focus key decision makers in State and local governments (e.g., governors, State legislatures, mayors, city managers, county commissioners/boards of supervisors) to support investment in information systems security measures and adopt enforceable management policies and practices;
- educating the general public of home users, students, children, and small businesses on basic cyberspace safety/security issues; and,
- elevating the exposure of cybersecurity issues and available resources by communicating through, and partnering with, local organizations, and primary and secondary schools.

Training and Education

To implement and maintain security, the nation needs a talented and innovative pool of citizens that are well trained. While the need for this pool has grown quickly with the expansion of the Internet and the pervasiveness of computers, networks, and other cyber devices, the investment in training has not kept pace. Universities are turning out fewer engineering graduates, and much of their resources are dedicated to other subjects, such as biology and life sciences. Though computer networks are widespread today, and the safety and security issues surrounding them are well known, few primary and secondary students are taught courses or modules on cybersecurity. This trend must be reversed if the United States is to lead the world with its cyber economy.

The strategic goals are: (1) to develop and sustain a well-trained, highly skilled, domestic corps of information technology (IT) security professionals sufficient for the nation's growing needs; and (2) to establish and maintain in the general population a basic proficiency in cybersecurity and cyber ethics. These objectives may be achieved through the following:

- promulgating guidelines, developed by State and local governments and private entities, covering cyber awareness, literacy, training, and education, including ethical conduct in cyberspace, tailored to each level of education;
- expanding current programs to increase the number of four-year colleges and universities with high-quality IT security programs and increasing the opportunities for skills training in IT security through non-degree programs, vocational schools, junior colleges, and technical institutes;
- creating a national cyberspace academy which would link Federal cybersecurity and computer forensics training programs;
- establishing clearly defined IT security career fields and subspecialties in the Federal government and each of the sectors of private industry; and,
- ensuring that opportunities exist for continuing education and advanced training in the workplace to maintain high skills standards and the capacity to innovate.

Certification

Related to education and training is the need for certification of qualified persons. Certification provides employers and consumers with greater information about the capabilities of potential employees or security consultants. Currently, some certifications for cybersecurity workers exist; however, they vary greatly in the requirements they impose. For example, some programs emphasize broad knowledge verified by an extensive multiple choice exam, while others verify in-depth practical knowledge on a particular cyber component. No one certification offers a level of assurance about a person's practical and academic qualifications, similar to those offered by the medical, legal, and accounting professions.

The strategic goal is to develop a nationally recognized standard for certification of information technology security professionals that could ensure consistent and competent assessment and maintenance of IT systems and networks. This may be accomplished by:

- enhancing existing programs and developing new capabilities, where necessary, to create a peer certification standard for IT security professionals similar to accounting, medical, and law certification processes. Certification could include advanced degrees and a nationwide standards exam, administered by a professional organization, to certify IT consultants and to serve as a standard for those hired by private companies;
- developing an accrediting body to verify that the various certification programs meet a minimum standard for System Administrator level and similar positions; and,
- requiring such certification before the Federal government hires certain levels of IT professionals and, over time, for current employees.

Information Sharing

The nation must be able to detect and analyze cyber incidents and attacks in a timely manner. The voluntary sharing of information about such incidents or attacks is vital to cybersecurity. Real or perceived legal obstacles make some companies hesitant to share information about cyber incidents with the government or with each other. First, some fear that shared data that is confidential, proprietary, or potentially embarrassing may become subject to public examination when shared with the government. Second, concerns about competitive advantage may impede information sharing between companies within an industry. Finally, in some cases, the mechanisms are simply not yet in place to allow efficient sharing of information.

The strategic goal is to increase the voluntary sharing of information about cybersecurity between public and private sector entities, as well as among private sector entities. This goal may be accomplished by:

- enhancing existing mechanisms for information sharing to ensure that they are sufficient and cover all necessary information sources; and,
- creating a legal and political environment for the sharing of critical information that removes uncertainty around how shared information might be used.

Cybercrime

Once incidents are detected, they must be addressed. A rapid response can stem the tide of an ongoing attack and lessen the harm that is ultimately caused. The nation currently has laws and mechanisms to ensure quick responses to large incidents. Response also includes analyzing and disseminating practical information to owners and users affected by the incident. This is followed, ideally, by investigation, arrest, and prosecution of the perpetrators, or, in the case of state-sponsored actions, by a diplomatic or military response. Unfortunately, some incidents are not reported, and, even when they are, cannot be responded to effectively by local authorities due to lack of training or experience. State and local law enforcement capabilities vary significantly.

The strategic goal is to prevent, deter, and significantly reduce cyber attacks by ensuring the identification of actual or attempted perpetrators followed by an appropriate government response, which in the case of cybercrime includes swift apprehension, and appropriately severe punishment. This can be accomplished by the following means:

- improving information sharing and investigative coordination within the Federal, State, and local law enforcement community working on critical infrastructure and cyberspace security matters, and with other agencies and the private sector;
- continuing to assess the adequacy of Federal sentencing guidelines penalties for cybercrime to ensure appropriate punishment for cyber offenses;
- empowering Federal, State, and local law enforcement by exploring means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of critical infrastructure incidents;
- developing better data about victims of cybercrime and intrusions; and,
- working internationally to ensure that appropriate tools are available to respond to cyber incidents.

Market Forces

Much of cyberspace has a history and tradition of private and unregulated operation. Private investment and innovation has made the Internet and, more generally, cyberspace the vital and robust infrastructure that it is today. As cyberspace has become such an important component of the nation's critical infrastructure, the need to make it secure, reliable, and resilient has become imperative. This need requires additional investment and resources from the owners and suppliers of elements of cyberspace.

The best way to ensure that the investment is made is for the market to demand it, rather than for government to require it. In some instances, the government may resort to policies that encourage private participation, such as awareness efforts on the importance of cybersecurity, voluntary standards and initiatives, funding and procurement of government systems, and public-private partnerships. Efforts should be made to create an environment where these forces can be effective. Cybersecurity regulation should not be considered unless there is an overriding need to protect the health, safety, and well-being of the American people.

The strategic goal is to minimize interference in the market while promoting and increasing cybersecurity. This goal may be accomplished by:

- leveraging corporate governance and industry standard setters to promote cybersecurity;
- working cooperatively with the insurance industry to facilitate the creation of risk-transfer mechanisms for cybersecurity;
- developing greater transparency of security preparedness, and promoting best practices, possibly through self-regulating organizations such as market exchanges; and,
- fostering innovative cybersecurity products and services through technology transfers to the private sector.

Privacy and Civil Liberties

The nation's Strategy must be consistent with the core values of its open and democratic society. Accordingly, Americans expect government and industry to respect their privacy and protect it from abuse. This respect for privacy is a source of our strength as a nation; accordingly, one of the most important reasons for ensuring the integrity, reliability, availability, and confidentiality of data in cyberspace is to protect the privacy and civil liberties of Americans when they use—or when their personal information resides on—cyber networks. To achieve this goal, the National Strategy incorporates privacy principles—not just in one section of the Strategy, but in all facets. The overriding aim is to reach toward solutions that both enhance security and protect privacy and civil liberties.

The strategic goal is to achieve security in cyberspace without infringing on individual privacy and civil liberties. This goal can be accomplished through the following steps:

- continuing government commitment to rigorous enforcement of existing laws protecting privacy and civil liberties;
- consulting regularly with privacy advocates, industry experts, and the public at large to ensure broad input into, and consideration of, privacy issues in implementing the National Strategy to achieve solutions that protect privacy while enhancing network and host security;
- expanding current annual GISRA audits to incorporate a privacy review for each Federal agency;
- encouraging industry to voluntarily incorporate appropriate privacy protections into their planning and products;
- ensuring that the Federal government leads by example in implementing strong privacy policies and practices in the agencies; and,
- educating end-users about privacy issues and policies, and encourage them to make informed choices about privacy.

Developing National Plans and Policy

The final category of national-level issues involves the nation's planning and policies for addressing organized efforts to attack the cyber infrastructure, and for situations in which the infrastructure fails, whether due to attack or a natural occurrence. The consequences of such a failure must be thoroughly understood. Because critical infrastructures are highly interconnected, these consequences can be complex and complicated to model. Once understood, the nation must have a plan to respond to major incidents efficiently and effectively. A discussion of four important aspects of the nation's policies and plans follows.

Analysis and Warning

The nation's ability to respond to cyber outages or attacks depends, first, on its ability to detect incidents early. Today, multiple organizations, both government and private, collect information about events and new vulnerabilities that occur on the Internet and connected networks and information systems. Organizations are also in place to disseminate this information to those who need it to help mitigate potential negative impacts. Some industry sectors have information sharing and analysis centers (ISACs) to spread early-incident information to all companies in that sector. ISACs and government share information on a two-way basis.

Despite progress being made in detection and information dissemination, some gaps remain. Internet service providers, (ISPs), and the nation as a whole, do not have a single collection and dissemination point for issuing warnings of incidents. There is no clearly defined, joint incident response procedure or team. Forward looking analysis capabilities are sparse and suffer from lack of information. Moreover, incident information is often source sensitive and may have national security implications.

The strategic goal is to detect incidents at their earliest inception; to respond to them efficiently; and, to the extent possible, predict them in advance. This goal can be accomplished by:

- exploring the development of a national cyberspace network operations center;
- improving government data analysis capabilities including increased use of data from agencies;
- encouraging expanded sharing and analysis of data by public-private entities; and,
- facilitating the improvement and expansion of incident response capabilities.

Continuity of Operations, Reconstitution and Recovery

The nation could benefit from an integrated public-private plan for responding to significant outages or disruptions in cyberspace. Many organizations have plans for how they will recover their cyber network and capabilities in the event of a major outage or catastrophe. However, there is no mechanism for coordinating such plans across the private and public sectors.

The strategic goal is to provide for a national plan for continuity of operations, recovery, and reconstitution of services during a widespread outage of information technology systems in one or more sectors. Accomplishing this goal is possible through public-private efforts that will:

- coordinate and regularly update the development of cybersecurity contingency plans, including a plan for recovering Internet functions
- determine what thresholds would warrant the implementation of cybersecurity contingency or Internet recovery plans; and,
- exercise such contingency and recovery plans on a regular basis.

National Security

The nation faces adversaries including foreign governments and terrorist groups that could launch cyber attacks of national security concern. In peacetime, America's enemies will conduct espionage on our government, university research centers, and private companies. They may also seek to prepare for cyberstrikes during a confrontation by mapping U.S. information systems, identifying key targets, 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. They may also attempt to slow the U.S. military response by disrupting systems of the Department of Defense, the intelligence community, and other government organizations as well as critical infrastructures.

The strategic goal is to improve our national security posture in cyberspace to limit the ability of adversaries to pressure the United States and quickly remove threats once identified. The National Security Council, Department of Defense, the Department of Justice, the intelligence community and other Federal departments and agencies should:

- work closely with State and local governments and the private sector to improve the nation's overall cybersecurity posture;
- ensure a strong counterintelligence posture to counter cyber-based intelligence collection against the U.S. Government, and commercial and educational organizations;
- improve the nation's ability to quickly attribute the source of threatening attacks or actions, seeking to develop the capability to suppress threats before attacks occur;
- improve understanding of incident response coordination to significant cyber attacks among law enforcement agencies, national security agencies, and defense agencies; and,
- continue to reserve the right to respond in an appropriate manner when U.S. vital interests are threatened by attacks through cyberspace.

When a nation, terrorist group or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution or even to information warfare means. The United States reserves the right to respond in an appropriate manner when its vital interests are threatened by attacks through cyberspace, just as it would with any other kind of aggression.

Interdependency and Physical Security

When damage occurs to one infrastructure, others are often affected. Events in cyberspace can impact systems in physical space, and vice versa. A train derailed in a Baltimore tunnel and the Internet slowed in Chicago. A campfire in New Mexico damaged a gas pipeline and IT-related production halted in Silicon Valley. A satellite spun out of control hundreds of miles above the Earth and affected bank customers could not use their ATMs.

Cyberspace also has physical manifestations: the buildings and conduits that support telecommunications and Internet networks. These physical elements have been designed and built to create redundancy and avoid single points of failure. Nonetheless, the carriers and service providers should independently and collectively continue to analyze their networks to strengthen reliability and intentional redundancy. The FCC, through its National Reliability and Interoperability Council (NRIC), and the Board through the National Security Telecommunications Advisory Committee (NSTAC), can contribute to such efforts and should identify any governmental impediments to strengthening the national networks.

The strategic goal for interdependency and physical protection of cyberspace is to mitigate the potential negative effects that the disruption of one infrastructure might have on another.

Attaining this goal may be accomplished through government and private industry efforts to:

- foster information sharing between owners of critical infrastructure, government, and private groups that are working to model systems and develop solutions;
- develop a robust national modeling capability for critical infrastructure interdependencies; and,
- create awareness among cyber infrastructure owners and operators of the potential impacts that the loss of the infrastructure might have on others, and steps to minimize negative effects.

AGENDA

LEVEL 4: National Priorities

RECOMMENDATIONS

*Specific actions that government and nongovernment entities can take to promote cybersecurity.**

R4-1 A public-private partnership should refine and accelerate the adoption of improved security for Border Gateway Protocol, Internet Protocol, Domain Name System, and others.

R4-2 A public-private partnership should perfect and accelerate the adoption of more secure router technology and management, including out-of-band management.

R4-3 Internet service providers, beginning with Tier 1 companies or major access providers, should consider adopting a "code of good conduct" governing their cybersecurity practices, including their security-related cooperation with one another.

R4-4 A public-private partnership should identify and address fundamental technology needs for the Internet, possibly making use of the existing programs and potentially establishing a fund for such activities.

R4-5 A public-private partnership should, as a high priority, develop best practices and new technology to increase security of digital control systems and supervisory control and data acquisition systems (SCADA) in utilities, manufacturing, and other networks.

R4-6 Government and industry, working in partnership, should determine the most critical DCS/SCADA-related sites and develop a prioritized plan for short-term cybersecurity improvements in those sites. DCS/SCADA users should consider adopting the Department of Energy's *"21 Steps to Improve Cybersecurity of SCADA Networks."*

R4-7 The R&D committee of the President's Critical Infrastructure Protection Board (PCIPB) should undertake a comprehensive review and gap analysis of existing mechanisms for outreach, identification and coordination of research and development among academia, industry and government. The committee will complete its work and present its recommendations on the need to reform, expand, or establish such mechanisms to the PCIPB in February 2003.

R4-8 The President's Board should coordinate with the Director of OSTP and the Board's R&D Committee on an annual basis to define a program of Federal government research and development including near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research.

R4-9 Federally funded near-term IT security research and development for FY04 and beyond should include priority programs identified by OSTP and the R&D Committee. Existing priorities include, among others, intrusion detection, Internet infrastructure security (including protocols such as BGP, DNS), application security, denial of service, communications security (including SCADA system encryption and authentication), high assurance systems, and secure system composition.

R4-10 The private sector should consider including in near-term research and development priorities, programs for highly secure and trustworthy operating systems. If such systems are developed and successfully evaluated, the Federal government should accelerate procurement of such systems.

R4-11 Federally and privately funded research and development should include programs to examine the security implications of emerging technologies.

R4-12 Federal departments and agencies must be especially mindful of security risks when using wireless technologies. Federal agencies should consider installing systems that continuously check for unauthorized connections to their networks. Agencies should carefully review the recent NIST report on the use of wireless technologies and take into account NIST recommendations and findings. In that regard, agency policy and procedures should reflect careful consideration of additional risk reduction measures including the use of strong encryption, bi-directional authentication, shielding standards and other technical security considerations, configuration management, intrusion detection, incident handling, and computer security education and awareness programs.

R4-13 Government and industry should actively promote awareness for individuals, enterprises, and government of the security issues involved in the adoption of wireless technologies, especially those utilizing the 802.11b standard and related standards. Industry and government should work closely together to promote the continued development of improved standards and protocols for wireless LANs that have built-in, transparent security.

R4-14 A voluntary, industry-led, national effort should consider developing a clearinghouse for promoting more effective software patch implementation. Such an effort may include increased exchange of data about the impact that patches may have on commonly used software systems, including, where practicable, the results of testing.

R4-15 The software industry should consider promoting more secure "out-of-the-box" installation and implementation of their products, including increasing: (1) user awareness of the security features in products; (2) ease-of-use for security functions; and, (3) where feasible, promotion of industry guidelines and best practices that support such efforts.

R4-16 A national public-private effort should promulgate best practices and methodologies that promote integrity, security and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development.

R4-17 The PCIPB's Awareness Committee, in cooperation with lead agencies, should foster a public-private partnership to develop and disseminate cybersecurity awareness materials, such as audience-specific tools and resources for annual awareness training.

R4-18 The StaySafeOnline campaign should be expanded to include national advertising aimed at several audience groups. It should also develop materials for schools, and companies.

R4-19 States should consider creating Cyber Corps scholarship-for-service programs at State universities, to fund the education of undergraduate and graduate students specializing in IT security and willing to repay their grants by working for the States. The existing Cyber Corps scholarship-for-service program should be expanded to additional universities, with both faculty development and scholarship funding. The program should also add a faculty and program development effort for community colleges.

R4-20 The CIO Council and Federal agencies with cybersecurity training expertise should consider establishing a Cyberspace Academy, which would link Federal cybersecurity and computer forensics training programs.

R4-21 Public and private research labs across the nation should explore the benefits of establishing programs like the Cyber Defenders Program at the Department of Energy's Sandia National Laboratory.

R4-22 The PCIPB's Committee on Training should explore the potential benefits of establishing a multi-department corps of IT and cybersecurity specialists taking maximum advantage of innovative, efficient, and flexible human resource programs.

AGENDA

LEVEL 4: National Priorities

R4-23 State, local and private organizations should consider developing programs and guidelines for primary and secondary school students in cyber ethics, safety, and security.

R4-24 IT security professionals, and IT security associations and organizations, should explore approaches to, and the feasibility of, establishing a rigorous certification program, including a continuing education and retesting program.

R4-25 The Congress and the Executive Branch should work together to remove impediments to information sharing about cybersecurity and infrastructure vulnerabilities between the public and private sectors.

R4-26 Appropriate Federal agencies should develop a strategy to encourage citizens and corporations to report incidents of cybercrime, cyber attacks and unauthorized intrusions. In addition, this strategy could also explore mechanisms which facilitate such reporting.

R4-27 The FBI and Secret Service should continue to improve coordination of their field offices' cybercrime investigations and consider expanding pilot Joint Task Forces.

R4-28 Improve information sharing and investigative coordination within the Federal, State, and local law enforcement community working on critical infrastructure and cyberspace security matters, and with other agencies and the private sector.

R4-29 The Federal government should collect survey data regarding victims of cybercrime (i.e., businesses, organizations, and individuals) in order to better establish a baseline understanding of the problem and measure future effectiveness.

R4-30 The Federal government should review the level of training and funding for Federal, State, and local law enforcement for forensic and investigative efforts to address critical infrastructure incidents and cybercrime.

R4-31 The Federal government should continue to assess the Federal sentencing guidelines to see if they are adequate for cybercrime.

R4-32 The President's Board, working with OMB and in partnership with the private sector and State governments, should review Federal and States regulations and laws that impede market forces from contributing to enhanced cybersecurity.

R4-33 The PCIPB's Financial and Banking Information Infrastructure Committee (FBIIC), working with the insurance industry, should explore the options for developing an effective risk-transfer mechanism for cybersecurity, including improving risk modeling and availability of loss data.

R4-34 Corporations should consider annually disclosing the identity of their IT security audit firm and the general scope of its work, the corporate and board governance system for IT security, company adherence to IT security best practices or standards, and corporate participation in ISACs and other IT security programs.

R4-35 The President's Board, working with the Institute of Internal Auditors and Corporate Board Members Association and similar groups should continue and enhance the effectiveness of programs of awareness and best practices.

R4-36 The Executive branch should consult regularly with privacy advocates, industry representatives and other interested organizations to facilitate consideration of privacy and civil liberties concerns in the implementation of the National Strategy, and to achieve solutions that protect privacy while enhancing network and host security.

R4-37 As part of the annual departmental IT security audits, agencies should include a review of IT related privacy regulation compliance.

R4-38 The appropriate Federal agencies should consider reviews of the IT security issues related to the implementation of the Gramm, Leach, Bliley Financial Modernization Act and the Health Insurance Portability and Accountability Act.

R4-39 ISPs, hardware and software vendors, IT security-related companies, computer emergency response teams, and the ISACs, together, should consider establishing a Cyberspace Network Operations Center (Cyberspace NOC), physical or virtual, to share information and ensure coordination to support the health and reliability of Internet operations in the United States. Although it would not be a government entity and would be managed by a private board, the Federal government should explore the ways in which it could cooperate with the Cyberspace NOC.

R4-40 The Federal government should complete the installation of the Cyber Warning Information Network (CWIN) to key government and nongovernment cybersecurity-related network operation centers, to disseminate analysis and warning information and perform crisis coordination.

R4-41 Industry, in voluntary partnership with the Federal government, should complete and regularly update cybersecurity crisis contingency plans, including a recovery plan for Internet functions.

R4-42 The Federal government should review emergency authorities and determine if the existing authorities are sufficient to support Internet recovery.

R4-43 The United States should establish a vigorous program to counter cyber-based intelligence collection against U.S. government, industry, and university sites.

R4-44 The National Security Council should lead a study to improve understanding of incident response coordination for significant cyber attacks among law enforcement agencies, national security agencies, and defense agencies.

R4-45 The United States should continue to improve its ability to quickly attribute the source of threatening attacks or actions, seeking to develop the capability to suppress threats before attacks occur.

R4-46 The United States should continue to reserve the right to respond in an appropriate manner when its vital interests are threatened by nation-states or terrorist groups engaged in cyber attacks.

R4-47 Public-private partnerships should identify cross-sectoral interdependencies both cyber and physical. They should develop plans to reduce related vulnerabilities, in conjunction with programs proposed in the *National Strategy for Homeland Security*. The National Infrastructure Simulation and Analysis Center should support these efforts.

R4-48 Owners and operators of information system networks and network data centers should consider developing remediation and contingency plans to reduce the consequences of large-scale physical damage to facilities supporting such networks. Where requested, the Federal government could help coordinate such efforts and provide technical assistance.

R4-49 Owners and operators of information system networks should, possibly working with the Federal government on a voluntary basis, develop appropriate procedures for limiting access to critical facilities.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D4-1 How can government, industry, and academia address issues important and beneficial to owners and operators of cyberspace but for which no one group has adequate incentive to act?

D4-2 How could out-of-band management for routers be implemented on the Internet, and what are the costs and benefits?

D4-3 How should private sectors craft outreach programs to reach all levels of the DCS/SCADA user community to increase awareness of vulnerabilities, consequences, and mitigation measures?

D4-4 What training courses and materials should such programs include to equip DCS/SCADA users with the skills necessary to improve security?

D4-5 Technology transfer, the process by which existing knowledge, facilities or capabilities developed under Federal R&D funding are utilized to fulfill public and private needs, must be enhanced. The most vital part of technology transfer, the adoption of new security technologies by the private sector, especially the vendor communities, should be the object of discussion for a private / public partnership. What mechanisms could effectively be applied to encourage the adoption of existing and emerging security technologies by vendors?

D4-6 What are the potential security and privacy implications of emerging technologies such as wireless LANS?

D4-7 Should government work closely with emerging technology product vendors to promote disclosure of the vulnerabilities associated with their products' use and encourage vendors to make security easier to apply for the average user?

D4-8 How and by what means should curriculum for software engineers change to reflect more secure coding practices?

D4-9 Is there an appropriate way to define standard time limits for the patching of systems?

D4-10 What metrics should be used to measure cybersecurity awareness for various audiences and the effectiveness of cybersecurity warnings?

D4-11 What roles can private citizens play in raising awareness about cybersecurity?

D4-12 How can government and private industry establish programs to identify early students with a demonstrated interest in and/or talent for IT security work, encourage and develop their interest and skills, and direct them into the workforce?

D4-13 How can government and industry identify national training and education standards for cybersecurity professions that will meet the demands of U.S. enterprises?

D4-14 Should an accrediting body be created that would set a baseline standard for system administrator-level security knowledge requirements?

D4-15 Should other levels of the IT security profession be considered for peer certification or accreditation?

D4-16 Should the Federal government provide support to ISACs such as funding, technical tools or facilities?

D4-17 How may victims rights groups aid in creating greater awareness about the potential dangers of cybercrime?

D4-18 Is there a gap between Federal, State, and local laws on cybercrime? If so, what are the implications?

D4-19 What lessons can be learned from the "Basel Accord" that might drive cybersecurity improvements in other infrastructures?

D4-20 Should there be a review of State and Federal requirements for disclosure of information which could help potential attackers; e.g., State filings?

D4-21 How can industry be encouraged to incorporate appropriate privacy protections into their planning and products, using flexible, non-regulatory approaches?

D4-22 How can government organizations work to facilitate harmonious approaches in privacy across jurisdictional boundaries?

D4-23 How can the Federal government and the private sector develop people with the ability to "deep dive" data and detect patterns of attack?

D4-24 It took over four decades to develop an indications and warning capability for conventional and nuclear threats. How can the United States develop a similar "incidents and warning" architecture to protect against cyber threats that would be highly effective?

D4-25 Is there a need for a new authority, which is not anchored in war mobilization and national defense, to manage priority delivery of goods and services for critical infrastructure purposes?

D4-26 Identifying the key infrastructure interdependencies requires an active discussion between the public and private sectors. What processes should be established to help shape how the Federal government prioritizes and funds interdependency and vulnerability studies?

D4-27 Because cyber attacks can be launched from anywhere in the world, it is important to develop capabilities to rapidly determine the origin of an attack or exploit in order to respond effectively. This capability, commonly referred to as "attribution," is central to determining if an attack is sponsored by a foreign power. How can government and industry analysts enhance attribution capabilities in order to more rapidly identify the source of an attack?

D4-28 How can the national security community enhance the discipline of counter intelligence analysis to better support cyberspace security?

LEVEL 5: GLOBAL

The strategic goal is to work with the international community to ensure the integrity of the global information networks that support critical U.S. economic and national security infrastructure. This goal can be achieved through a range of initiatives. The United States will:

- promote the development of an international network to identify and defend against cyber incidents as they begin;
- encourage all nations to pass adequate cybersecurity laws so that U.S. law enforcement can investigate and prosecute cybercrime committed against the United States and its interests, whether it originates domestically or abroad;
- work through international organizations to foster a "Culture of Security" worldwide, to ensure the long-term security of the global information infrastructure; and,
- promote the international adoption of common international technical standards that can help assure the security of global information infrastructures.

Issues and Challenges

The U.S. interest in promoting cybersecurity extends well beyond its borders. Critical domestic information infrastructures are directly linked with Canada, Mexico, Europe, Asia, and South America. The nation's economy and security depend on far-flung U.S. corporations, military forces, and foreign trading partners that, in turn, require secure and reliable global information networks to function. The vast majority of cyber attacks originates or passes through systems abroad, crosses several borders, and requires international cooperation to stop.

In 1998, the United States received a wake-up call to the national security dimensions of the threat. Eventually dubbed "Solar Sunrise," this incident found U.S. military systems under electronic assault, with computer systems in the United Arab Emirates the apparent source. Unclassified logistics, administrative, and accounting systems essential to the management and deployment of military forces were penetrated at a time that military action was being considered against Iraq due to its failure to comply with UN inspection teams trying to uncover evidence of weapons of mass destruction. The timing of the attacks raised U.S. suspicion that this was the first wave of a major cyber attack by a hostile nation.

It was eventually learned that two California teenagers under the guidance and direction of a sophisticated Israeli hacker, himself a teenager, had orchestrated the attacks using hacker tools readily available on the Internet. They had attempted to hide their involvement by connecting through overseas computers. Even cybercrimes committed by Americans against U.S. computers often have an international component.

Another event illustrated the threat to the global economy no less starkly. Early in February 2000, computer servers hosting several of the largest commercial web sites on the Internet were flooded with connection requests, which clogged systems and consumed server capacity. Ultimately, these distributed denial-of-service (DDoS) attacks paralyzed large parts of the Internet. Only through close cooperation between U.S. and Canadian law enforcement investigators was it discovered that a Canadian teenager, operating under the moniker of "Mafiaboy," had been breaking into legions of computers around the world for many months. Retaining control over these compromised servers, he created a "zombie army" which on command would flood the servers of his next corporate victim. The slowdowns and outages that occurred resulted in more than an estimated billion dollars in economic losses.

Only a few months later, on the morning of May 4, 2000, the "I love you" virus began infecting computers around the globe. First detected in Asia, this virus quickly swept around the world in a wave of indiscriminate attacks on government and private sector networks. By the time the destructive pace of the virus had been slowed, it had infected nearly 60 million computers and caused billions of dollars in damage. Cooperation among law enforcement authorities around the world led to the identification of the perpetrator, a computer science dropout in the Philippines.

He was neither charged nor punished for his deeds because, at the time, the Philippine criminal code did not explicitly outlaw such actions.

Together, these incidents make clear that U.S. domestic efforts alone cannot deter or prevent this tide of attacks. We must work closely with our international partners to put into place those cooperative mechanisms that can help prevent the damage resulting from such attacks; and if prevention fails, have those instruments in place that can help us to investigate and prosecute such crimes.

Discussion of Strategy

The United States will promote a wide range of initiatives to enhance cyberspace security globally and will disseminate key policy messages through the full array of bilateral, multilateral and international fora, as appropriate. These initiatives will: build real-time, "24/7" watch-and-warning networks to identify incidents and stop them; establish and link a network of cyberspace security coordinators in each nation; use international

organizations to promote regionally the principles and standards essential to fostering a global culture of cyberspace security; assist nations in developing the laws and acquiring the skills to effectively investigate and prosecute cybercrime across international borders; and foster collaboration among the best minds in the world on long-term solutions to cybersecurity.

Strengthening International Coordination

Threat Management: For the past three years, the United States has been reaching out to other countries on the issue of cyberspace security. These efforts will be expanded to ensure that international coordination in preventing debilitating cyber incidents is institutionalized. We will encourage each nation to develop its own watch-and-warning network capable of informing government agencies, the public, and other countries about impending attacks or viruses. To facilitate real-time sharing of the threat information as it comes to light, the United States will foster the establishment of an international network capable of receiving, assessing, and disseminating this information globally. Such a network will build on the capabilities of nongovernmental institutions such as the Forum of Incident Response and Security Teams (FIRST) and such long-standing international telecommunications institutions as the International Telecommunication Union (ITU) of which nearly every nation is a member together with over 600 private sector organizations.

National Cyberspace Coordinators

The United States will urge each nation to build on the common Y2K experience and appoint a centralized point-of-contact who can act as a liaison between domestic and global cybersecurity efforts. Establishing these points of contact can greatly enhance the international coordination and resolution of cyberspace security issues.

North American Cyberspace Security

Particular emphasis will be put on ensuring that North America will be a "Safe Cyber Zone." Working with Canada and Mexico to identify best practices for securing the many shared and connected information networks that underpin telecommunications, energy, transportation, and banking and finance systems, emergency service, food, public health, and water systems, the United States will seek coordinated solutions to ensure the integrity and reliability of those systems critical to Americans way of life.

Working Through International Organizations

Combating Cybercrime: The United States will actively foster international cooperation in investigating and prosecuting cybercrime. Ongoing multilateral efforts, such as those in the G-8, Asia-Pacific Economic Council (APEC), Organization of Economic Cooperation and development, and the Council of Europe, are important to success in this area. The United States will work to implement agreed-upon recommendations and action plans that are developed in these fora. Among these initiatives, the United States in particular will urge countries to join the 24-hour, high-tech crime contact network begun within the G-8, and now expanded to the Council of Europe membership, as well as other countries.

The United States has signed and supports the recently concluded Council of Europe Convention on Cybercrime, which requires countries to make cyber attacks a substantive criminal offense and to adopt procedural and mutual assistance measures to better combat cybercrime across international borders. The United States will encourage other nations to accede to the Convention or, at a minimum, make their laws consonant with these requirements.

Efforts to Develop Secure Networks: To ensure the security of information systems and to promote the sharing of important knowledge, the United States will engage in cooperative efforts to solve technical, scientific, and policy-related problems connected with assuring the integrity of information networks. Key initiatives will encourage the development and adoption of international technical standards and facilitate collaboration and research among the world's best scientists and researchers.

The United States will also promote such efforts as the Organization for Economic Cooperation and Development (OECD), *Guidelines for the Security of Information Systems and Networks,* which strive to inculcate a "culture of security" across all participants in the new information society.

Because most nations' key information infrastructures reside in private hands, the United States will seek the participation of U.S. industry to engage foreign counterparts in a peer-to-peer dialogue, with the twin objectives of making an effective business case for cybersecurity, and explaining successful means for partnering with government on cybersecurity.

AGENDA
LEVEL 5: GLOBAL

RECOMMENDATIONS

Specific actions that government and nongovernment entities can take to promote cybersecurity.

R5-1 The Federal government, in coordination with the private sector, should work with individual nations and with nongovernmental and international organizations to foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge. In addition, such networks could help support efforts to investigate and respond to those attacks.

R5-2 The United States should encourage nations to accede to the Council of Europe (COE) Convention on Cybercrime, or to ensure that their laws and procedures are at least as comprehensive.

R5-3 The United States should work together with Canada and Mexico to identify and implement best practices for securing the many shared critical North American information infrastructures.

R5-4 The United States should work through international organizations and in partnership with industry to facilitate dialogue and partnership between foreign public and private sectors on information infrastructure protection, and to promote a global "culture of security."

R5-5 Each country should be urged to appoint a national cyberspace coordinator.

R5-6 The United States should draw upon the global science and technology base by pursuing collaborative research and development in cybersecurity.

PROGRAMS

Existing efforts in cybersecurity.

P5-1 *Involvement in Multi-lateral Organizations:* The United States has had great success promoting cybersecurity in conjunction with other nations through participation in multilateral organizations such as the G-8 and the Council of Europe (COE), and such involvement will continue.

P5-2 *Support for COE Convention:* The United States has, and will continue to recruit countries to accede to the Convention or to enact procedural and substantive cybercrime laws at least as comprehensive as the Convention.

P5-3 *Bilateral Discussions:* The United States has contributed to significant improvements in the cybersecurity of other nations and the cooperation of those nations with U.S. law enforcement efforts, by conducting bilateral discussions that encourage countries to improve legal systems and foster bilateral cooperation in cybercrime prevention, investigation, and prosecution.

P5-4 *Advisory and Educational Outreach:* The United States has advised countries developing procedural and substantive cybercrime laws and provided educational seminars regarding the virtues and benefits of an adequate cybercrime legal regime. The United States also provides training and technical assistance to foreign law enforcement to improve their capacity to cooperate in fighting cybercrime.

P5-5 *International Watch-and-Warning Networks:* The United States participates in international networks, one of which was established by the National Infrastructure Protection Center, to detect early and prevent cyber attacks that cross international borders.

P5-6 *International Law Enforcement Networks:* The United States participates in international networks, such as the *"24-Hour Contacts for International High-Tech Crime"* maintained by the G-8, to investigate and prosecute the perpetrators of cyber attacks that cross international borders.

DISCUSSIONS

Issues highlighted for continued analysis, debate, and discussion.

D5-1 What role should the private sector play to best assist developing countries in establishing a "culture of security?"

SUMMARY OF RECOMMENDATIONS*

LEVEL 1: THE HOME USER AND SMALL BUSINESS

R1-1 Because automated hacking programs scan the Internet for unprotected broadband connections to exploit, those home users and small businesses planning to install a DSL or cable modem should consider installing firewall software first. (Some Internet service providers (ISPs), offer firewall software with DSL or cable modem set up.) Once firewall software is installed, it is important to regularly update it by going to the vendor's web site.

R1-2 Because new computer viruses are introduced every week, home users and small businesses should regularly ensure that they are running an up-to-date "antivirus system." (Some antivirus vendors offer automatic updates online. Some Internet service providers scan all incoming e-mail for viruses before the e-mail gets to the user's computer.)

R1-3 Because new viruses often come as e-mail, home users should use caution when opening e-mail from unknown senders, particularly those with attachments. To reduce the number of unknown senders, home users should consider using software that controls unsolicited advertisements, called "spam." (Some ISPs offer programs to block spam. Some ISPs also offer to block all incoming e-mail except from those friends and associates that the user selects.)

R1-4 Home users should also regularly update their personal computer's operating systems (such as Microsoft Windows, Macintosh, Linux) and major applications (software that browses the Internet or creates documents, charts, tables, etc.) for security enhancements by going to the vendors web sites. (Some software vendors offer automatic updates online.)

R1-5 Internet service providers, antivirus software companies, and operating system/application software developers should consider joint efforts to make it easier for the home user and small business to obtain security software and updates automatically and in a timely manner, including warning messages to home users about updates and new software patches.

LEVEL 2: LARGE ENTERPRISES

R2-1 CEOs should consider forming enterprisewide corporate security councils to integrate cybersecurity, privacy, physical security, and operational considerations.

R2-2 CEOs should consider regular independent Information Technology (IT) security audits, remediation programs, and reviews of "best practices" implementation.

R2-3 Corporate boards should consider forming board committees on IT security and should ensure that the recommendations of the chief information security official in the corporation are regularly reviewed by the CEO.

R2-4 Corporate IT continuity plans should be regularly reviewed and exercised and should consider site and staff alternatives. Consideration should be given to diversity in IT service providers as a way of mitigating risks.

R2-5 Corporations should consider active involvement in industrywide programs to: (a) develop IT security best practices and procurement standards for like companies; (b) share information on IT security through an appropriate information sharing and analysis center (ISAC); (c) raise cybersecurity awareness and public policy issues; and, (d) work with the insurance industry on ways to expand the availability and utilization of insurance for managing cyber risk.

R2-6 Corporations should consider joining in a public-private partnership to establish an awards program for those in industry making significant contributions to cybersecurity.

R2-7 (1) Enterprises should review mainframe security software and procedures to ensure that the latest effective technology and procedural measures are being utilized; (2) IT vendors and enterprises employing mainframes should consider developing a partnership to review and update best practices of mainframe IT security and to ensure that there continues to be an adequate trained cadre of mainframe specialists; and (3) IT security audits should include comprehensive evaluations of mainframes.

LEVEL 3: CRITICAL SECTORS THE FEDERAL GOVERNMENT

R3-1 In order to enhance the procurement of more secure IT products, the Federal government, by 4Q FY03, will complete a comprehensive program performance review of the National Information Assurance Program (NIAP), to determine the extent to which NIAP is cost effective and targets a clearly identified security gap; whether it has defined goals to close the gap, whether it is achieving those goals, and the extent to which program improvements, streamlining, or expansion are appropriate and cost effective.

R3-2 The Federal government, by 3Q FY03, will assess whether private sector security service providers to the Federal government should be certified as meeting certain minimum capabilities.

R3-3 The Federal government, by 3Q FY03, using the E-Government model, will explore the benefits (including reducing resource pressures on small agencies) of greater cross-government acquisition, operation, and maintenance of security tools and services.

R3-4 Through the ongoing E-Authentication initiative, the Federal government, by 2Q FY03, will explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms to further promote consistency and interoperability.

R3-5 Federal departments should continue to expand the use of automated, enterprise-wide security assessment and security policy enforcement tools and actively deploy threat management tools to preempt attacks. By 2Q FY03, the Federal government will determine whether specific actions are necessary (e.g., through the policy or budget processes) to promote the greater use of these tools.

R3-6 The Federal government will continue to assess the technical viability and cost effectiveness of various options that provide for the continuity of operations during service outages such as VPNs, "private line" networks, and others.

R3-7 The Federal government should lead in the adoption of secure network protocols. The Federal government will review new secure network protocols as they are published to determine whether they fill a security gap and whether their adoption would have a cost-effective impact on the operations and security of the Federal government.

R3-8 By the end of 2Q FY03, the Federal government will consider the cost effectiveness of a scenario-based security and contingency preparedness exercise for a selected cross-government business process. Should such an exercise take place any security weaknesses shall be included as part of agencies' GISRA corrective action plans.

R3-9 OMB, in conjunction with the CIO council,will determine on a case by case basis whether to employ a lead agency concept for governmentwide security measures. The alternatives will generally include GSA, NIST, the proposed Department of Homeland Security, and the Department of Defense.

LEVEL 3: CRITICAL SECTORS STATE AND LOCAL GOVERNMENTS

R3-10 State and local governments should consider establishing IT security programs for their departments and agencies, including awareness, audits, and standards. State, county, and city associations should consider providing assistance, materials, and model programs.

R3-11 State and local governments should consider participating in the established information sharing and analysis centers (ISACs) with similar governments.

R3-12 State and local governments should consider expanding training programs in computer crime for law enforcement officials, including judges, prosecutors, and police. The Federal government could assist in coordinating such training and explore whether funding assistance is feasible.

LEVEL 3: CRITICAL SECTORS HIGHER EDUCATION

R3-13 Each college and university should consider establishing a point-of-contact, reachable at all times, to Internet service providers (ISPs) and law enforcement officials in the event that the school's IT systems are discovered to be launching cyber attacks.

R3-14 Colleges and universities should consider establishing together: (a) one or more information sharing and analysis centers (ISACs) to deal with cyber attacks and vulnerabilities; (b) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (c) one or more set of best practices for IT security; and, (d) model user awareness programs and materials.

LEVEL 3: CRITICAL SECTORS PRIVATE SECTORS

R3-15 Each sector group should consider establishing an information sharing and analysis center (ISAC) that should cooperate with other ISACs. The Federal government will explore linking the ISACs with appropriate cybersecurity warning-and-analysis centers upon request, and could facilitate the provision of information related to critical infrastructure protection when necessary.

R3-16 Each sector group should consider conducting a technology and R&D gap analysis, in conjunction with OSTP efforts to prioritize Federal cybersecurity research to address identified gaps. The sectors and OSTP should coordinate on the conduct of such research.

R3-17 Each critical infrastructure sector group should consider developing best practices for cybersecurity and, where appropriate, guidelines for the procurement of secure IT products and services.

R3-18 Each sector group should consider working together on sector specific information security awareness campaigns.

R3-19 Each sector should consider establishing mutual assistance programs for cybersecurity emergencies. The Department of Justice and the Federal Trade Commission should work with the sectors to address any barriers with such cooperation.

LEVEL 4: NATIONAL PRIORITIES SECURING THE MECHANISMS OF THE INTERNET

R4-1 A public-private partnership should refine and accelerate the adoption of improved security for Border Gateway Protocol, Internet Protocol, Domain Name System, and others.

R4-2 A public-private partnership should perfect and accelerate the adoption of more secure router technology and management, including out-of-band management.

R4-3 Internet service providers, beginning with Tier 1 companies or major access providers, should consider adopting a "code of good conduct" governing their cybersecurity practices, including their security-related cooperation with one another.

R4-4 A public-private partnership should identify and address fundamental technology needs for the Internet, possibly making use of the existing programs and potentially establishing a fund for such activities.

LEVEL 4: NATIONAL PRIORITIES DCS/SCADA

R4-5 A public-private partnership should, as a high priority, develop best practices and new technology to increase security of digital control systems and supervisory control and data acquisition systems (SCADA) in utilities, manufacturing, and other networks.

R4-6 Government and industry, working in partnership, should determine the most critical DCS/SCADA-related sites and develop a prioritized plan for short-term cybersecurity improvements in those sites. DCS/SCADA users should consider adopting the Department of Energy's *"21 Steps to Improve Cybersecurity of SCADA Networks."*

LEVEL 4: NATIONAL PRIORITIES RESEARCH AND DEVELOPMENT

R4-7 The R&D committee of the President's Critical Infrastructure Protection Board (PCIPB) should undertake a comprehensive review and gap analysis of existing mechanisms for outreach, identification and coordination of research and development among academia, industry and government. The committee will complete its work and present its recommendations on the need to reform, expand, or establish such mechanisms to the PCIPB in February 2003.

R4-8 The President's Critical Infrastructure Protection Board should coordinate with the Director of OSTP and the board's R&D Committee on an annual basis to define a program of Federal government research and development including near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research.

R4-9 Federally funded near-term IT security research and development for FY04 and beyond should include priority programs identified by OSTP and the R&D Committee. Existing priorities include among others, intrusion detection, Internet infrastructure security (including protocols e.g. BGP, DNS), application security, denial of service, communications security including SCADA system encryption and authentication, high assurance systems, and secure system composition.

R4-10 The private sector should consider including in near-term research and development priorities, programs for highly secure and trustworthy operating systems. If such systems are developed and successfully evaluated, the Federal government should accelerate procurement of such systems.

R4-11 Federally and privately funded research and development should include programs to examine the security implications of emerging technologies.

LEVEL 4: NATIONAL PRIORITIES
SECURING EMERGING SYSTEMS

R4-12 Federal departments and agencies must be especially mindful of security risks when using wireless technologies. Federal agencies should consider installing systems that continuously check for unauthorized connections to their networks. Agencies should carefully review the recent NIST report on the use of wireless technologies and take into account NIST recommendations and findings. In that regard, agency policy and procedures should reflect careful consideration of additional risk reduction measures including the use of strong encryption, bi-directional authentication, shielding standards and other technical security considerations, configuration management, intrusion detection, incident handling, and computer security education and awareness programs.

R4-13 Government and industry should actively promote awareness for individuals, enterprises, and government of the security issues involved in the adoption of wireless technologies, especially those utilizing the 802.11b standard and related standards. Industry and government should work closely together to promote the continued development of improved standards and protocols for wireless LANs that have built-in, transparent security.

LEVEL 4: NATIONAL PRIORITIES
VULNERABILITY REMEDIATION

R4-14 A voluntary, industry-led, national effort should consider developing a clearinghouse for promoting more effective software patch implementation. Such an effort may include increased exchange of data about the impact that patches may have on commonly used software systems, including, where practicable, the results of testing.

R4-15 The software industry should consider promoting more secure "out-of-the-box" installation and implementation of their products, including increasing: (1) user awareness of the security features in products; (2) ease-of-use for security functions; and, (3) where feasible, promotion of industry guidelines and best practices that support such efforts.

R4-16 A national public-private effort should promulgate best practices and methodologies that promote integrity, security and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development.

LEVEL 4: NATIONAL PRIORITIES
AWARENESS

R4-17 The President's Critical Infrastructure Protection Board's Awareness Committee, in cooperation with lead agencies, should foster a public-private partnership to develop and disseminate cybersecurity awareness materials, such as audience-specific tools and resources for annual awareness training.

R4-18 The StaySafeOnline campaign should be expanded to include national advertising aimed at several audience groups. It should also develop materials for schools and companies.

LEVEL 4: NATIONAL PRIORITIES
TRAINING AND EDUCATION

R4-19 States should consider creating Cyber Corps scholarship-for-service programs at State universities, to fund the education of undergraduate and graduate students specializing in IT security and willing to repay their grants by working for the States. The existing Cyber Corps scholarship-for-service program should be expanded to additional universities, with both faculty development and scholarship funding. The program should also add a faculty and program development effort for community colleges.

R4-20 The CIO Council and Federal agencies with cybersecurity training expertise should consider establishing a Cyberspace Academy, which would link Federal cybersecurity and computer forensics training programs.

R4-21 Public and private research labs across the nation should explore the benefits of establishing programs like the Cyber Defenders Program at the Department of Energy's Sandia National Laboratory.

R4-22 The PCIPB's Committee on Training should explore the potential benefits of establishing a multi-department corps of IT and cybersecurity specialists taking maximum advantage of innovative, efficient, and flexible human resource programs.

R4-23 State, local and private organizations should consider developing programs and guidelines for primary and secondary school students in cyber ethics, safety, and security.

LEVEL 4: NATIONAL PRIORITIES
CERTIFICATION

R4-24 IT security professionals, and IT security associations and organizations, should explore approaches to, and the feasibility of, establishing a rigorous certification program, including a continuing education and retesting program.

LEVEL 4: NATIONAL PRIORITIES
INFORMATION SHARING

R4-25 The Congress and the Executive Branch should work together to remove impediments to information sharing about cybersecurity and infrastructure vulnerabilities between the public and private sectors.

LEVEL 4: NATIONAL PRIORITIES CYBERCRIME

R4-26 Appropriate Federal agencies should develop a strategy to encourage citizens and corporations to report incidents of cybercrime, cyber attacks and unauthorized intrusions. In addition, this strategy could also explore mechanisms which facilitate such reporting.

R4-27 The FBI and Secret Service should continue to improve coordination of their field offices' cybercrime investigations and consider expanding pilot Joint Task Forces.

R4-28 Improve information sharing and investigative coordination within the Federal, State, and local law enforcement community working on critical infrastructure and cyberspace security matters, and with other agencies and the private sector.

R4-29 The Federal government should collect survey data regarding victims of cybercrime (i.e., businesses, organizations, and individuals) in order to better establish a baseline understanding of the problem and measure future effectiveness.

R4-30 The Federal government should review the level of training and funding for Federal, State and local law enforcement for forensic and investigative efforts to address critical infrastructure incidents and cybercrime.

R4-31 The Federal government should continue to assess the Federal sentencing guidelines to see if they are adequate for cybercrime.

LEVEL 4: NATIONAL PRIORITIES
MARKET FORCES

R4-32 The President's Board, working with OMB and in partnership with the private sector and State governments, should review Federal and States regulations and laws that impede market forces from contributing to enhanced cybersecurity.

R4-33 The PCIPB's Financial and Banking Information Infrastructure Committee (FBIIC), working with the insurance industry, should explore the options for developing an effective risk-transfer mechanism for cybersecurity, including improving risk modeling and availability of loss data.

R4-34 Corporations should consider annually disclosing the identity of their IT security audit firm and the general scope of its work, the corporate and board governance system for IT security, company adherence to IT security best practices or standards, and corporate participation in ISACs and other IT security programs.

R4-35 The President's Critical Infrastructure Protection Board, working with the Institute of Internal Auditors and Corporate Board Members Association and similar groups should continue and enhance the effectiveness of programs of awareness and best practices.

LEVEL 4: NATIONAL PRIORITIES
PRIVACY AND CIVIL LIBERTIES

R4-36 The Executive Branch should consult regularly with privacy advocates, industry representatives and other interested organizations to facilitate consideration of privacy and civil liberties concerns in the implementation of the National Strategy, and to achieve solutions that protect privacy while enhancing network and host security.

R4-37 As part of the annual departmental IT security audits, agencies should include a review of IT related privacy regulation compliance.

R4-38 The appropriate Federal agencies should conduct reviews of the IT security issues related to the implementation of the Gramm, Leach, Bliley Financial Modernization Act and the Health Insurance Portability and Accountability Act.

LEVEL 4: NATIONAL PRIORITIES
CYBERSPACE ANALYSIS AND WARNING

R4-39 ISPs, hardware and software vendors, IT security-related companies, computer emergency response teams, and the ISACs, together, should consider establishing a Cyberspace Network Operations Center (Cyberspace NOC), physical or virtual, to share information and ensure coordination to support the health and reliability of Internet operations in the United States. Although it would not be a government entity and would be managed by a private board, the Federal government should explore the ways in which it could cooperate with the Cyberspace NOC.

R4-40 The Federal government should complete the installation of the Cyber Warning Information Network (CWIN) to key government and nongovernment cybersecurity-related network operation centers, to disseminate analysis and warning information and perform crisis coordination.

LEVEL 4: NATIONAL PRIORITIES CONTINUITY OF OPERATIONS, RECOVERY, AND RECONSTITUTION

R4-41 Industry, in voluntary partnership with the Federal government, should complete and regularly update cybersecurity crisis contingency plans, including a recovery plan for Internet functions.

R4-42 The Federal government should review emergency authorities and determine if the existing authorities are sufficient to support Internet recovery.

LEVEL 4: NATIONAL PRIORITIES
NATIONAL SECURITY

R4-43 The United States should establish a vigorous program to counter cyber-based intelligence collection against U.S. government, industry, and university sites.

R4-44 The National Security Council should lead a study to improve understanding of incident response coordination for significant cyber attacks among law enforcement agencies, national security agencies, and defense agencies.

R4-45 The United States should continue to improve its ability to quickly attribute the source of threatening attacks or actions, seeking to develop the capability to suppress threats before attacks occur.

R4-46 The United States should continue to reserve the right to respond in an appropriate manner when its vital interests are threatened by nation-states or terrorist groups engaged in cyber attacks.

LEVEL 4: NATIONAL PRIORITIES
INTERDEPENDENCIES AND PHYSICAL SECURITY

R4-47 Public-private partnerships should identify cross-sectoral interdependencies both cyber and physical. They should develop plans to reduce related vulnerabilities, in conjunction with programs proposed in the *National Strategy for Homeland Security*. The National Infrastructure Simulation and Analysis Center should support these efforts.

R4-48 Owners and operators of information system networks and network data centers should consider developing remediation and contingency plans to reduce the consequences of large-scale physical damage to facilities supporting such networks. Where requested, the Federal government could help coordinate such efforts and provide technical assistance.

R4-49 Owners and operators of information system networks should, possibly working with the Federal government on a voluntary basis, develop appropriate procedures for limiting access to critical facilities.

LEVEL 5: GLOBAL

R5-1 The Federal government, in coordination with the private sector, should work with individual nations and with nongovernmental and international organizations to foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge. In addition, such networks could help support efforts to investigate and respond to those attacks.

R5-2 The United States should encourage nations to accede to the Council of Europe (COE) Convention on Cybercrime or to ensure that their laws and procedures are at least as comprehensive.

R5-3 The United States should work together with Canada and Mexico to identify and implement best practices for securing the many shared critical North American information infrastructures.

R5-4 The United States should work through international organizations and in partnership with industry to facilitate dialogue and partnership between foreign public and private sectors on information infrastructure protection, and to promote a global "culture of security."

R5-5 Each country should be urged to appoint a national cyberspace coordinator.

R5-6 The United States should draw upon the global science and technology base by pursuing collaborative research and development in cybersecurity.

**Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

ACRONYMS

AICPA	American Institute of Certified Public Accountants
BGP	Border Gateway Protocol
CIAO	Critical Infrastructure Assurance Office
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CWIN	Cyber Warning and Information Network
DARPA	Defense Advanced Research Projects Agency
DCS	Digital Control System
DDoS	Distributed Denial of Service Attack
DoS	Denial-of-Service attacks
DSL	Digital Subscriber Line
FBIIC	Financial and Banking Information Infrastructure Committee (of the PCIPB)
FCC	Federal Communications Commission
FedCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams
FTC	Federal Trade Commission
FY	Fiscal Year
GISRA	Government Information Security Reform Act of 2000
GSA	General Services Administration
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IHE	Institution of Higher Education
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
LAN	Local Area Networks
NACD	National Association of Corporate Directors
NCS	National Communications Systems
NERC	North American Electric Reliability Council
NIAC	National Infrastructure Assurance Council
NIAP	National Information Assurance Partnership
NIPC	National Infrastructure Protection Center
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NS/EP	National Security/Emergency Preparedness
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSTAC	National Security Telecommunications Advisory Committee
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCIS	Partnership for Critical Infrastructure Security
PCIPB	President's Critical Infrastructure Protection Board
R&D	Research and Development
SBA	Small Business Administration
SCADA	Supervisory Control and Data Acquisition
SFS	Scholarship for Service (NSF hosted)
TCP/IP	Transport Control Protocol / Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Networks
WLAN	Wireless Local Area Network