NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION

EXECUTIVE SUMMARY

TABLE OF CONTENTS

THE WHITE HOUSE

WASHINGTON

In less than one generation, the information revolution and the introduction of the computer into virtually every dimension of our society has changed how our economy works, how we provide for our national security, and how we structure our everyday lives. Whether we are simply turning on the lights in our homes, boarding a plane, or summoning help when a loved one falls ill, we are relying on one or more elaborate computer-driven systems. Similarly, many of our most sophisticated defense systems rely on commercial power, communications, and transportation, which are also computer-controlled. In the future, computer-related technologies will continue to open new vistas of opportunity for the American people.

Yet this new age of promise carries within it peril. All computer-driven systems are vulnerable to intrusion and destruction. A concerted attack on the computers of any one of our key economic sectors or governmental agencies could have catastrophic affects.

We know that the threat is real. Where once our opponents relied exclusively on bombs and bullets, hostile powers and terrorists can now turn a laptop computer into a potent weapon capable of doing enormous damage. If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack.

That is a major reason why, after reviewing the report of the President's Commission on Critical Infrastructure Protection, I issued Presidential Decision Directive 63 in May 1998. This directive requires that the Executive Branch assess the cyber vulnerabilities of the Nation's critical infrastructures -- information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsible for the continuity of federal, state, and local governments. The directive places special emphasis on protection of the government's own critical assets from cyber attack and the need to remedy deficiencies in order to become a model of information

security. The directive also calls for the Federal Government to produce a detailed Plan to protect and defend America against cyber disruptions.

The National Plan for Information Systems Protection is the first major element of a more comprehensive effort. The Plan for cyber defense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats. It presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety.

For this Plan to succeed, government and the private sector must work together in a partnership unlike any we have seen before. This effort will only succeed if our Nation as a whole rises to this challenge. Therefore, I have asked the members of my Cabinet to work closely with representatives of the private sector industries and public services that operate our critical infrastructures. We cannot mandate our goals through Government regulation. Each sector must decide for itself what practices, procedures, and standards are necessary for it to protect its key systems. As part of this partnership, the Federal Government stands ready to help.

The Federal Government does, however, have an important role to play itself. This includes research and development efforts in the field of computer security, educating a corps of young computer scientists to help defend our federal cyber systems, and assisting the private sector as it creates defensive measures for its information technologies.

As we move forward in this effort, all Americans should know that increasing our computer defenses cannot and will not come at the expense of our civil liberties. We must never undermine the very freedoms we are seeking to protect.

The milestones I have established in the Plan are ambitious. Achieving them will require the continuing commitment of our national leadership, intense public-private cooperation, and the legislation and appropriations necessary to bring them to realization. However, it is an essential undertaking that we must begin now, so that we can continue to enjoy the extraordinary opportunities of the Information Age and create the security we require for our prosperity and growth in the next century.

MESSAGE FROM THE NATIONAL COORDINATOR

The accompanying National Plan is the first attempt by any national government to design a way to protect its cyberspace.

A New American Dependence…A New Threat to America

More than any other nation, America is dependent upon its cyberspace. Attacks upon our cyberspace could crash electrical power grids, telephone networks, transportation systems, and financial institutions. All of those sectors depend upon control networks involving computer systems.

In the next war, the target could be America's infrastructure and the new weapon could be a computer-generated attack on our critical networks and systems. We know other governments are developing that capability.

We need, therefore, to redesign the architecture of our national information infrastructure. Over the last decade we built it quickly and without adequate concern for security, without thought that a sophisticated enemy might attack it. Now we must fix it, to protect, guard against, or reduce the existing vulnerabilities.

The President has directed that a Plan for defending our cyberspace be initially in effect by December 2000 and be fully operational by May 2003. To reach those deadlines, we must move quickly, for there is much to do.

A Real Public-Private Partnership…Not Dictated Solutions

The President has ordered that the Federal Government will be a model of computer system security. Today it is not. The Defense Department is well on its way to creating secure systems, but civilian Agencies are also critical and they are generally still insufficiently protected from computer system attack. This Plan proposes additional steps to be taken by DoD and by the rest of the Federal Government.

The private sector infrastructure is, however, at least as likely to be the target for computer system attack. Throughout the modern era, critical industries and utilities have been targets for destruction in conflicts. America's strength rests on its privately owned and operated critical infrastructures and industries.

Already, privately owned computer networks are being surveyed, penetrated, and in some cases made the subject of vandalism, theft, espionage, and disruption. While the President and Congress can order Federal networks to be secured, they cannot and should not dictate solutions for private sector systems.

Thus, the Plan, at this stage, does not lay out in great detail what will be done to secure and defend private sector networks, but suggests a common framework for action. Already some private sector groups have decided to unite to defend their computer networks. As they commit

to this activity, the Federal Government can and will help them, in the spirit of a true public-private partnership. The Government will not dictate solutions and will eschew regulation. Nor will the Government infringe on civil liberties, privacy rights, or proprietary information.

This is Version 1.0 of the Plan. We earnestly seek and solicit views about its improvement. As private sector entities make more decisions and plans to reduce their vulnerabilities and improve their protections, future versions of the Plan will reflect that progress.

Elements of the Solution...and above all, Trained People

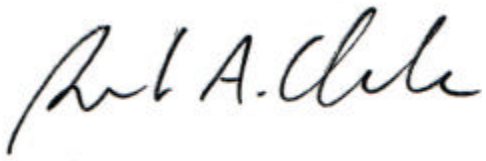
As you will see in the text, the Plan will build a defense of our cyberspace relying on new security standards, multi-layered defensive technologies, new research, and trained people. Of all of these, the most urgently needed, the hardest to acquire, and the *sine qua non* for all else that we will do, is a cadre of trained computer science/information technology (IT) specialists.

When America quickly wired itself for electricity a century ago, it quickly trained electricians and electrical engineers for that new economy. So far, America is failing to train the IT specialists it needs to operate, improve, and secure its new IT-based economy. The Plan proposes steps to stimulate the higher education market to produce what America urgently needs in this area.

We will follow up our plan for cyber defense with a second plan focusing on how Government can work with the Nation's infrastructure sectors to help assure the reliability and physical security of essential services from major disruptions. This forthcoming plan will rely heavily on input from the companies and organizations that comprise the complex networks that provide for economic well being, health, safety, and security of the American people.

The People and the Congress

This Plan is the result of the extensive work of many, throughout the Federal Government. In their name, we offer it to the American People and their elected representatives in the hope that together this country can improve upon the Plan, take the necessary steps, and defend America's cyberspace and all of our strength and people who now depend upon it.



Richard A. Clarke
National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism

EXECUTIVE SUMMARY

Defending America's Cyberspace

Introduction

The Federal Government and private sector cooperated during the millennial rollover event to provide a smooth transition into the Year 2000. The extensive preparations undertaken to avoid glitches and service disruptions to information systems paid off, and critical systems continued to operate without any major interruptions. That said, we must remember that we are in a very dynamic environment. The nature of cyberattacks and the needed preparations to protect information systems from future attacks are in constant flux. As new protective measures are developed and put into place, those who threaten us become more innovative. The Federal Government is currently assessing the Year 2000 experience to determine what aspects may have relevance for the future and for the continued protection against cyberattacks.

This document is the first attempt by any nation to develop a plan to defend its cyberspace. The President in Presidential Decision Directive 63 (PDD-63) directed its development. Designating it as "Version 1.0" acknowledges that the Plan is in the early stages of development and remains a work in progress.

The first version of the Plan largely focuses on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Subsequent versions of the Plan will incorporate a broader range of concerns contemplated under PDD-63, including the specific role industry and state and local governments will play—on their own and in partnership with the Government—in protecting privately owned infrastructures; the need to protect physical, as well as cyber-based, infrastructures from deliberate attack; and the examination of the international aspects of critical infrastructure protection. Comments by industry, Congress, state and local governments, and the general public are sought for improvements that could be included in these subsequent versions.

What Are Critical Infrastructure Systems and Assets?

Critical infrastructures are those systems and assets—both physical and cyber—so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety.

While PDD-63 calls for this National Plan to prioritize critical infrastructure protection goals, principles, and long-term planning efforts, its initiatives are explicitly designed to complement and focus existing Federal Computer Security and IT requirements.

The Threat

Every day in America, thousands of unauthorized attempts are made to intrude into the computer systems that control key government and industry networks: defense facilities, power grids, banks, government agencies, telephone systems, and transportation systems.

Some of these attempts fail. Some succeed. Some gain "systems administrator status," download passwords, implant "sniffers" to copy transactions, or insert trap doors to permit an easy return.

Some attacks are the equivalent of car thief "joy riders," committing a felony as a thrill. Others are committed for industrial espionage, theft, revenge-seeking vandalism, or extortion. Some may be committed for intelligence collection, reconnaissance, or creation of a future attack capability. The perpetrators range from juveniles to thieves, from organized crime groups to terrorists, potentially hostile militaries, and intelligence services. What has emerged in the last several years is an increase in the seriousness of the threat.

We know of foreign governments creating offensive attack capabilities against America's cyber networks.

America is vulnerable to such attacks because it has quickly become dependent upon computer networks for many essential services. It has become dependent while paying little attention to protecting those networks. Water, electricity, gas, communications (voice and data), rail, aviation, and other critical functions are directed by computer controls over vast information systems networks.

The threat is that in a future crisis a criminal cartel, terrorist group, or hostile nation will seek to inflict economic damage, disruption and death, and degradation of our defense response by attacking those critical networks. Director of Central Intelligence George Tenet testified to Congress: "This threat is very real."

Protecting Privacy and Civil Liberties

Infrastructure assurance goals can be accomplished in a manner that is consistent with a full range of civil liberty interests. In fact, some infrastructure assurance programs may have a positive impact on personal privacy and other civil liberties by enhancing the level of security in data and communications in networked environments.

The Federal Government has a positive obligation to protect the private information of its citizens that resides on its computers. The Government was entrusted with this information because American citizens believe their critical, personal information will be held securely within these systems.

The Federal Government recognizes the risk that technologies designed to protect information and systems, if not carefully utilized, could inadvertently undermine civil liberties. Even with the best of intentions, technology that protects against intrusions, when cast too broadly, might profile innocent activity. Where individual rights are at issue, careful consideration of all related issues is essential.

The legal landscape does not always offer clear guidance in areas of jurisdiction, security standards, and consent issues. Cyber-intrusions often present complicated legal and jurisdictional

issues. As a result, Government programs that protect infrastructures and civil liberties require careful planning, analysis, and input from all affected parties.

While all the proposals in the Plan have been developed in a manner fully consistent with existing law and constitutionally guaranteed expectations of privacy, portions of the Plan may give rise to concerns that personal privacy rights may be sacrificed in exchange for infrastructure assurance objectives.

Finding solutions to infrastructure assurance in a manner that is consistent with civil liberties is a dynamic process that must involve both Government and private sector communities. The process must recognize the complexity and importance of existing jurisprudence and work to structure new programs to prevent unintended consequences.

In that context, several key principles serve as a starting point for analyzing programs in the Plan; consulting with privacy communities to define acceptable solutions; conducting ongoing, rigorous, and thorough legal reviews of Plan programs; committing to comply with statutory and regulatory protections; government leading by example; reviewing applications of various legal privacy solutions; working with Congress; working with the National Academy of Sciences; focusing on education and awareness; and committing to the Principles of Privacy established by the Privacy Working Group of the Information Infrastructure Task Force.

How the National Plan Complements Federal Computer Security and Information Resources Management Responsibilities	
National Plan Implementation	**IRM Responsibilities**
Identify key nodes, critical infrastructure system dependencies within Federal Government.	**OMB: Use this information to manage Agency vulnerability and risk assessments, as required by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources (A-130)."**
Identify key national security assets and infrastructure systems.	**OMB: Use this information to incorporate infrastructure protection into Government Performance and Results Act (GPRA) Agency reports to OMB, as directed by PDD-63.**
Identify infrastructure system needs, dependencies, and on shared threats and vulnerabilities.	**Agency CIO/CFO: Use this information to focus budget proposals for critical infrastructure systems.**
Identify infrastructure system threats, vulnerabilities; identify where system threats and vulnerabilities are shared among Agencies.	**Agencies: Use this information to assess vulnerability and risk of Agency critical information systems, as required by A-130.** **OSTP and OMB: Use this information to focus research and development agenda.**
Identify and seek coordination with partners in private sector; identify shared infrastructure dependencies, and shared threats and vulnerabilities.	**CIO Council: Use this information to plan private sector outreach; utilize relationships built under National Plan structure.**

Federal Computer Security and Information Resources Management Responsibilities

Core responsibility for managing Federal computer security and information technology management falls to the Office of Management and Budget (OMB). In contrast to the National Plan's emphasis on national security systems and partnering with private industry, OMB has significant statutory responsibility for setting policy for the security of Federal automated information systems. Significant authorities include:

Issue and Focus	*Authorities*
Computer Security and Privacy—Ensure public access to data.	**Computer Security Act of 1987**
Performance and Results—Manage Agency performance of mission, including performance of its practices.	**Government Performance and Results Act of 1993**
Efficiency—Maximizing the use of information collected; minimizing the public burden for data requested.	**Paperwork Reduction Act of 1995**
Agency responsibility to manage Information Technology—procurement, investment, security. Creates CIO position within each Agency.	**Clinger-Cohen Act of 1996**
OMB implements these core principles through recommendations and oversight of the CIO Council.	**Executive Order 13011**

OMB's principal vehicle for implementing these requirements is OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources (A-130)." These responsibilities require OMB to oversee development of recommended practices and standards, vulnerability and risk assessments, and access to information by the public. OMB A-130 addresses each of these issues in great detail. During the past several years, OMB has issued other relevant materials, including those relating to:

- Internet and website privacy statement;
- recommended computer practices and standards; and
- major systems acquisitions.

The Plan: A Programmatic Overview

The goal of the Plan is to achieve a critical information systems defense with an initial operating capability by December 2000, and a full operating capability by May 2003. When that systems defense is in place, the United States should have achieved the capability to ensure that:

> *"Any interruption or manipulation of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."—**President Clinton in PDD-63***

To meet the ultimate goal established by President Clinton for defending the Nation's critical infrastructures against deliberate attack by 2003, the current version of the Plan has been designed around three broad objectives:

- ***Prepare and Prevent***: those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

- ***Detect and Respond***: those actions required identifying and assessing an attack in a timely way, and then to contain the attack, quickly recover from it, and reconstitute affected systems.

- ***Build Strong Foundations***: the things we must do as a Nation to create and nourish the people, organizations, laws, and traditions which will make us better able to Prepare and Prevent, and Detect and Respond to attacks on our critical information networks.

Version 1.0 of the Plan proposes 10 programs for achieving these objectives. They include:

Prepare and Prevent

- Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities

Detect and Respond

- Program 2: Detect Attacks and Unauthorized Intrusions

- Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law

- Program 4: Share Attack Warnings and Information in a Timely Manner

- Program 5: Create Capabilities for Response, Reconstitution, and Recovery

Build Strong Foundations

- Program 6: Enhance Research and Development in Support of Programs 1-5
- Program 7: Train and Employ Adequate Numbers of Information Security Specialists
- Program 8: Outreach to Make Americans Aware of the Need for Improved Cyber-Security
- Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8
- Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data

The remainder of this Executive Summary describes each program, along with its associated milestones.

The Plan, as approved by the President, provides broad direction and guidance for Agencies and Departments in the preparation of their budgets, but it is not a budget decision document. Decisions about Agency funding for protection of information systems will be made in the regular OMB budget formulation process, and subject to available appropriations.

Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities

"First, know thyself."

The First Program is for Government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks to attack, then develop and implement realistic programs to remedy the vulnerabilities, while continuously updating the assessment and remediation effort.

The initial necessary step in preparing a defense of critical information systems and computer networks is a thorough assessment of the potential critical infrastructure system assets, interdependencies, and vulnerabilities. We will continue to assess the capability of our opponents to disrupt our critical infrastructure. In addition, however, we must also depend upon identifying our critical infrastructures and assessing their vulnerabilities.

We do not yet have a sense of shared infrastructure system interdependencies. Our experience indicates that many, if not most, information systems are highly vulnerable to intrusions, especially those assisted by insiders. Despite the widespread use of firewalls and password systems, unauthorized intrusions occur with great frequency. Some firewalls have limited functionality or are not regularly updated, and techniques exist for getting around firewalls. Often users do not use complex passwords or do not change them regularly. Commonly available software programs can penetrate passwords. Users may also innocently use software given to

them by hackers, secretly installing a trap door on the entire system. Other users may violate rules and install unauthorized modems—so they may work at home—thereby unintentionally permitting others to enter the network.

Key components of identifying possible areas of exploitation on a computer network are:

- an identification of the most critical assets, based on clear distinctions between Agency/Department national security versus day-to-day mission criteria;

- an analysis of the shared interdependencies, whether within Government or between Government and/or the private sector;

- an assessment of network vulnerabilities by systems administrators, operators, security professionals, and the Chief Information Officer based on identification of critical assets and shared interdependencies; and

- an evaluation by outside experts trained in identifying success of mitigation efforts.

Recommended practices and standards for information systems security can assist organizations in their efforts to identify and address vulnerabilities. While much work has been done, a commonly accepted framework of information systems security recommended practices and standards is still in its formative stages. Close cooperation between the Federal Government, the private sector, and standards-setting bodies can lead to a more robust and accepted set of guidelines for organizations to follow in identifying vulnerabilities and prioritizing remedial actions. The Federal Government itself intends to strengthen its own system of information security recommended practices and standards in advancing the widespread use of such guidelines.

Recognizing that all vulnerabilities cannot be remedied immediately due to both technical and fiscal constraints, Government Departments and private sector groups must prioritize remediation efforts, based on the critical assets and interdependencies analysis throughout a 3-5 year period. Detailed funding requirements must be prepared by Chief Infrastructure Assurance Officers (CIAO), Chief Information Officers (CIO) and Chief Financial Officers (CFO) working together, and adopted by Cabinet members or Chief Executive Officers (CEO) and corporate boards of directors.

“An Internet year” is a term commonly used to mean three calendar months. Information technology is evolving so quickly, that those programs and plans adopted a year ago will likely bear little relevance to the technologies available now. As networks change, new vulnerabilities are introduced. As hackers explore systems, they discover vulnerabilities that were not previously known. Therefore, a continuous process is needed for reviewing the new vulnerabilities, the new protections, and standards and recommended practices as they become available. Special attention should be given to the danger of single-points-of-failure resulting from technology change.

Because assessments on critical assets, shared interdependencies, and vulnerabilities can provide an enemy a blueprint of how to attack, these assessments must themselves be protected. Steps need to be taken to ensure appropriate safeguards, including possible Legislation *(see Program 9).*

Federal Government Departments and Agencies will be required to continuously perform meaningful risk and vulnerability assessments and develop realistic, multi-year remediation plans. They will also be required to continuously update the assessments and plans. Similar updates are required to ensure information systems security recommended practices and standards remain relevant. The Federal Departments, which PDD-63 designated as Sector Liaisons, will work with the private sector to encourage similar ongoing assessment and remediation work.

Editors Note: *All milestones included in the Plan correspond to the milestone number as it appears in this Executive Summary regardless of what component plan it belongs.*

Program 1 Milestones

Milestone	Activity	Target Date
1.1	Federal Phase One Departments will perform initial vulnerability assessments and develop remediation plans. An Expert Review Team (ERT) will analyze the reports.	COMPLETED (February 1999)
1.2	Federal Phase Two Departments will, with the exception of NASA, perform initial vulnerability assessments and develop remediation plans. An ERT will analyze the reports.	COMPLETED (May 1999)
1.3	Federal Departments and Agencies will submit a multi-year vulnerability remediation plan with their FY2001 budget submissions to OMB and annually thereafter. The ERT will work with the Departments on implementation of their remediation plans.	COMPLETED (June 1999)
1.4	The CIO Council will create an interagency working group on Federal information systems security recommended practices whose primary focus will be to identify, coordinate, and consolidate ongoing government security recommended practice activities. The working group shall report at least annually to the CIO Council regarding recommendations for security practices. The group may also recommend to NIST modified Federal Information Processing Standards. NSA and NIST will continue to develop recommended practices in accordance with the Computer Security Act of 1987.	COMPLETED (November 1999)
1.5	The Federal Government will develop a pilot framework and database, with examples, for capturing *Practices for Securing Critical Information Assets.*	COMPLETED (December 1999)
1.6	Federal Departments and Agencies will ensure the timely installation of appropriate software patches and other fixes to computer systems vulnerabilities. As necessary, OMB will monitor the effectiveness of Agency processes.	February 2000

Milestone	Activity	Target Date
1.7	Enhance the Certificate and CRL Profile for use between Federal-PKI users and members of external PKIs through MISPC to address key management through publication of the MISPC, V2; and, enhance baseline for the interoperability of PKI components to address confidentiality (publish as MISPC V2) by establishing the Federal Bridge Certification Authorities.	February 2000
1.8	The Federal Government will complete the first version of the *Critical Physical Infrastructure Protection Plan*.	March 2000
1.9	The interagency working group on recommended practices will provide written reports, at least annually, to the CIO Council on recommended new and modified security practices. The CIO Council will publish each report following interagency review and comment.	June 2000
1.10	DoD Critical Asset Owners, Defense Infrastructure (DI) Sector Critical Infrastructure Assurance Officers and Installations will identify an initial cut of critical assets and conduct preliminary vulnerability assessments. In addition, DI Sector CIAOs will perform sector-level vulnerability assessments, and identify critical sector assets.	August 2000
1.11	Defense Sectors and DoD Critical Asset Owners will establish preliminary methodology and processes for physical security vulnerability assessments, technical assist visits, certification and accreditation results, personnel security incidents, and cyber incidents.	August 2000
1.12	The Federal Government will develop methodologies to identify critical infrastructure assets and shared interdependencies.	September 2000
1.13	DoD will complete a survey and review of the physical protection of its critical cyber systems, including both its classified and unclassified networks.	September 2000
1.14	Private sector Information Sharing and Analysis Centers could develop suggested guidelines for member corporations to perform Assessment and Remediation Programs.	FY 2000
1.15	The DoD will conduct an updated examination of the DoD Critical Infrastructure Protection Program to identify and recommend remediation of significant physical vulnerabilities of critical computer network related infrastructure.	FY 2000
1.16	Private sector Information Sharing and Analysis Centers could assess sector- or industry-wide shared vulnerabilities.	FY 2000
1.17	DoD will create organizational structures to identify and fix vulnerabilities; develop and deploy intrusion detection systems; and launch key innovative research and development projects.	November 2000

Milestone	Activity	Target Date
1.18	DoD Critical Asset Owners with their Sector CIAOs will provide remediation plans and resource the plans. In addition, DoD Installations will provide installation-level remediation plans with the Sector CIAOs and resource the plans.	November 2000
1.19	DoD Sector CIAOs will monitor response activities, coordinate appropriate sector mitigation and reconstitution activities, and provide support to the National Military Command Center (NMCC).	November 2000
1.20	DoD Sector CIAOs will resource and perform sector-level remediation and integrate and reconcile asset-level remediation plans within each sector.	December 2000
1.21	Federal Agencies and Departments should have assessed information systems vulnerabilities, adopted a multi-year funding plan to remedy them, and created a system for continuous updating. Private sector companies of every critical sector could do the same.	December 2000
1.22	Demonstrate the interoperability of PKI-aware applications, such as electronic mail, using the Federal PKI and the published *Security Requirements for Certificate Issuing and Management Components* for public review.	December 2000
1.23	No later than January 2001, Departments and Agencies, to the extent required under law, shall report to OMB and NIST on the degree to which they have adopted relevant security recommended practices and Federal Information Processing Standards (FIPS).	January 2001
1.24	The CIPIS will integrate and reconcile Defense sector-level remediation; review sector mitigation plans and business planning operations; review DI Sector reconstitution plans; draft integrated DI Sector reconstitution plans; and draft measures of effectiveness.	March 2001
1.25	Signed Electronic Mail: All electronic mail will be signed; encryption of mail is encouraged throughout DoD.	October 2001
1.26	Perform the first validation of a PKI component against the *Security Requirements for Certificate Issuing and Management Components.*	December 2001
1.27	DoD will issue its most secure Certificates/Tokens to all users in implementing its Public Key Infrastructure.	January 2002

Milestone	Activity	Target Date
1.28	Defense Sectors will complete development and application of risk management principles associated with infrastructure dependency and component criticality assessments to national Defense critical infrastructure. Complete task by: developing and implementing consistent Risk Management Framework; identifying sources of risks and uncertainties; identifying casual relationships; determining likelihood and range of consequences; assessing extreme events; constructing risk of extreme events; identifying tradeoffs; and identifying and analyzing options.	December 2002
1.29	The remediation plans should have eliminated the most significant known vulnerabilities in critical information systems networks in Government Agencies and key corporations. Ongoing vulnerability assessment and remediation will be underway.	May 2003

SCOPE NOTE
PROTECTING BOTH CYBER AND PHYSICAL CRITICAL INFRASTRUCTURES

Protecting the Nation's critical infrastructures has long been a subject of Government concern. Dams, bridges, tunnels, power plants, and other important physical structures have been specially protected for more than 50 years. In 1995, PDD-39 directed the Attorney General to lead a Government-wide effort to re-examine the adequacy of our infrastructure protection.

The Attorney General's review highlighted the lack of attention that had been given to protecting our cyber infrastructure: critical information systems and computer networks. The President's Commission on Critical Infrastructure Protection (PCCIP) was a direct outgrowth of that review. The PCCIP found major vulnerabilities in protection of cyber infrastructure and found no system or program to address it.

Thus, in PDD-63, the President stated his intent that the U.S. will eliminate significant vulnerabilities "to both physical and cyberattacks on our critical infrastructures, especially our cyber systems."

To readdress the physical vulnerabilities of non-cyber systems, the FBI, DoD, and other Agencies will review the 1995 efforts, updating them as required, and coordinating the FBI Key Asset Initiative and the DoD Critical Infrastructure Protection Program.

A new *Critical Physical Infrastructure Protection Plan* is being developed and will feature necessary initiatives and programs to ensure protection of these infrastructures. The DoD and FBI, working with the CIAO, are taking the lead on developing the plan. Once completed, a review of the crosswalks and linkages between the *National Information Systems Protection Plan* and this new physical protection plan will be created. Version 2.0 or later iterations of the cyber protection plan could then reflect that crosswalk review. These two plans may be integrated in the future.

Program 2: Detect Attacks and Unauthorized Intrusions

"Today, we don't even know when we are being attacked."

The Second Program installs multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers (first in DoD, then the Federal Intrusion Detection Network [FIDNet] in coordination with other Federal Agencies) will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks and assist sites in defeating attacks.

Our best efforts to identify and fix vulnerabilities will slow, but not stop, malicious intrusions into information systems. Commonly used software will continue to possess vulnerabilities. Interaction among different software and hardware combinations creates holes in security. Disgruntled employees with access to a system can often create significant damage without their unusual behavior being noticed until it is too late.

Given the vulnerability of systems and software, the number of potential target systems, and the frequency of unauthorized intrusions, the development and deployment of detection and monitoring systems are imperative. These intrusion detection systems are already in use in the Executive Branch and Congress. Networking intrusion detection monitors across Federal Departments and Agencies with a central capability to analyze system anomalies is a key next step in enhancing system security.

Examples of successful linkage of alarms are seen throughout society. For instance, an individual burglar alarm in a house is less effective if the alarm does not automatically sound at the local police detachment if there is an intrusion.

Installing Intrusion Detection Monitors and Defensive Detection Systems

Among the first steps necessary to detect unauthorized intrusions or activities on a network are the installation and implementation of highly automated programs, including the following four types of Defensive Detection Systems:

- intrusion detection monitors on either side of firewalls, which are regularly updated;
- access and activity rules for authorized users and a scanning program to identify anomalous activity by apparently authorized users;
- enterprise-wide management programs that can identify what systems are on the network, determine what they are doing, enforce access and activity rules, and potentially apply security upgrades; and

- techniques to analyze operating system code and other software to determine if malicious code, such as logic bombs, or other dangerous code such as trap doors (whether originally for malicious or benign purposes) have been installed.

The Plan calls for the installation of the "best of breed" program in each of the four types of Defensive Detection Systems where appropriate on critical information system networks. Such installation can be mandated within the Government. The Government may also share evaluations of such systems through Information Sharing and Analysis Centers (see *Program 4* below).

Networked Systems of Intrusion Detection Monitors

To protect critical Federal systems in civilian (non-DoD) Agencies, the Plan also calls for linking Defensive Detection Systems protecting individual Government systems with a central analytic cell at the General Services Administration's Federal Computer Incident Response Capability (FedCIRC) that will perform real-time analysis of system anomalies from multiple networks. The NIPC is notified for further action if Agencies or the FedCIRC determine there is sufficient indication of illegal conduct. As soon as any one site is attacked, word of the attack would be flashed where appropriate to all other sites.

With the current state of technology, this system—the Federal Intrusion Detection Network (FIDNet)—and other such networked monitoring systems require a combination of automated sensing and human management. The automated system allows for the efficient collection of data about system anomalies from key network nodes within Government networks. Currently, analysis of systems anomalies largely depends on human management at the Agency and by specially trained analysts at the GSA FedCIRC. With continued R&D, increasing amounts of the analysis will be automated using artificial intelligence tools. Automated tools for quickly updating systems defenses in the face of an intrusion are also needed.

FIDNet will become one of three linked systems, which together define the U.S. Government's critical systems' protection capabilities:

- the DoD Joint Task Force-Computer Network Defense (JTF-CND) has been created and is monitoring critical Defense networks and coordinating actions to restore functionality after an intrusion/attack;

- the National Security Incident Response Center (NSIRC) provides expert assistance to the JTF-CND, FIDNet, and NIPC in isolating, containing, and resolving attacks and unauthorized intrusions threatening national security systems. The NSIRC will coordinate its incident reporting and vulnerability assessments with the JTF-CND, FIDNet, and NIPC for attacks and intrusions directed against the national security systems; and

- for civil Federal Departments' critical information networks, a Federal Intrusion Detection Network (FIDNet) will be created, modeled on the DoD system, implemented and operated at the GSA. Consistent with legal limits and requirements, FedCIRC will coordinate with the NIPC when indications of illegal conduct require analytic assistance from or warning

notification through the NIPC's Analysis and Warning section, or criminal or national security investigation coordinated by the NIPC's Computer Investigations and Operations section.

The Department of Justice has preliminarily found that the FIDNet concept is consistent with the Electronic Communications Privacy Act. A comprehensive legal review—conducted by representatives of numerous Agencies—is underway to ensure that FIDNet, as it is developed, remains consistent with Government privacy and civil liberty policies and statutory and constitutional safeguards.

Program 2 Milestones

Milestone	Activity	Target Date
2.1	Establish analysis and response centers linking intrusion detection systems in the Air Force, Navy, Army, and DoD Agencies. Establish the National Security Incident Response Center (NSIRC).	COMPLETED (FY 1998)
2.2	Install the initial 500 intrusion detection monitors on critical DoD systems.	COMPLETED (December 1998)
2.3	Establish a DoD-wide hub for intrusion detection, the Joint Task Force-Computer Network Defense (JTF-CND).	COMPLETED (Spring 1999)
2.4	Release departmental cyber-security plan and realign DOE CIO office under the Office of Security and Emergency Operations.	COMPLETED (September 1999)
2.5	Initiate searches for malicious code on Federal systems.	FY 2000
2.6	Pilot an intrusion detection network (FIDNet) for civilian Federal Agencies, with 22 critical Federal sites connected by October 2000.	FY 2000
2.7	Upgrade access/activity monitoring and install enterprise-wide management systems where appropriate on Federal systems.	FY 2000
2.8	Complete R&D on handling 'scaling' and other issues on large intrusion detection networks with automated processing and adaptive capabilities.	October 2000
2.9	Develop and regularly update standards for detection systems.	October 2000
2.10	Upgrade firewalls and intrusion detection monitors where required in the Federal Government.	January 2001

Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law.

"People form governments to defend themselves from foreign enemies and domestic criminals."

The Third Program assists, transforms, and strengthens U.S. law enforcement and intelligence agencies to be able to deal with a new kind of threat and a new kind of criminal, one that acts against computer networks.

In the past, the overseas threat to our infrastructure in the homeland was from bombers, intercontinental missiles, and submarines. Those systems could be located and counted by intelligence agencies. Now, the threat to our infrastructure from computer-based attacks can originate from capabilities and locations that are much more difficult to find and assess.

U.S. Intelligence Agencies are giving high priority to collection of information on foreign information warfare capabilities and intentions, consistent with Executive Order 12333, Attorney General Guidelines, and Director of Central Intelligence directive protocols.

While it is vital that U.S. Intelligence attempt to collect information on potential foreign enemy plans and capabilities, cyber threats pose a different and more difficult challenge than intelligence collection about traditional military threats. The Intelligence Community is engaging in the process of developing new solutions to dealing with this difficult challenge.

Attacks on computer networks, whether physical or cyber, usually violate Federal or state laws. Proving that an attack has taken place, finding out who has done it, and proving their guilt requires new skills that seamlessly integrate law enforcement, intelligence analysis, and national security responses. The National Infrastructure Protection Center (NIPC) at the FBI is an interagency center using information from all sources, including open sources, the private sector, law enforcement, and the U.S. Intelligence Community, to provide early warning of attacks and to respond in part by gathering information necessary to identify the responsible party. Further, the NIPC has both law enforcement and Foreign Counter-intelligence missions, and operates under authorities that cover activities in both of these areas. The Center has representatives from Defense, Intelligence, the NSA, and other Federal Agencies and is taking the lead to develop and improve capabilities to determine when an attack has taken place, analyze the scope and origins of an attack, and find the perpetrator(s).

Warnings of possible attacks, and appropriate incident and vulnerability data, will be shared with the private sector and state and local governments. This information is critical in their efforts to improve their defenses against attack (see *Program 4*).

Building on the other programs, U.S. law enforcement agencies are tightening and improving domestic law enforcement mechanisms and tools. We are strengthening our capability to prosecute those who commit crimes on computer networks by increasing the number of technically trained prosecutors in the Department of Justice's Computer Crimes and Intellectual Property section, and in each U.S. Attorney's office through the Computer Telecommunications

Coordinator program. We are also working with trusted law enforcement counterparts from other nations to build a system of enhanced international cooperation, and develop a common approach to criminalizing unauthorized intrusions and attacks on critical cybersystems.

We are determined to ensure that those who seek to misuse cyber technology for criminal gains or other nefarious ends, whether they do so on behalf of nation states, terrorists, or criminal organizations, are found and punished. We must not let them escape justice because their criminal activity may have originated or passed through one or more foreign jurisdictions. At the same time, policies and programs must be developed consistent with existing rules and policies concerning the permissible roles of domestic law enforcement and national security agencies for domestic and foreign activities, respectively.

Program 3 Milestones

Milestone	Activity	Target Date
3.1	Increase the focus of Federal law enforcement and intelligence agencies in collecting, tracking, and analyzing information about cyber-threats and vulnerabilities to critical information systems.	COMPLETED (FY 1999)
3.2	The Intelligence Community, DoD, and Federal law enforcement agencies will sponsor a series of workshops on developing new techniques for information collection and analysis suited to addressing the threat of cyberattack.	FY 2000

Program 4: Share Attack Warnings and Information in a Timely Manner

"An attack on one shall be considered an attack on all."

When the "Solar Sunrise" attack on Air Force computers was first noted in February 1998, there were inadequate procedures or methods of knowing whether such attacks were ongoing against other DoD systems, key Federal networks, or critical private sector systems. Today there is a nascent system to do that. The Plan calls for a more effective nationwide system to pass information in real time about attacks, including:

- *Improved Federal information sharing:* In the immediate term, we need to do a better job with the data that we already have available. Collectively, Federal systems administrators have extensive data on anomalies and possible intrusions. These Federal systems administrators should send data on system anomalies to the Federal Computer Incident Response Capability (FedCIRC), including the enhanced capabilities of the FIDNet system. Indications of illegal activity or intrusions will be provided directly to the NIPC for analysis. The FedCIRC also serves as an important recipient and provider of incident data. Having access to all-source information, the NIPC and FedCIRC can combine this reporting with other information they have to determine patterns of intrusions or connections among seemingly random occurrences.

Within DoD, the National Military Command Center (NMCC) and the Joint Task Force-Computer Network Defense (JTF-CND) will receive, consolidate, and assess DoD Sector reports; develop DoD indications and report them to the NIPC; issue DoD warning; and receive, assess, and disseminate national warning.

- *ISACs:* For the private sector and state and local governments, the Plan encourages the creation of Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local governments and could receive warning information from the Government. As a result of a White House conference on "ISACs and Information Sharing," and several sessions hosted by Federal Departments designated by PDD-63 as Sector Liaisons (including meetings hosted by former Treasury Secretary Robert Rubin and Secretary of Energy Bill Richardson), several industry groupings have decided to create Information Sharing and Analysis Centers. Other industry groupings are in the process of evaluating proposals. *(See the accompanying boxes on the New Mexico Critical Infrastructure Assurance Council and the Financial Services ISAC).*

  The NIPC will provide ISACs with information about threats, vulnerabilities, and relevant incidents.

  Although in no way required, for those corporations that wish to do so, ISACs could also be a voluntary way to inform Federal Agencies about attempted intrusions and other attacks. ISACs might "sanitize" the data (e.g., by removing the name of the corporation). Companies are encouraged, however, to inform their local FBI field offices directly of computer attacks.

Banking and Finance Sector ISAC Opens For Business

On October 1, 1999, the U.S. Secretary of Treasury announced the opening of the banking and financial services information security facility, the Financial Services Information Sharing and Analysis Center (FS/ISAC).

The Center is a joint public-private industry initiative designed to facilitate the sharing of information about cyber-threats to the financial services industry. It enhances the industry's ability to prevent, detect, and respond to attacks on its technological infrastructure by providing an anonymous venue for rapid distribution of information about such threats.

Membership in the FS/ISAC is open to all members of recognized financial service associations. Currently, 12 organizations representing both private and public interests have signed letters confirming their interest in participating in the Center. The facility is managed by a private contractor and fully funded by participating corporations.

- *Removing barriers to information sharing*: Companies may wish to discuss possible system vulnerabilities with Government experts, but be deterred from doing so because of the possibility that information disclosed to the Government could become subject to a request

for public disclosure under the Freedom of Information Act (FOIA). Sensitive information on Government vulnerabilities should already be protected from FOIA exposure under existing law. In furtherance of this National Plan, the Critical Infrastructure Assurance Office and the Department of Justice co-hosted a July 1999 White House conference with public and private sector experts on Freedom of Information. Participants discussed the extent that FOIA issues may prove to be a possible disincentive to information sharing. An interagency working group has been tasked with recommending the full range of possible solutions with input from the private sector. Other legal concerns expressed by the private sector, including antitrust and liability issues, are being dealt with similarly.

- *FIDNet and JTF-CND:* As permitted by privacy and law enforcement restrictions, FIDNet and the JTF-CND incident detection systems will share incident data between themselves.
- *The National Security Incident Response Center (NSIRC):* The NSIRC will be provided data from both the FedCIRC and JTF-CND in order to conduct detailed incident analysis and vulnerability assessments. NSIRC vulnerability assessments will be used to develop hardware and software Computer Network Defenses.

Program 4 Milestones

Milestones	Activity	Target Date
4.1	DOJ and CIAO host a White House Conference Center meeting on the Freedom of Information Act and protecting information on critical systems' vulnerabilities.	COMPLETED (July 1999)
4.2	Create a 24-hrs capability for notification of computer attacks at the National Infrastructure Protection Center.	COMPLETED (FY 1999)
4.3	Develop mechanisms for the regular sharing of Federal threat, vulnerability, and warning data with private sector Information Sharing and Analysis Centers (ISAC).	FY 2000
4.4	The CIAO and GSA will sponsor a White House Conference for Federal CIRCs/CERTS to further coordination and the development of common operating systems.	FY 2000
4.5	Propose legislative changes (if needed) to assist the formation of Centers.	FY 2000
4.6	Cooperate with private sector groupings to establish ISACs in several key industries.	FY 2000 and ongoing
4.7	Create "test-bed" or prototype computer security information sharing programs at the statewide level and with multi-state authorities.	FY 2000
4.8	Establish additional Information Sharing and Analysis Centers.	FY 2000

New Mexico Critical Infrastructure Assurance Council

Prototype for State Government and Statewide
Public-Private Partnership in Protecting
Critical Computer Systems and Physical Infrastructures

The New Mexico Critical Infrastructure Assurance Council (NMCIAC) is a cooperative, private- and public-sector enterprise founded initially to further the exchange of information among the business community, industry, educational institutions, the Federal Bureau of Investigation (FBI), New Mexico state government, and other Federal, state and local agencies to ensure the protection of the critical infrastructure in New Mexico. NMCIAC addresses threats, vulnerabilities, countermeasures, and responses to infrastructure attacks, unauthorized system intrusions, and factors that may impact NMCIAC member organizations and/or the general public. Both physical and cyber protection are addressed through the referral and dissemination of information regarding threats to critical systems. NMCIAC is affiliated with the FBI's InfraGard/NIPC initiatives for cyber and physical protection.

It is the first and only all-volunteer statewide organization in the U.S., and serves as a prototype for similar organizations to be developed in the remaining 49 states. In its relatively short life span, the group has recruited 36 organizations representing both private and public sectors. NMCIAC uses a working group format to accomplish its stated objective. These groups are defined by critical infrastructure area: information and communications; utilities (natural gas, oil, electricity, and water); banking and finance; transportation; emergency management; emergency and government services; Information Sharing and Analysis Center; and management and operations.

NMCIAC has identified six principal tasks:

- Establish and manage a state-based Information Sharing and Analysis Center (ISAC);
- Form and operate an advanced, secure communication system;
- Identify and evaluate threat reduction, response, and recovery technologies;
- Institute and conduct a training, outreach, technology transfer, and technical assistance program;
- Develop and share a state-level model for critical infrastructure protection; and
- Manage and operate NMCIAC.

To meet these challenges and encourage participation, NMCIAC offers its members many benefits, including an intrusion alert network; a members only informational Web site; a vehicle by which to lobby for needed changes and improvements in the industry; training seminars to assist each member in carrying out his duties; and member-developed programs that can be implemented in each of their respective organizations.

NMCIAC's success serves a beacon for other industry and state and local government entities interested in working together to protect their critical information systems. The lessons learned through the cooperative efforts in New Mexico can benefit every sector of our society in the fight to maintain our critical infrastructures. In fact, NMCIAC officials are cooperating with Virginia officials to develop a similar program in that state.

What Information Sharing and Analysis Centers Could Do For Industry

The Plan calls upon industry associations or groupings to form industry-wide computer security centers known as Information Sharing and Analysis Centers to:

- share information among the corporations on the nature of vulnerabilities, attempted attacks, or unauthorized intrusions; such information could be "sanitized" by the Centers to protect the identity of a particular company;
- coordinate shared R&D requirements unique to the industry;
- examine industry-wide vulnerabilities and dependencies; and
- develop employee education and awareness programs about information security; and share employee training programs.

How the Government Will Help Information Sharing and Analysis Centers

The Plan calls for the Government to assist such Information Sharing and Analysis Centers by:

- providing near-real-time data on significant attacks, strategic assessments of the threat to networks, information about attack techniques being employed, and vulnerability information;
- coordinating Federal R&D in information systems security with that of industry, and helping to address needs not being met by market forces;
- providing materials and other support to education and awareness programs; and
- assisting in seeking changes to applicable laws on Freedom of Information, liability, and antitrust where appropriate in order to foster industry-wide Centers.

Program 5: Create Capabilities for Response, Reconstitution, and Recovery

"…isolate and minimize damage....restore required capabilities rapidly"

The Fifth Program is to limit an attack while it is underway and to build into corporate and agency continuity and recovery plans the ability to deal with information attacks.

Information warfare attacks may not be limited in their scope to isolated incidents. They may be directed at an entire industry or agency, a whole sector of the economy, a region of the country, or the Nation itself. With data on attacks flowing from the JTF-CND, FIDNet, and industry groups' Information Sharing and Analysis Centers, the NIPC will work with Federal Agencies and the private sector so that together, they can identify the scope of an ongoing attack.

Once a widespread attack has been identified, the Centers may work in concert with law enforcement and other agencies, to initiate a response, which could include recommendations to systems managers to implement pre-planned measures to:

- block access to their networks by suspect users;
- initiate "defense condition" security precautions not normally employed;
- apply new security software "patches" aimed at the attack technique being employed;
- isolate elements of the network;
- suspend operations of portions of the network; and
- commence operations of emergency continuity systems.

Simultaneously, law enforcement and other agencies would be attempting to locate the origin of the attacks and take appropriate measures to terminate them. The private sector and law enforcement are encouraged to consult on response so that the private sector reaction does not needlessly hamper or eliminate the possibility of investigation of the intrusion, attribution to the accountable parties, and if possible, prosecution of the offender.

The goal for Government and the recommendation for industry is that every critical information system have a response plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Corporate and Agency recovery plans have, in many cases, focused only or largely on physical disruption: floods, blizzards, or bombings that disable headquarters. The plans usually assume that operations shift to an alternate headquarters from which directions will continue to be given

over the existing corporate or Agency information systems network. Plans usually now include "back-up" computer databases in case the headquarters system is unavailable.

Recovery plans must now also be designed for contingencies when all or part of the information network is itself compromised. Alternative methods of passing minimal essential information must be available. Expert teams must be quickly available to assist in reconstitution efforts, including analyzing software problems disabling the network, designing alternative avenues, and reinitiating network operations.

The Y2K Information Coordination Center was created to coordinate the flow of information about possible Y2K-related disruptions during the recent millennial rollover. The Center, staffed by a mix of both Government and industry experts, also works with a system of National Information Centers (NICs) that collect information on the status of different sectors.

In PDD-67, the President directed every Federal Department and Agency to submit by the end of FY99 new continuity of operations plans. Those plans will include measures to ensure continuity of operations during any PDD-63 emergency.

The Federal Sector Liaisons will work with their counterparts in industry to encourage that corporate recovery plans adequately address information attack reconstitution. The Commerce Department's interagency Critical Infrastructure Assurance Office (CIAO) will sponsor a White House conference and an ongoing dialogue with the insurance and audit industries to develop a better understanding of risk management, recommended practices, and metrics.

Program 5 Milestones

Milestone	Activity	Target Date
5.1	Departments and Agencies will modify their continuity of operations plans to include contingencies involving and PDD-63 emergency.	COMPLETED (December 1999)
5.2	CIAO will sponsor a White House conference with audit and insurance industry representatives and Sector Coordinators focusing on business controls and the evolving role of the audit community in the Information Age.	FY 2000
5.3	JTF-CND and other Government Agencies will develop protocols and recommendations for additional defensive steps that would be taken on Government networks upon warning of information attack.	FY 2000
5.4	FEMA will initiate modernization of its emergency communications systems.	IOC: FY 2000 FOC: FY 2003

Program 6: Enhance Research and Development in Support of Programs 1-5

"Information Technology is progressing at the speed of Internet years, four for every calendar year."

The Sixth Program systematically establishes research requirements and priorities needed to implement the Plan, ensures their funding, and creates a system to ensure that our information security technology stays abreast with changes in the threat and in overall information systems. It also creates an Institute for Information Infrastructure Protection (I^3P) to fill the gaps in CIP research technology development, which are not being met by private sector market demands or Government Agency mission objectives.

Many of the tasks required in the first five steps of the Plan cannot be performed well or, in some cases, cannot be performed at all with today's technology. The interagency Critical Infrastructure Coordination Group (CICG) has created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works with Agencies and the private sector to:

- gain agreement on requirements and priorities for information security research and development;
- coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;
- communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and
- identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, led to the Administration budget request for FY2000 of $500M for critical infrastructure protection research (*see Annex B*). Among the priorities identified by the process are:

- technology to support large-scale networks of intrusion detection monitors;
- artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;
- methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster;

- technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and

- technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

Institute for Information Infrastructure Protection

In R&D and other key technical areas, neither private sector market demands nor Agency mission objectives fully meet the Nation's requirements. The I^3P will fill these gaps, supporting research and technology development to protect our critical information and telecommunications infrastructures from attack or other failures. It would also provide demonstration and development support in key areas like benchmarks and standards, and curriculum development.

The idea for an Institute originated in December 1998, when the President's Committee of Advisors on Science and Technology (PCAST) proposed to the President that the Government establish a new, not-for-profit institute to address R&D issues associated with information infrastructure protection.

The Institute would have only a small expert staff, which would carry out its missions by funding and tasking existing organizations or groups, similar to how the Defense Research Projects Agency (DARPA) operates. The Institute would supplement, not absorb, existing research and world coordinate its information infrastructure protection activities closely with ongoing efforts in the Federal Government, the private sector, and academia.

Through the Commerce Department's National Institute of Standards and Technology (NIST), the Institute would have close working ties to both industry and concerned Federal Agencies. To ensure coordination and relevance to Federal priorities, the Institute would report to a Federal Coordinating Council consisting of the President's Science Advisor, the OMB Deputy Director, the NSA Director, the DARPA Director, the NIST Director, the NSF Director, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism (NSC). I^3P would also seek industry guidance from the National Infrastructure Advisory Council (NIAC) and Sector Coordinators. Private corporations and Federal Agencies would be encouraged to also fund and support projects or to lend in-kind support.

CICG R&D Sub-Group Sponsored Conferences in 1999-2000

The CICG R&D Sub-Group is sponsoring a number of workshops on focused, cross-cutting R&D themes:

- Intrusion, Malicious Code, and Anomalous Activity Detection (February 22-23, 1999)
- Interdependencies Among Critical Information Systems Infrastructures (August 11-12, 1999)
- Hostile Code (TBD)
- Insider Threat (TBD)
- Intrusion Detection (TBD)
- Reconstitution/Recovery (TBD)

Program 6 Milestones

Milestone	Activity	Target Date
6.1	Coordinate Federal critical infrastructure protection R&D for the FY2000 budget and subsequent budget years. Identify R&D required to implement the Plan, develop a multi-year funding strategy, and include the first year's requirements in departmental budget requests for FY2001.	COMPLETED (June 1998)
6.2	OSTP will annually update the Federal Government critical infrastructure protection R&D priorities, in consultation with the private sector and academia.	September 1999 and ongoing thereafter
6.3	Hold conferences with industry, academic, and government experts on the major R&D priorities in support of the Plan, and establish public-private mechanisms to coordinate Federal R&D in critical infrastructure protection with private sector efforts. Coordinate efforts and resources with the Program 7 initiative in personnel and training to build and bolster the development of research enabling skills among graduate and undergraduate students.	December 1999 and ongoing thereafter
6.4	Identify target dates for maturation from research into acquisition for major projects required to support the Plan.	January 2000
6.5	Evaluate creating a central R&D Federal fund to support cross cutting projects and ensure coordinated public-private research for the FY2002 budget and beyond.	March 2001
6.6	Creation of the Information Infrastructure Institute (I^3) with funding of multiple research projects.	FY 2001

Program 7: Train and Employ Adequate Numbers of Information Security Specialists

"We just don't have the trained people."

The Seventh Program surveys the numbers of people and the skills required for information security specialists within the Federal Government and nationwide, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Nationwide, evidence suggests a growing danger of a shortage of skilled information technology (IT) personnel. Within the subset of information systems security personnel, the shortage is acute. Within the Federal Government, the lack of skilled information systems security personnel amounts to a crisis. This shortfall of workers reflects a scarcity of university graduate and undergraduate information security programs. In addressing these problems, we will leverage the ongoing efforts made by the Defense Department, National Security Agency, CIO Council, and various Federal Agencies.

The Federal Cyber Services (FCS) training and education initiative introduces five programs to help solve the Federal IT security personnel problem.

- *The Completion of an Office of Personnel Management IT occupational study*. This study will help identify the number of IT positions in the Federal Government, the core competencies needed for these positions, and the training and certification requirements for these positions.

- *The development of Center(s) for Information Technology Excellence (CITE)*. These Centers will train and certify current Federal IT personnel and help maintain their skill levels throughout their careers. These Centers will leverage the significant progress made by the Defense Department and other Federal Agencies on this issue.

- *The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT workers and security managers*. This program will fund up to 300 students per year in their pursuit of undergraduate or graduate degrees in the information security field. In return, the students will serve in the Federal IT workforce for a fixed period following graduation. The program will also have a meaningful summer work and internship element. An important part of the SFS program is the need to identify universities for participation in the program and assist in the development of information security faculty and laboratories at these universities.

- *The development of a high school recruitment and training initiative*. This program would identify promising high school students for participation in summer work and internship programs that would lead to certification to Federal IT workforce standards and possible future employment. This effort will also examine possible programs to promote computer security awareness in secondary and high school classrooms.

- *The development and implementation of a Federal INFOSEC awareness curriculum*. This effort is aimed at ensuring the entire Federal workforce is developing computer security literacy. It will leverage several outstanding existing Federal Agency awareness programs.

Program 7 Milestones

Milestone	Activity	Target Date
7.1	Begin university outreach effort to promote SFS program. Develop certification requirements for SFS candidates and begin holding seminars to recruit potential candidates. Develop proposals for any additional authorities required.	January 2000
7.2	Complete a review of Federal-wide information systems security training and education programs to identify existing programs and any gaps or redundancies.	March 2000
7.3	Establish the standards, accreditation requirements and guidelines for a university to apply for and be selected to participate in the SFS program.	April 2000
7.4	Using DoD and private sector models, develop Federal IT security worker certification programs for system administrator and ISSOs, and the training programs needed to meet these certification goals.	May 2000
7.5	Develop and distribute the Federal workforce INFOSEC awareness curriculum. Maintain the program at a CITE, which will periodically review and upgrade the content.	March 2000
7.6	Establish the standards that institutions will have to meet to be designated as CITEs.	May 2000
7.7	Design and implement the high school and secondary school outreach programs to include conferences, summer work and internships.	May 2000
7.8	Designate the universities selected to participate in the first year of the SFS program.	May 2000
7.9	Complete the OPM-led study of information systems security occupational needs within the Federal Government. This will provide reliable data for recruitment, marketing, selection, pay, and competency development for Federal IT security professionals.	May 2000
7.10	Conduct a pilot information systems training program for prospective SFS faculty. This will be the precursor to our faculty development program.	Summer 2000
7.11	Recruit SFS graduate and undergraduate college students for the first year beginning January 2001, and 300 students for each subsequent year.	Fall 2000
7.12	Identify, designate and resource the CITEs. The Centers will develop, distribute and provide high caliber information systems security training and certifications for Federal IT workers; and offer technical certification and training programs to SFS and high school program students on their summer work programs.	October 2000
7.13	Enroll the first SFS program students.	January 2001
7.14	First graduates of SFS program enter Federal IT workforce.	May 2002

Program 8: Conduct Outreach to Make Americans Aware of the Need for Improved Cyber-Security

"Action follows understanding."

The Eighth Program will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyberattack.

Defending America's cyberspace will require action by all Americans—business leaders, education and other private sector institutions, the government (Federal, state, and local), and ultimately, the general public. A foundation for the many actions outlined in the Plan is the understanding and awareness of the new threats posed to our information systems, and the need for action.

There has been—so far—no "electronic Pearl Harbor" to galvanize public awareness about the need for action. Nor do many Americans appreciate the extent to which our economy and national security now depend on computers and information systems—oftentimes their functionality is hidden from everyday life.

Consequently, a broad-reaching awareness effort is needed. In its initial phase, this will include at least three elements:

- educating America's children about cyber-ethics and appropriate behavior and use of the Internet and other communications tools through the *CyberCitizens Program*;

- forging a partnership with America's corporate and information technology leaders, the *Partnership for Critical Infrastructure Security*, in which we jointly acknowledge the need to take specific action to improve our Nation's cyber-security in the private sector and the government, and join together in a nationally recognized program; and

- ensuring that Federal employees are themselves a model of awareness of the need for information systems security.

A fourth element would be added over time:

- building on the above elements, extending our awareness campaign to reach other private organizations and the general public.

These actions are a foundation for ensuring the national commitment to proactively defending America's information based infrastructures.

Program 8 Milestones

Milestone	Activity	Target Date
8.1	Educate America's children about appropriate behavior and ethics in using computer systems by creating the CyberCitizens Program.	COMPLETED (May 1999)
8.2	Increase corporate and government awareness of the threat to critical information systems and computer networks by creating a public-private *Partnership for Critical Infrastructure Security* and initiating an awareness campaign.	February 2000
8.3	Begin mandatory cyber-security awareness briefings to all Federal Government personnel with access to sensitive information systems, upon entry into service and on at least a bi-annual basis.	March 2000

Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8

"Just as the Government must form a partnership with private industry, the Executive Branch and Congress must work closely together to defend our Nation's critical infrastructures."

The Ninth Program develops the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation between the Federal Government, including Congress, and private industry.

The President has proposed initiatives and directed Federal Departments and Agencies to make their own critical systems secure and work to build a partnership with the private sector to protect our Nation's infrastructures. He submitted a $1.501 billion budget for FY2000 to defend our critical infrastructure. We cannot achieve these goals except in close cooperation with the Congress.

Congressional members and committees already have demonstrated that they share our perception of the potential dangers from attack on our Nation's critical cyber-driven systems, and give high priority to taking protective actions. We are reviewing existing laws, previously introduced legislative proposals, and developing a package of new proposals designed to promote security of critical infrastructures.

As identified in the other programs, we may need new legislation to build the cornerstone partnership between industry and the Government. In order to facilitate formation of private sector Information Sharing and Analysis Centers and information sharing in the private sector and with the Government, we need to ensure our ability to protect sensitive information and allay potential liability and antitrust concerns associated with sharing such information by and with private industry.

We are also examining the need for new legislative authorities in order to implement effectively certain initiatives in the National Plan. Keeping in mind the overarching need to protect the civil liberties and privacy of our citizens, we will develop legislative frameworks to promote interim and full operating capability to protect critical systems. We need Congress' support for the

President's budget to fund Program 1-8 initiatives. Our success in meeting the milestones established in the National Plan will depend upon the level of funding provided.

We look forward to continuing the productive dialogue with Congress on the best approaches and mechanisms to protect critical systems and to its active participation in developing future versions of the National Plan.

Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data.

"…the right of the people to be secure in their persons, houses, papers, and effects..."

The Tenth Program is incorporated in every other program and is making what we do in the protection of critical cyber systems conform to Constitutional and other legal rights.

While safeguarding our critical infrastructures is vital, protecting our civil liberties is paramount. All the proposals in the Plan have been developed in a manner fully consistent with existing law and expectations of privacy. The Plan calls for an annual public-private colloquium on Cyber Security, Civil Liberties, and Citizen Rights to ensure that those implementing the Plan remain sensitive to civil liberties and that they share their proposals on cyber security with those inside and outside of Government with expertise and concern for citizen rights.

The National Infrastructure Assurance Council (NIAC), a board of individuals from outside of the Federal Government, will be asked to also conduct an annual review of implementation of the Plan relative to civil liberties, privacy rights, and proprietary data protection.

The design of the Plan incorporates privacy protections established by Fourth Amendment jurisprudence. Any action by the Government to search a citizen's computer or the content of electronic communications must be in accordance with existing laws, such as the Electronics Communications Privacy Act. Citizens entering sensitive Government property, including Websites, should be advised if monitoring of their activity on the site is a condition of entry. The Plan calls for a system to ensure appropriate warnings are in place and are clear whenever a sensitive site is subject to monitoring.

The U.S. Government has been working with the private sector to develop enforceable rules for privacy protection to ensure that Internet users are notified of what information is collected and how it will be used, an opportunity for the person to choose how his or her information will be used, an assurance that the data will be secure, and an opportunity for reasonable access to the information and mechanisms for recourse if their information is used improperly.

Program 10 Milestones

Milestone	Activity	Target Date
10.1	The Federal Government, working with outside organizations, will initiate an annual public-private colloquium on Cyber Security, Civil Liberties, and Citizens Rights.	FY 2000
10.2	The NIAC and other appropriate authorities will conduct an annual review of the Plan's implications for civil liberties, privacy rights, and proprietary data. It will additionally review other relevant Government and private sector initiatives, and Government treatment of proprietary data, to further more comprehensive information sharing.	FY 2000