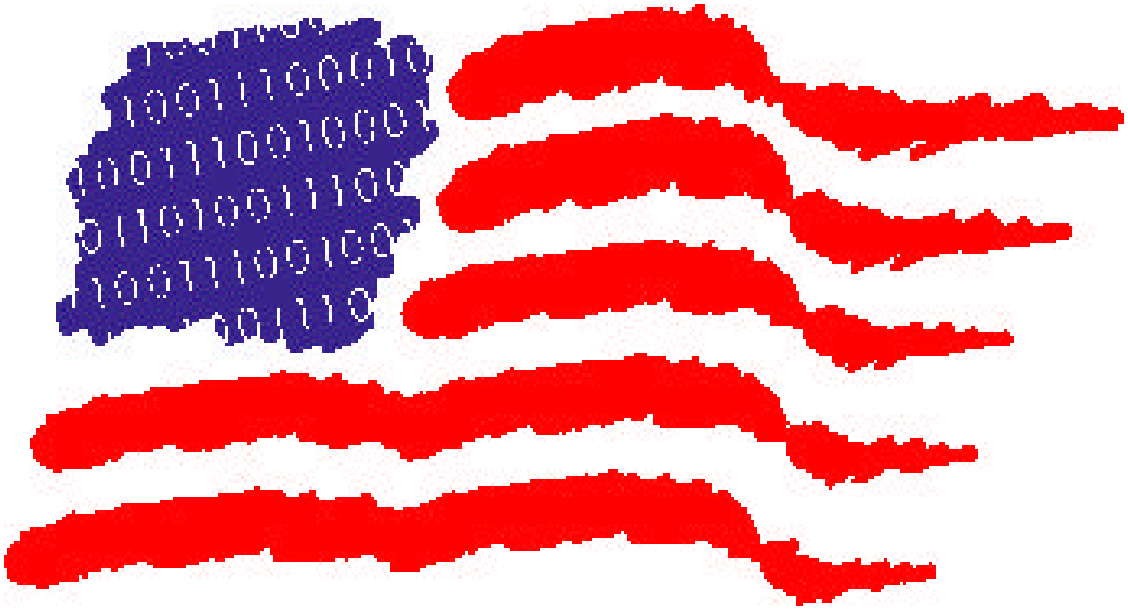
Defending America's Cyberspace



National Plan for Information Systems Protection

Version 1.0

An Invitation to a Dialogue

The White House

2000

NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION

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 in 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. The Government will not, however, 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

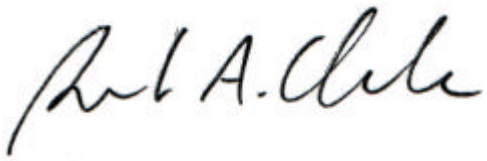
As you will see in the text, the Plan will build a defense of our cyberspace relying on new security standards, multi-layered defensive technologies, new research, and trained people. Of all of these, the most urgently needed, the hardest to acquire, and the *sine qua non* for all else that we will do, 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 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, 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 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 (January 2000)

Milestone	Activity	Target Date
1.6	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
1.7	The Federal Government will complete the first version of the Critical Physical Infrastructure Protection Plan.	June 2000
1.8	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
1.9	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
1.10	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
1.11	The Federal Government will develop methodologies to identify critical infrastructure assets and shared interdependencies.	September 2000
1.12	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
1.13	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.	FY 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

Milestone	Activity	Target Date
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
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 causal 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 is 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 support 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, 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 will be required to 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, including communications and financial services, 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 ISACs.	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.

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.

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 Institute for Information Infrastructure Protection (I^3P) 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 required 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 for SFS candidates and develop 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.	May 2000
7.6	Establish the standards that institutions will have to meet to be designated as CITEs.	June 2000
7.7	Design and implement the high school and secondary school outreach programs to include conferences, summer work and internships.	July 2000
7.8	Designate the universities selected to participate in the first year of the SFS program.	Summer 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 the Federal IT workforce.	Summer 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: 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*.	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. Congress supported many of these initiatives by including $1.737 billion in the FY 2000 enacted budget.

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 future

President's budgets 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

1. THE THREAT TO AMERICA'S CRITICAL INFRASTRUCTURES

We are at risk. The United States depends more on computers today then ever before. The pace of the technological drive to install computer controls in every critical infrastructure far outstrips our potential to design computer security software, train information technology security personnel, or develop and promulgate computer security recommended practices and standards. We have created a gaping vulnerability in our national security and economic stability. This affects not only our computer-controlled systems for electrical power, telecommunications, and nearly every utility, but also the vital databases that maintain our medical data, criminal records, and proprietary information. We are vulnerable to mischief-making hackers, hardware and software failures, cyber criminals and, most alarmingly, to deliberate attack from nation states and terrorists.

Consider the following incidents:

- A communications satellite above Kansas tumbles out of control. The pagers for more than 35 million Americans cease to function.

- Telephone service for a large region is cut off—blinding a major regional airport and endangering airplanes in their final approach.

- Two of America's largest cities have their 911 service disrupted, causing confusion, slow response, and potentially, needless deaths.

- Widespread intrusions into Army, Navy, Air Force, and DoD logistics and support computer systems are discovered during the middle of our February 1998 confrontation with Iraq. There is no clear idea of where the intrusions were coming from, how long they had been occurring, or what information had been removed or compromised.

- A new computer virus moves rapidly across the Internet, overloading systems with superfluous e-mails and shutting down major portions of corporate and government systems.

All of these events have occurred—not on the same day, and not all the result of deliberate action by America's adversaries—but all within the last 36 months. Consider the business and political implications if the U.S. were facing major foreign policy challenges, preparing to deploy our diplomatic and military strengths, and these events were tied to our adversaries—and to their ultimatum that the U.S. change its policies or else more were to follow.

The extent of these computer intrusions, attacks, and vulnerabilities is pervasive and includes our military, Federal, and civil infrastructures. No one is immune from computer network attack:

- Deputy Secretary of Defense Dr. John Hamre recently testified, "The world is an increasingly dangerous place. As we've improved our ability to monitor network activities, the number of probes, intrusions, and cyber events we can observe continues to increase. We now are detecting 80 to 100 events daily. Of these, approximately 10 will require detailed investigation."

- In 1998, a telecommunications company installed an intrusion detection system on their Internet connection and discovered nearly 4,000 intrusion attempts per month. While many were harmless scans, several hundred each month were aggressive attempts to enter their databases and remove telephone card numbers.

- In 1998, a civil aviation company was attempting to assess its computer vulnerabilities. The red team assisting them was able to crack 90 percent of their servers and access their payroll data, and more critically, their flight data input program.

- In response to U.S. military action in March 1999, five non-DoD Federal Agency computer systems were simultaneously attacked with either email "spamming" or attempts to modify and vandalize web pages.

Please see the table on page 3 for additional information on cyber events recorded since 1986.

Since the beginning of the 20th century, military doctrine has made destroying or disrupting the supply, communications, and economic infrastructures that support military power nearly as important as attacks on military forces themselves. While America has traditionally been largely beyond the physical reach of our adversaries, the computer age has provided potential adversaries with a whole new range of options. Our infrastructures are now at risk in ways that even 10 years ago might have seemed far-fetched.

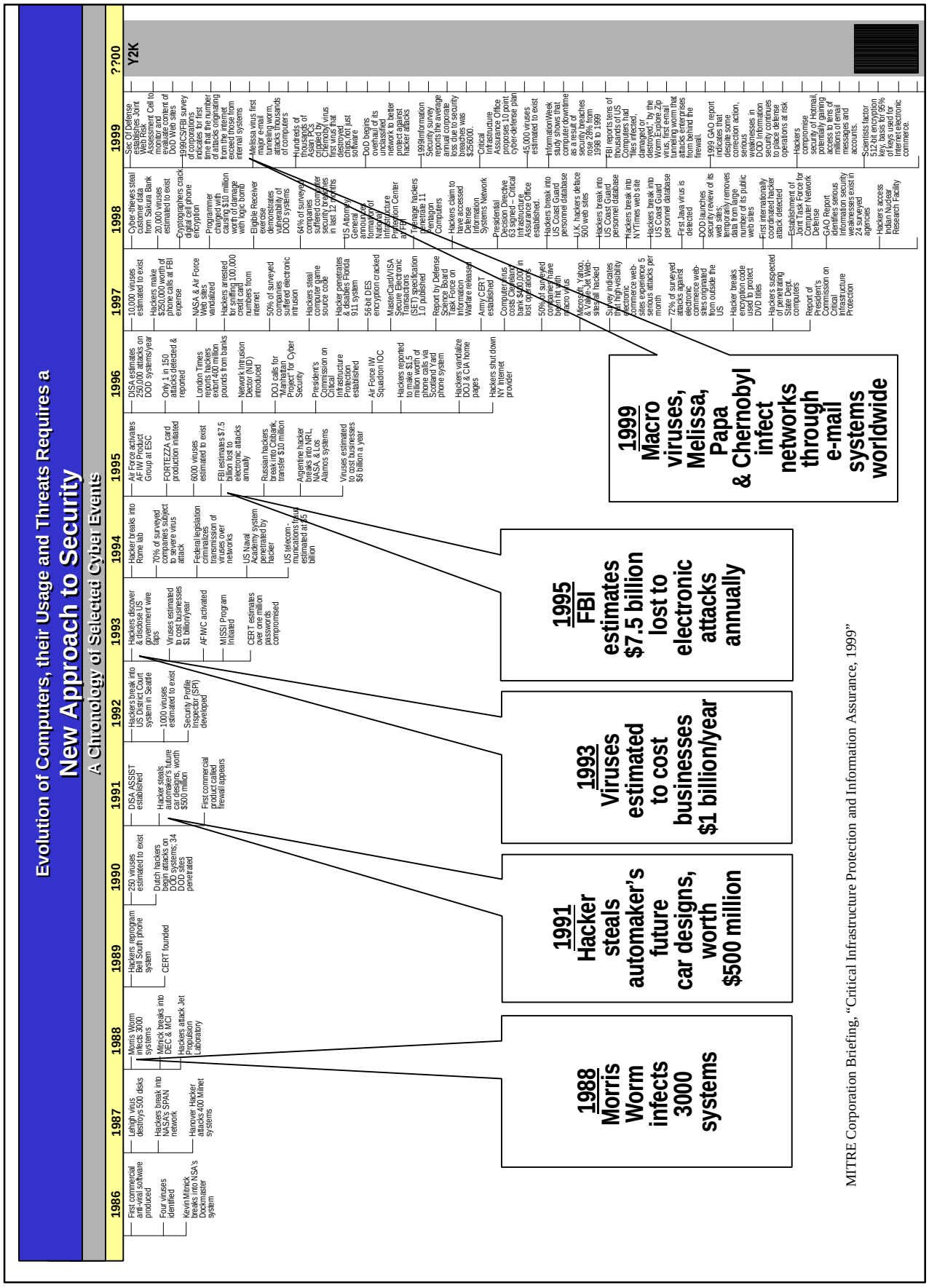
The Nation depends on interlinked information systems to run our telecommunications, power, transportation, financial, and national security functions, among others. With few exceptions, these networks are vulnerable to disruption and intrusion by technology-savvy groups. Increasingly, these networks are at risk as targets for America's adversaries. Business networks, at least as much as Government networks, are at risk.

We can act now to protect ourselves, or we can act later after events galvanize concern. But if we delay, the fundamental combination of increasing dependence, increasing vulnerability, and increasing risk will make the eventual consequences far worse for our lack of action now.

Increasing Dependence on Information Networks

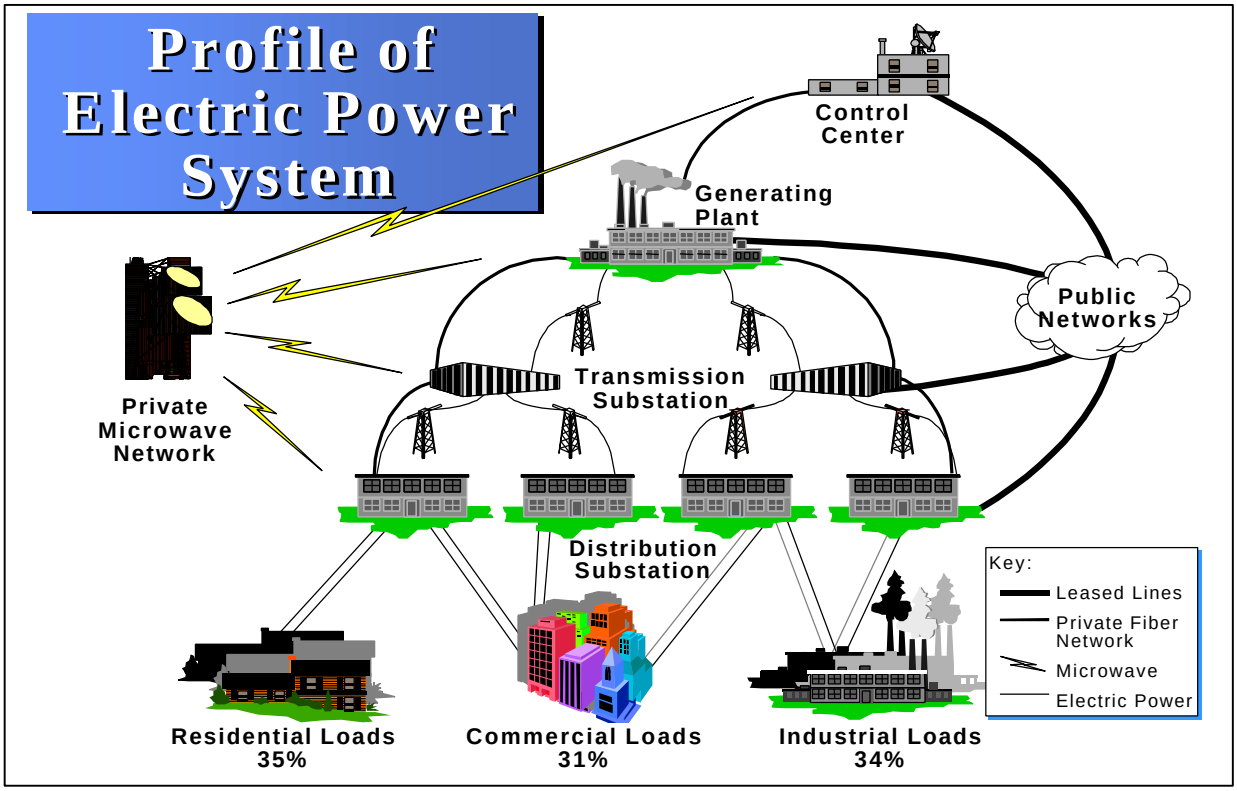
Like nowhere else, the United States is building up and fully exploiting the information economy. Manufacturers, financial institutions, transportation providers, countless other businesses, and the Federal, state, and local governments have all seized upon and continue to build the information networks that enable increased efficiency, cost reductions, and new and desirable services.

For example, producers and suppliers now use electronic links to lower costs through just-in-time manufacturing. Electric power and telecommunications providers have networked and interlinked their control systems to provide faster and cheaper services. Interconnected computer networks now often control the flow of power, water, financial services, and transportation services. Governments at all levels also rely on the same networks and infrastructures to provide essential services.



MITRE Corporation Briefing, "Critical Infrastructure Protection and Information Assurance, 1999"

No infrastructure has embraced the computer revolution more aggressively than electrical power. More critically, the electric power infrastructure is the life-blood for all other national infrastructures, and therefore its security and assurance is the key to our national security and economic stability, and guarantee the provision of our emergency medical, fire, and police services. Any vulnerability in the electrical power grid must be aggressively identified and corrected.



Through information networks, businesses and governments have achieved significant efficiencies and a new range of service offerings. But at some point in this information technology revolution, without making a conscious decision to do so, we created both corporate and national dependencies on these new systems. The economic strength of the Nation, the profitability and viability of many businesses, and the functioning of the Federal Government, are now dependent on the reliable operation of these complex networks.

Extensive Vulnerabilities in Information Networks

Deliberate intrusions into many networked systems are cheap, quick, and easy. Many of the vulnerabilities of our information infrastructures are widely known with intruders sharing this information over the Internet or in other ways. Numerous powerful attack methods have been automated in sophisticated ways and cyber-burglar tool kits are easily found on the Internet. Anyone intent on attacking our information infrastructures can do so with only a minimal investment in equipment, a moderate level of technical skill, a collection of tools that can be easily assembled, and knowledge of vulnerabilities and technologies that can be found on the Internet and other open sources.

There is little risk to cyber intruders. Unlike attacks against physical infrastructures, cyberattacks against information networks do not require physical proximity. Attacks can come from anywhere in the world, over the Internet, other networks, and dial-up lines, used either singly or in combination. By launching attacks across a span of communications systems and computers, intruders can effectively disguise their identity and location. Tracing these attacks is difficult and time consuming.

Cyber-intruders can easily create diversions that disguise their true intent and allow their attacks to achieve their desired impact. Through the use of viruses, network worms, Trojan horses, computer time bombs, and other forms of automated attacks, intruders can easily disrupt the operations of thousands of organizations and networks. While this is a problem in its own right, cyber-intruders can use these activities to divert the focus of system and network operators, security incident response teams, and investigators away from their true targets. Attacks against critical systems could easily go unnoticed when the background noise reaches high levels

*"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks."—**Foreign Government Newspaper***

Information Age Threat Spectrum

Increasing Risk—Growing Lists of Potential Cyberattack Protagonists

Today, the capabilities needed for an infrastructure attack may be no more than a personal computer and the skill in using it. Such adversaries do not have to operate from a large military-industrial complex that can be monitored by our highly sophisticated and multi-capable intelligence apparatus. The type of attack that concerns us now could come from a computer located anywhere—in a hostile or friendly nation, or even in the United States. It is within the potential of those with criminal or hostile intent to electronically deny us access to critical information networks, deceive us through manipulation or alteration of our information systems, or conduct traditional and economic espionage.

U.S. adversaries span a wide range. Beginning in the 1970s, we learned the painful truth that some of our adversaries are not nation-states. These non-state actors include terrorists, narcotics traffickers, and international criminals. Their opposition to U.S. policies, goals, and values will not come in the form of a diplomatic demarche or overt military confrontation. A successful cyberattack on U.S. infrastructures is well within their means, and would likely suit their ends.

Nation-States

We know of several nations developing information warfare capabilities. Obviously, not all of these are robust or mature programs, but Intelligence estimates that these countries are developing aggressive Computer Network Exploitation (CNE) and/or Computer Network Attack (CNA) capabilities. While few talk about their capabilities publicly, some have discussed the value of CNA programs in the open press.

*"An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the U.S. economy. If we overlook this point and simply rely on the building of a costly standing army…it is just as good as building a contemporary Maginot line."—**Foreign Government Newspaper***

We also know that certain countries have specifically targeted the United States in their information warfare planning efforts. Potential adversaries will attack the United States' critical infrastructures in order to achieve one of three main objectives: assist government-sponsored companies in acquiring an advantage over U.S. competitors; damage the economic stability of our nation by targeting our financial or industrial resources; or damage our national security by conducting military or intelligence operations.

*"While maintaining our nuclear deterrent potential at the proper level, we need to devote more attention to developing the entire range of means of information warfare."—**Foreign Government Leader***

Economic Competitors

According to President Clinton's *1998 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, a number of countries target U.S. industrial and economic information. Not only is such espionage conducted by official intelligence organizations, but also major foreign industrial sectors play a prominent role in their nation's business intelligence efforts. They actively target U.S. citizens, firms, industries, and the U.S. Government to steal advanced critical technologies, trade secrets, proprietary information, and the results of research and development initiatives in support of their own priorities and agendas. This threat has been developing for some time.

Criminals

While the international aspect of financial cyber crime has important national security and economic stability implications, in terms of financial loss to U.S. companies it pales in comparison to the impact caused by computer criminal activities. Credit card companies, telephone companies, and financial institutions all operate in the face of an increasingly aggressive cyber-criminal environment. An Ernst and Young/*InformationWeek* survey found that more than 72% of U.S. corporations found an increased security threat to their data in the past five years.

Potential use by organized crime groups, both domestic and international, is an immediate and increasing concern not only for United States law enforcement, but also for the worldwide law enforcement community. These criminal organizations are exploiting high technology for a variety of purposes, not the least of which is financial gain and competitive advantage, as well as a desire to gain sensitive law enforcement information that is resident in police computers and networks.

The extent of attacks on U.S. corporations is difficult to estimate. In some cases, companies do not even recognize the extent of the losses, in others, they fear the negative publicity. The 1996 Senate minority report captured the general corporate feeling well:

*"The commercial sector is loath to report computer intrusions for fear of affecting customer or shareholder confidence. Company insiders confirm to the Staff that they experienced intrusions on a regular basis, but fear reporting them to the government and other agencies that might put them into a public record."—**Senate Minority report, "Security in Cyberspace" Hearings***

Hackers

Some time ago, hackers were characterized as computer-savvy teenagers and over-zealous programmers who were unlikely to engage in criminal or malicious activities, and were thought to be motivated by curiosity and technical challenges. Unfortunately, a new generation of hackers appears to be motivated more by greed or malice than by simple intellectual curiosity. Hackers have begun to realize both the value of the information contained in computer systems and the potential profit that can be derived by stealing telecommunications services and committing computer fraud. Today's hackers insert malicious code and launch denial-of-service attacks for a wide variety of reasons, including greed, political goals, theft of information, or just

plain mischief making, and their ability to cause significant damage to computer systems has greatly increased.

SOLAR SUNRISE

WHAT: Hacking incident during which DoD computer systems were systematically attacked

WHEN: 1 to 26 February 1998

WHO: Two 16-year-old boys in California assisted by an Israeli teenager

ATTACKS:

- Targeted DoD Network Domain Name Servers, exploiting a well-known vulnerability on the SOLARIS Operating System
- Widespread
- Appeared to be carefully coordinated
- Targeted key parts of DoD unclassified networks, including key support systems for the Global Transportation System, Defense Finance System, Medical, Personnel, Logistics, and official unclassified e-mail
- Many passwords were obtained

LESSONS LEARNED: Confirmed Exercise ELIGIBLE RECEIVER 97-1 findings:

- Indications and warning system needs improvement
- Intrusion detection systems improving, but still insufficient
- Government organizational deficiencies exist; DOJ and DoD relationship unclear
- Problems in characterization and attribution of attack remain
- Need to establish a standing response team
- Need to invest in training and people

RESULTS: Three people were apprehended; two U.S. persons were prosecuted and sentenced for crimes related to the SOLAR SUNRISE intrusions. Prosecution of the third person is pending in Israel.

Terrorists

Terrorists in the past have sought to conduct violent acts against non-combatant targets with the intent to influence an audience. Traditionally, terrorism is defined as the systematic use of violence as a means to intimidate or coerce societies or governments. Typically, this has occurred through bombings or other attacks on targets with high profiles, or that raise significant media attention, or that symbolize the government or ideology to which the terrorist organization is opposed. However, the opportunities afforded by information warfare techniques allow terrorists greater tools to inflict fear into a civilian population or wreak havoc throughout targeted institutions.

A recent report commissioned by the U.S. Air Force detailed the increasing use of cyber tools by terrorists, and the threat this portends for the United States:

"The rise of networks is likely to reshape terrorism in the information age and lead to the adoption of netwar—a kind of information age conflict that will be waged principally by non-state actors.

"There is a new generation of radicals and activists who are just beginning to create information age ideologies. New kinds of actor such as anarchistic and nihilistic leagues of computer hacking 'cyboteurs' may also partake of netwar.

*"Adversaries in asymmetrical conflicts are at an advantage in cyberspace because no one dominates, and those in power and authority have only primitive situational knowledge."—**RAND***

There have been several well-publicized actions by terrorist organizations, including the 1997 denial-of-service attacks launched by the Tamil guerrilla group, "Internet Black Tigers," against Sri Lankan computers throughout Europe, North America, and Asia during a two-week period.

Insiders

*In April 1988, a disgruntled employee unleashed a logic bomb that destroyed a New Jersey engineering firm's computer file controlling its production line operations. The logic bomb not only disabled the company's operations, it also corrupted the firm's backup computer files. With no ability to recover or reconstitute its operations, the firm was eventually forced into bankruptcy.—**Various News Articles***

Imbedded in all the various forms of cyber warfare is the significant vulnerability to insiders. Insiders may ultimately prove to be the greatest threat to our critical infrastructures—military Federal, and civil. Most often it is the insider who has the best understanding of an organization's culture and has the greatest knowledge about the operations of an infrastructure and its supporting systems. Disgruntled workers, paid informants, compromised or coerced employees, former employees, and business associates can be motivated to plan and conduct attacks for reasons such as revenge, financial gain, and fear. Malicious insiders may act alone, or in collusion with outside individuals or organizations seeking to attack an infrastructure.

Conclusion

Unfortunately, very little of our historical defense and intelligence community investment will help predict or even detect a computer-based attack upon our networked systems. Our national intelligence capabilities can "see" movement of troops and military equipment, "sense" the launch of missiles and certain other activities, and "hear" the sound of deployed submarines or command and control communications. But they are not designed to deal with the detection of cyberattack.

It is important to understand that more than an attack on a Defense Department or an intelligence community computer is at stake. We have multiple points of vulnerability—most in the private

sector—which would bear the brunt of cyberattacks: banking and finance, telecommunications, utilities. Owners and operators of computer systems are also their own first line of defense for the integrity, availability, and confidentiality of their systems and the information and data they contain.

For an attack to be successful it only has to cause disruption—not loss of life—to a significant number of Americans. The attack does not have to be national in scope. Disrupting power in a single large city, or halting the operation of one large bank nationwide would have dramatic repercussions far beyond the number of people directly affected. Such a focused attack would become an immediate, and perhaps overwhelming, distraction for our national leadership as they try to determine who carried it out, why they did it, and where they might strike next.

The bottom line is this: the threat to networked information systems and the critical infrastructures that they support is that they are vulnerable to attack, and that it is within the capability and interest of U.S. adversaries to do so. The only defense against this kind of ubiquitous threat is to carefully assess and correct the vulnerabilities to attack, while preparing the tools for immediate response and reconstitution. Failing to take these measures would be a failure of due diligence to an emerging threat—a failure that places America's businesses, communities, and Government at risk.

2. PROTECTING PRIVACY AND CIVIL LIBERTIES

Proposals in the Plan may raise civil liberty and personal privacy issues with some citizens. Concerns have been expressed that some cyber-security tools may, by looking at content, chill free speech. Another concern is that—if initiatives limit the ability of individuals to communicate anonymously, or collect and analyze data relating to network use—the Government and private sector may invade the privacy of network users.

Since issuing Executive Order 13010, which created the President's Commission on Critical Infrastructure Protection (PCCIP), the Administration has analyzed processes and structures that support infrastructure assurance objectives while maintaining and strengthening America's privacy. The President emphasized the importance of privacy rights in Presidential Decision Directive 63.

As outlined in this chapter, the Government will include civil liberty and privacy issues as part of a comprehensive national strategy for infrastructure assurance. Identifying civil liberties as a concern, without working through particular processes for approaching complex issues, is insufficient. This chapter discusses key issues and potential conflicts between information assurance and the protection of privacy, and ways that the Plan will address those interests.

Critical Infrastructure Programs To Promote Privacy Protection

Infrastructure assurance goals must be accomplished in a manner that maintains and even strengthens American's privacy and civil liberties. Some infrastructure assurance programs may increase personal privacy and other civil liberties by enhancing the level of security in data and communications in networked environments. Although infrastructure protection concerns may lead employers, both Government and private sector, to reserve certain monitoring rights on their networks, these will be consistent with civil liberties if conducted in accordance with existing laws and protections. Since such monitoring will take place on employer-owned networks and be carefully tailored to find network abuse, such programs protect both companies and users without intruding unreasonably on protected privacy rights.

The Plan includes a variety of programs that result in protection of personal privacy interests, including:

- requirements for Government to "lead by example" and "promote security awareness," which should encourage greater emphasis within Government on the privacy and reliability of communications, thus setting an ambitious standard for the private sector to follow;

- education and awareness programs, which include emphasis on computer ethics, which will foster greater respect for the privacy of communications;

- vulnerability assessment objectives and funding to protect against intrusions into Government and private sector critical assets, which will help to ensure the privacy of communications on those networks;

- development of partnership programs between Government and the private sector to promote voluntary cooperation on information security goals;

- protection of citizen information as a major component of all critical infrastructure plans; and enhanced protection of individually identifiable and confidential information;

- implementation of all infrastructure assurance programs in accordance with existing legal protections, such as the Electronics Communications Privacy Act (ECPA), the Privacy Act, and other laws; and

- when necessary, carefully tailored monitoring limited to achieving the designated infrastructure assurance goal.

The Federal Government recognizes the risk that technologies designed to protect information and systems, if not carefully implemented, 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.

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 also conduct an annual review of implementation of the Plan relative to civil liberties, privacy rights, and proprietary data protection.

Plan Intent

Within this complex environment, it is important to understand the history of the Plan and the Government's intent in implementing various programs. Three areas deserve attention.

First, the Plan incorporates contributions from a broad range of participants. As early as 1995, when the Government initiated a methodical review of possible infrastructure assurance strategies, cooperation with numerous partners has always been the preferred approach. Findings and recommendations in the PCCIP report, which are incorporated into PDD-63 and the Plan, include valuable insights from academia, industry, and numerous Government Agency communities. Government has carefully integrated knowledge obtained from outreach during the past several years into Plan programs and implementation strategies.

Second, the Plan initiatives are based principally on existing laws, institutions, and programs, thus incorporating the protections contained in those statutes and regulations. This philosophy—of coordinating, facilitating, and working with available mechanisms—is based additionally on a belief that infrastructure assurance cannot be achieved overnight. Other related philosophies include:

- relying on voluntary cooperation to implement the Plan;
- cooperating with the private sector, including owners and operators, rather than imposing new Federal regulations; and
- focusing on, and promoting, private sector-Government partnerships so that any impact on privacy interests will be with the informed consent of those affected.

Third, and most significantly, this Plan does not seek to achieve infrastructure assurance at the expense of civil liberties. Plan implementation will involve strict adherence to existing traditions and institutions, as well as the safeguards guaranteed under the Constitution and Federal law. In carrying out this Plan, the Federal Government, must and will comply with all existing Federal laws that protect civil liberties and privacy and will not seek new intrusive Government authority to accomplish its goal of infrastructure protection.

Concerns

Several programs outlined in the Plan nonetheless may raise civil liberty concerns. Other portions of the Plan, because they are silent on mechanisms and implementation strategies, could lead the reader to incorrectly conclude that personal privacy rights may be sacrificed in exchange for infrastructure assurance objectives. They will not.

Among programs of note is the Federal Intrusion Detection Network (FIDNet). The FIDNet is a network of intrusion detection sensors protecting select critical systems in civilian Federal Agencies. These sensors would look for attacks, based on a variety of methods, and issue alerts.

Several significant FIDNet features include:

- intrusion detection at critical system nodes;
- automated system for incident reporting and handling; and
- a centrally managed operational structure at the General Services Administration for processing, disseminating, warning, and coordinating status of the affected critical infrastructure systems.

Significantly, FIDNet is structured carefully to identify a small class of intrusions. FIDNet focuses on attacks upon Federally owned, non-public networks or domains. FIDNet allows each of the participating Government Agencies to continue monitoring its own systems, in accordance

with existing law. A preliminary legal review by the Justice Department has concluded that, subject to certain limitations, the FIDNet concept complies with the Electronic Communications Privacy Act (ECPA). However, an interagency legal review team continues to look at FIDNet issues and implications of the ECPA and many other statutes such as the Privacy Act of 1974 as the FIDNet concept continues to develop.

Solutions

Finding solutions to infrastructure assurance problems that protect 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, nine key principles serve as a starting point for analyzing programs in the Plan.

- *Consulting with Privacy Communities to Define Solutions*: The Federal Government should request privacy community input into crafting solutions that support the Plan and civil liberties. The complexity of (1) civil liberty laws and policies; (2) programs in the national plan; and (3) technical issues underlying many of the programs, all require careful attention. Privacy advocates are requested to identify possible areas of concern and to design appropriate and lawful solutions.

- *Rigorous and Thorough Legal Review of Plan Programs*: The Plan's initiatives are being reviewed by an interagency legal review team to ensure that privacy and civil liberties issues are appropriately addressed.

- *Commitments to Existing Congressional Protections*: Plan programs must meet standards carefully designed by Congress. Legislation, including the Electronic Communications Privacy Act, the Privacy Act of 1974, and the Computer Security Act of 1987, shape Plan-related activities. The Plan recognizes the complexity of civil liberty law, especially the central roles played by Congress and the Judiciary.

- *Leading by Example*: The Government will continue to "lead by example" in the areas of information security and related infrastructure protection issues. This includes better and more complete information security training and education, and protection of information in the Government's hands. For instance, security and privacy reviews are being built into the standard procedures for the development of new Government computer systems.

- *Reviewing Application of Various Privacy Solutions*: The critical infrastructure community is engaged in a thorough review of privacy solutions and practices. These include Fair Information Practices, forms of Consent, and disclosure issues. Government Agencies with practical expertise and special knowledge of privacy issues, including OMB and the Federal Trade Commission, will continue to assist in the development of relevant privacy policies.

- *Working with Congress*: Congress is responsible for legislating privacy and civil liberty issues. Plan drafters will consult with Congress as part of the review process. This includes congressional Agencies with special expertise, such as the General Accounting Office.

- *Working with the National Academy of Sciences*: Part of the Government's challenge is to apply developing technologies to protect infrastructures and civil liberties. The National Academy of Sciences and National Academy of Engineering have extensive experience in these areas. Organizations, such as the Computer Technology Sciences Board, have studied protection of medical information and differing technologies.

- *Focusing on Education and Awareness*: The Plan's mission includes emphasis on educating the public about civil liberties and privacy issues. The Education and Awareness programs will emphasize computer ethics and related topics.

- *Commitments to Principles of Privacy*: The Plan will adhere to *The Principles for Providing and Using Personal Information* developed by the Privacy Working Group of the Information Infrastructure Task Force. This includes those principles that address information privacy, information integrity, information quality, acquisition of information, notice to those providing information, protection of personal information, and fairness in use of information.

Adherence to these nine principles will facilitate a clearer understanding of Plan objectives and the protection of America's privacy. This will ensure that tenets associated with personal freedoms are integrated into the Plan's programs.

Protecting Civil Liberties Milestones		
Milestone	**Activity**	**Target Date**
10.1	The Federal Government, working with outside organizations, will initiate annual public-private colloquium on Cyber Security, Civil Liberties, and Citizens Rights.	FY 2000
10.2	The National Infrastructure Advisory Committee (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

3. THE PLAN: GOALS AND SCOPE

The Goal of the Plan

The growing threat of highly organized, systematic cyberattack by hostile powers or terrorist organizations creates new risks for every segment of our Nation. For businesses, this threat poses a danger to business operations survivability, public confidence, customer relationships, and investor confidence. For Government, it poses a risk that critical services will not be reliably provided. For national security, the risk is that military, intelligence, and diplomatic response will be disrupted or compromised.

This Plan outlines steps to reduce these risks to a level acceptable to the American people.

In PDD-63, the President established a national goal that the U.S. would achieve and maintain "the ability to protect our Nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.
- state and local governments to maintain order and to deliver minimum essential public service; and
- the Federal Government to perform essential national security missions and to ensure the general public health and safety.

"Any disruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."

The Scope of the Plan: Security of Critical Computer and Information Systems

The Information Technology revolution that has taken place in America during the 1990s, and the dependence on information systems it has created, makes a national level program for information systems security and defense essential. Any plan for national information systems security and defense would necessarily have a broad scope.

This version of the Plan focuses on protection of critical information infrastructure systems from both cyber and physical attack. Consideration of other critical physical infrastructures and security issues are being dealt within a separate effort (*see page xviii*).

Critical physical infrastructure security was the focus of a 1995 review mandated by the President in PDD-39 and chaired by the Attorney General. Critical physical infrastructure has been for many years the focus of the FBI Key Asset Initiative and the DoD Key Asset Protection Program (KAPP) (now included in the DoD Critical Infrastructure Protection Program). Thus, plans and programs are in place to address the security of dams, bridges, tunnels, power lines, generating stations, etc., with the interdependency linkages to other critical information infrastructure systems reflected in a bridging document.

These existing critical physical infrastructure security programs are also the subjects of a new review, which will lead to The *National Plan for Critical Physical Infrastructure Protection* to be issued in 2000. The two plans (Information Systems and Critical Physical Infrastructure Protection) will be coordinated with crossover issues identified and will eventually be consolidated into one plan.

As called for in PDD-63, Lead Federal Agencies are developing critical infrastructure protection plans in conjunction with companies in each key sector of the economy (e.g., transportation, banking). Every Federal Department is also developing a plan to protect its own critical infrastructures, which include both cyber and physical dimensions. Federal Departments, in conjunction with their private sector counterparts where appropriate, will develop their plans for information systems and critical physical infrastructure protection.

Federal Computer Security and IRM 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.

How the National Plan Complements Federal Computer Security and Information Resource Management Responsibilities	
National Plan Implementation	**IRM/Management 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.**

The Federal Budget

Since the President's issued PDD-63 in 1998, proposed Federal funding for critical infrastructure protection has increased. The FY 2000 enacted budget contains $1.737 billion for critical infrastructure protection. This represents more that a 50% increase over FY1998 enacted spending—the enacted Federal budget that immediately predates the issuance of PDD-63 (*see Annex B*).

In preparation for the FY2001 budget request, the Office of Management and Budget, in conjunction with the National Coordinator, created a special process to review national and departmental requirements in this area prior to the submission of proposed budgets by the Agencies and Departments (*see Annex B*).

This new review process is intended to ensure that:

- Agencies and Departments are allocating adequate resources within the overall funds assigned to them to implement the President's intent in PDD-63, the mandate in OMB's Circular A-130, and the requirements of the Computer Security Act;

- national-level requirements are addressed in future President's budgets, as well as those needs that are clearly related to a specific Agency or Department; and

- the President's review of the draft FY2001 budget identifies the decision points related to the National Plan for Information Systems Protection.

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.

Thus, the milestones in this version of the Plan are directional goals. The precise level of effort, resourcing, and dates of completion will be adjusted in each subsequent version of the Plan during the next several years to take into account specific budget decisions made by the President and the Congress.

Building the Public-Private Partnership

Building the public-private partnership to ensure action is a core theme of the Plan. Without the full participation of the private sector, Federal actions to protect critical infrastructures will have only a limited benefit.

In this version of the Plan, the *Framework for Critical Infrastructure Assurance By Private Sector and State and Local Government* is only an initial outline of what are still largely Federal initiatives for building the necessary partnership. As the partnership develops, we hope this component plan will reflect the decisions taken by private companies and organizations—not only those of the Federal Government.

To launch the public-private partnership, the Federal Government is asking business leaders throughout America in all the sectors that operate critical infrastructures, to join with it in acknowledging and building awareness of the need for increasing cyber security. Plans for creating a *Partnership for Critical Infrastructure Security* were discussed with senior executives from more than 85 companies at December 1999 meeting in New York. Further meetings early in 2000 are planned to develop the Partnership *(see Program 8 of the Executive Summary, and p. 72).*

Working with the Congress

The Administration will continue to work closely with Congress to develop the tools necessary to ensure the security of the Nation's critical infrastructures. These tools are not limited to funding, but include advice and assistance in solving the many legal and policy issues addressed in the Plan. Future versions of the Plan must grow out of a true dialog with Congress on how best to secure our critical infrastructures to achieve security and prosperity.

The Administration and the Congress have begun this dialog and cooperation. It has born some fruit in the development of this version of the Plan and will continue to do so as the Plan matures. Members of Congress have introduced legislative proposals and held hearings to address issues and lay the groundwork for legal reforms required to promote the security of our critical infrastructures. They have asked tough questions on issues such as protecting the privacy rights of individuals and the role of the Federal Government in monitoring cyberattacks on our infrastructure, and they have demanded straight answers. This Plan bears the mark of their diligence.

Continued adequate funding is essential for the effective implementation of the Plan, and for achieving Initial Operating Capability. Legislation may also be required to ensure the Government's ability to form a robust partnership with the private sector, remove legal obstacles to such cooperation, and provide for enhanced legal authorities and frameworks. The Administration will reach out to the Congress for their advice and assistance in achieving these goals.

Two Component Plans

The two component plans, *The Federal Government Critical Infrastructure Assurance Plan* and *The Framework for Critical Infrastructure Assurance By Private Sector and State and Local Government*, comprise the core of this effort to promote security for the Nation's key cyber systems. Work in the Government's civilian Agencies is in the initial design phase, as represented by this Plan. The Defense Department's efforts have progressed farthest and implementation has begun. The collaborative private sector groups, which the Plan proposes, are still in the formative phases. Future versions of the Plan will integrate elements of the plans for each sector of America's critical infrastructures, including banking and finance, emergency services, energy, telecommunications, and transportation.

Strategy for the Future

This multi-year Plan contains the key initiatives we feel are necessary to protect these infrastructures. They provide solid direction for every facet of our Nation—the private sector, and Federal, state and local governments—and represent the level of commitment needed to ensure protection of our critical infrastructures in the new millennium.

4. FEDERAL GOVERNMENT CRITICAL INFRASTRUCTURE ASSURANCE PLAN

The President has called upon the Federal Government to become a model of information systems security. Currently, it is not.

Our Government has become increasingly dependent on the computers and networks forming a critical information infrastructure that supports the most essential functions of our society—from the right of our citizens to be secure within our Nation's borders to our reliance on the continuity of essential services. Recent, serious real-world break-ins to Government computer networks have reinforced the Government's resolve to enhance its defenses against cyber crime, cyber terrorism, and information warfare that might be directed against the Federal Government infrastructure.

The Federal component of the Plan presents initiatives underway and planned by the Federal Government to protect these systems. Departments and Agencies are preparing individual plans to protect their own critical infrastructures. New processes have been created to ensure coordination among Agencies and consistency among plans. Initiatives are being launched that cut across many Agency responsibilities. Indeed, the challenge of developing a Federal Plan has brought together Agencies within the Federal Government that have never worked together before. Coordinated action is necessary because of the interrelation and interdependencies of the computer networks and systems on which our Government relies.

The Federal Plan is presented in two sections, preceded by a description of Federal organization to protect critical information infrastructures:

- *Civilian Agency Protection and Government-Wide Initiatives*: This plan discusses the infrastructure protection programs of civilian Federal Agencies, including law enforcement. It also outlines the initiatives that are being undertaken across the breadth of the Federal Government. It also provides examples of initiatives being taken by particular Departments to identify their most important information infrastructures; evaluate and fix potential vulnerabilities; and enhance their ability to recognize, prevent, and mitigate the consequences of any deliberate attack on their critical systems.

- *The Department of Defense Infrastructure Assurance Plan*: The Defense Department, because of its mission to defend the Nation, has been among the first Departments to respond to the challenge of protecting its own infrastructure. Its plan and resulting implementation are also the most developed among the Federal Departments and, in important respects, are serving as the model for other Departments and Agencies. Therefore, elements that reflect the unique scope and mission of the Defense Department, and those initiatives that serve as models for the rest of the Federal Government, are presented in some detail.

4A. FEDERAL ORGANIZATION FOR CRITICAL INFRASTRUCTURE PROTECTION

On May 22, 1998, the President issued Presidential Decision Directive 63 (PDD-63) calling for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States, especially cyber-based infrastructures. These infrastructures include telecommunications, banking and finance, energy, transportation, water systems, and essential Government services. The directive requires the Federal Government immediately to assess the vulnerabilities of its computer-based systems and remedy deficiencies, and produce a detailed Plan to protect our critical infrastructure and defend America against information warfare. It orders the Government to serve as a model to the rest of the country for how infrastructure protection is to be attained, and calls for a joint public-private action to protect critical infrastructures.

PDD-63 organizes the Federal Government to meet this growing security challenge:

- **National Coordinator for Security, Critical Infrastructure and Counter-Terrorism** at the White House National Security Council (NSC) oversees national policy development and implementation for critical infrastructure protection. The National Coordinator is a member of the Cabinet-level Principals Committee, and advises the President and the National Security Advisor on policy and implementation issues as they relate to our national critical infrastructures. The NSC Senior Director for Critical Infrastructure supports him.

- The **Critical Infrastructure Assurance Office (CIAO),** an interagency office housed at the Commerce Department, supports Plan development with Government Agencies and the private sector. The Office is also responsible for assisting Agencies in identifying their dependencies on critical infrastructures, and coordinating a national education and awareness program, legislative issues, and public affairs.

- The **National Infrastructure Protection Center (NIPC)**, an interagency office at the FBI, serves as a threat assessment center focusing on threat warnings, vulnerabilities, and law enforcement. The NIPC includes representatives from the FBI, Department of Defense, United States Secret Service, Intelligence Agencies, and other Government Agencies.

- For each infrastructure sector that could be a target for significant cyber or physical attacks, a single U.S. Government Department or Agency serves as the Lead Agency for liaison. Each Agency listed as a **Lead Agency** for a particular sector of the critical infrastructure will also designate a **Sector Liaison Official** to direct efforts in that sector. PDD-63 sector and Lead Agency designations are as follows:

Critical Infrastructure Sector	Lead Agency
Information and Communications	Commerce
Banking and Finance	Treasury
Water Supply	Environmental Protection Agency
Aviation, Highways, Mass Transit, Pipelines, Rail, Waterborne Commerce	Transportation

Critical Infrastructure Sector	Lead Agency
Emergency Law Enforcement Services	Justice/FBI
Emergency Fire Service, Continuity of Government Services	Federal Emergency Management Agency
Public Health Services	Health and Human Services
Electric and Power, Oil and Gas Production and Storage	Energy
Federal Government	General Services Administration

- The **Sector Liaison Officials** work closely with the National Coordinator on the **Critical Infrastructure Coordinating Group (CICG)**, the interagency committee analyzing critical infrastructure policy issues and developing policy recommendations to the Cabinet-level Principals Committee.

- Functional areas that have no private sector counterparts (Defense, intelligence, foreign affairs, law enforcement, and research and development) are also represented on the CICG by **Special Functional Coordinators**. These are:

Special Functional Coordinators	
State Department	Foreign Affairs
Defense	National Defense
Central Intelligence Agency	Foreign Intelligence
Justice/FBI	Law Enforcement and Internal Security
Office of Science and Technology Policy	Research and Development

4B: CIVILIAN AGENCY PROTECTION AND GOVERNMENT-WIDE INITIATIVES

Through the initiatives presented, the Federal Government can serve as a model for the private sector on how best to protect critical information system infrastructures. Significant progress in many areas is underway:

- the National Infrastructure Protection Center (NIPC) continues its mission to serve as an interagency national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigations and response entity;

- an Expert Review Team (ERT) works with Federal Agencies to improve information security, and coordinates efforts with other Federal bodies responsible for aspects of information security; and

- for the first time, the Federal Government is coordinating infrastructure protection R&D activities across the Federal Government to ensure consistency in plans, programs, and agendas and to focus Federal R&D resources on the most important infrastructure vulnerabilities.

Other proposed initiatives will help ensure the Federal Government's role model status by:

- creating nationwide system for response, reconstitution, and recovery after a cyberattack;

- providing Federal civilian Agencies with intrusion detection at critical system nodal sites; an automated system for incident reporting and handling; and a centrally managed operational structure for processing, dissemination, warning, and coordination functions that provide a coherent picture of the infrastructure's cyber status. A steering committee is currently investigating operational issues and determining the technological architecture of the Federal Intrusion Detection Network (FIDNet);

- establishing a national institute focused on infrastructure protection to help develop and disseminate the knowledge necessary to protect our information infrastructure, accelerating the development of recommended practices and standards and accreditation processes for adoption by both the Federal Government and the private sector;

- addressing the desperate shortage of Federal employees trained in systems security and administration through the Federal Cyber Services (FCS) program, which will educate more Americans in information systems security;

- strengthening the universities in their information security programs by creating INFOSECURITY Centers of Excellence to enhance development of undergraduate and graduate education programs geared toward producing top researchers and information systems security experts;

- launching a national awareness campaign to increase understanding and awareness of the need to increase cyber security, focusing initially on business leaders in all critical infrastructure sectors, Federal employees, and our Nation's school children, and, building on this base, to be expanded at a later date to other private sector organizations and the general public;

- proposing needed revisions to existing laws to meet the new threats to the Nation's information systems in a manner that assures protection both of our Nation's critical infrastructures and the civil liberties of our citizens; and

- working with private industry, through the public-private partnerships to ensure appropriate industry input into the Federal Government initiatives that involve or directly impact industry.

OBJECTIVE 1: ACTIONS TO PREPARE AND PREVENT

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

1.1 Federal Civilian Organization and Assessment

The Federal Government has undertaken significant organizational and planning measures to protect itself from cyberattack with the following initiatives:

1.1.1 Department plans and management accountability for information infrastructure protection:

- *Department and Agency Critical Infrastructure Protection Plans*: PDD-63 directs Departments and Agencies to develop plans to protect their critical infrastructures. Departments and Agencies with the highest priority systems, designated as Phase One Agencies, completed their initial plans to protect their own critical information systems in November 1998. These initial plans were followed by Phase Two Agency plans (February 1999). Plans will be implemented within two years.

Department of Defense organization for infrastructure protection is described in Chapter 4C.

The following Agencies, classified as Phase One, completed their plans in November 1998: Central Intelligence Agency (CIA); Department of Commerce (DOC); Department of Defense (DoD); Department of Energy (DOE); Department of Health and Human Services (HHS); Department of Justice (DOJ); Federal Bureau of Investigation (FBI); Department of Transportation (DOT); Department of the Treasury; Department of State (DOS); Department of Veterans Affairs (DVA); Environmental Protection Agency (EPA); Federal Emergency Management Agency (FEMA); National Security Agency (NSA).

The following Agencies, classified as Phase Two, completed their plans by February 1999: Department of Agriculture (USDA); Department of Education; Department of Housing and

Urban Development (HUD); Department of the Interior (DOI); Department of Labor (DOL); General Services Administration (GSA); National Aeronautics and Space Administration (NASA); Nuclear Regulatory Commission (NRC).

- *Special focus on the physical protection of critical information systems infrastructure:* All Agencies have the responsibility to identify physical vulnerabilities to information systems and take action to correct them within their agencies. Lead Agencies for critical infrastructure sectors will work with the private sector to correct them in non-Federal systems.

- *Ongoing Expert Review Process*: The Critical Infrastructure Coordination Group (CICG) established an Expert Review Team (ERT) to assist Departments and Agencies with PDD-63 compliance. An interim ERT was housed at the Critical Infrastructure Assurance Office (CIAO), and worked in conjunction with the Federal CIO Council, GSA, and OMB.

  The interim ERT was a new structure within the Federal Government. For the first time, a small but full-time group was devoted to enhancing critical infrastructure protection by:

  - providing a compendium of information on IT security;
  - ensuring a consistent framework for all Agency plans; and
  - furnishing its review and comments to the 22 Phase One and Two Agencies.

A permanent Expert Review Team (ERT) to assist Government-wide Agencies in adhering to Federal computer security requirements will be established at the Department of Commerce's National Institute of Standards and Technology (NIST).

- *Chief Infrastructure Assurance Officer—evaluating and remedying vulnerabilities*: Pursuant to PDD-63, Federal Government Departments and Agencies have appointed a Chief Infrastructure Assurance Officer, who may or may not be the same person as the Chief Information Officer. The Chief Information Officer is responsible for information assurance, and the Chief Infrastructure Assurance Officer is responsible for the protection of all other aspects of that Department's critical infrastructure. A key element of the Agency plans and implementation will be self-vulnerability evaluations. Each Department and Agency will identify its mission critical systems to the National Coordinator.

- *Verification Process*: The CIO Council will facilitate an audit process to verify the adherence of the Agencies to their infrastructure protection plans. This process will be developed in coordination with organizations such as NSA, the Information Technology Resources Board, GAO and IG.

1.1.2 Vulnerability analyses to independently test security:

- *Agencies will put in place programs to carry out several types of vulnerability testing and analysis, including*: routine automated system configuration/integrity/vulnerability testing using COTS tools, regular internal self-assessments, and independent external critical reviews.

  At an Agency's request, NSA and NIST will perform independent analyses of critical Federal information infrastructures, and provide independent reports of their results to the Agency's CIO. All Federal Agencies will designate representatives who may authorize access to their computer systems to facilitate vulnerability and red-teaming analyses. The Department of Justice will establish legal guidelines to facilitate vulnerability assessments of U.S. Government entities. In addition, Agency Inspectors General should have an important role in independent assessments. The CIO Council and the National Coordinator will work with Inspectors General to encourage their attention to these issues.

Expert Review of Department Critical Infrastructure Protection Plans

Evolutionary and Revolutionary Concept

The Expert Review Team (ERT), established in November 1998, was a landmark effort to ensure the quality, coherency, and effective implementation of Agency plans to protect their critical infrastructures. It is the first interagency team to:

- *Bring continuity and government-wide experience* and overview to the CIP planning process.
- *Review and comment* upon agency information security plans based on adherence to interagency agreed common essential plan elements.
- *Provide consistent monitoring and support* for plan implementation.
- *Facilitate the provision of technical assistance* to Federal Agencies.

Phase One

In the first phase of its work, the ERT focused on the development of common elements for the Agency plans and review of the extent to which initial plans addressed those elements:

- Agency Mission and Identification of Mission-Critical Infrastructure
- Threat Analysis
- Vulnerability Assessment
- Remedial Plans
- Emergency Plans
- Research and Development Needs
- Roles and Responsibilities
- Resource Requirements
- Implementation Schedule
- Coordination Efforts
- Recruitment, Retention, Education and Awareness Efforts
- Authorities and Guidance

In this phase, the ERT:

- Found that Agencies experienced the most difficulty in their initial plan preparation when addressing research and development needs, resources and requirements, and coordination efforts.
- Gave first priority to encouraging Agencies to address all necessary elements in their plans so that they would be adequately framed to provide ongoing assessments on an evolving basis.
- Requested that Agencies revise and re-file plans as necessary.
- Briefed the Agencies both Government-wide and individually on their assessment of initial plans.
- Instituted a new, give-and-take process designed not to critique the Agency plans, but to assist Agencies to improve their plans.
- Achieved a high degree of cooperation from the Agencies.

Phase Two

The ERT shifted from plan review to supporting plan implementation. Key components included:

- Working with Phase One and Two Departments and Agencies, as well as select other government organizations, to assist in the identification of their national security, critical national economic security, and critical public health and safety related responsibilities.
- Working with Phase One and Two Departments and Agencies, as well as select other government organizations, to assist in the identification of their infrastructure dependencies and IT associated interdependencies for the execution of their respective national security, critical national economic, and critical public health and safety-related responsibilities.

Milestones: Federal Department Initiatives to Strengthen Cyber Security

All major Federal Agencies shall ensure protection of mission critical computers and information systems that support information assurance standards. Departments will conduct vulnerability assessments of mission critical systems, identify interdependencies, develop mitigation plans, and update security measures on a regular basis.

Federal Department Initiatives to Strengthen Cyber Security		
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 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)
1.11	The Federal Government will develop methodologies to identify critical infrastructure assets and shared interdependencies.	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
1.16	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
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
1.29	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

Milestones: Physical Security of Information Systems

In order to address the physical security of critical computers and computer-controlled systems, the Federal Government will undertake the following activities:

Physical Security of Information Systems Milestones		
Milestone	**Activity**	**Target Date**
1.7	The Federal Government will complete the first version of the Critical Physical Infrastructure Protection Plan.	June 2000
1.12	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
1.15	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

1.2. Recommended Practices and Standards for Cyber-Security Widely Applied to Critical Information Systems

Protection of the critical information systems of the U.S. Government is crucial, both as a provider of essential services to the Nation, and as a model for others to emulate. A critical balance must be struck in these dual roles. The Federal Government will not, in general, be developing its own security solutions, but will look to private industry for standards and recommended practices; for commercial off-the-shelf (COTS) products; and for consulting services. However, as the single largest information systems customer in the world, the Federal Government can play an important role in shaping the development and use of cyber-security products, recommended practices, and standards.

In addition to Agency plans, OMB and GSA will work with other Agencies to implement the following program of activities to ensure that the U.S. Government serves as a model in its information systems security functions for the rest of the world:

- *Identify and adopt recommended practices and security standards for critical Federal information systems*: NSA and NIST have existing responsibilities to set standards for classified and sensitive but unclassified Federal information systems. OMB and GSA have other important roles in ensuring Federal information systems security. Using these existing authorities, NSA, NIST, GSA, and OMB, in conjunction with the National Coordinator, will identify or develop recommended practices and standards for critical Federal information systems. In coordination with the CIO Council, agencies will identify their critical information systems, and implement these practices and standards by January 2001.

  This considerable undertaking will depend on the ability to adopt technology and practices already in use in security proactive organizations. A three-step process will be used in developing recommended practices and standards for Federal use:

- First, identify and make use of existing private sector or Departmental standards and practices;

- Second, if necessary, work with existing private sector standards bodies and professional associations to develop new, or modify existing, private sector standards and practices to meet Federal information security needs; and

- Finally, there may be a need to develop customized standards and practices for truly unique Federal needs.

The intent is to encourage the adaptation or adoption of uniform information systems security recommended practices and standards throughout government and private industry.

- *Establish procurement standards*: GSA, DoD (for its own procurements) and OMB, working with NIST and NSA, will in the future revise procurement regulations to require the acquisition of information assurance products, systems, and services that meet Federal recommended practices and standards for information systems security. GSA and OMB will develop procedures and deadlines for Agency adoption and implementation. NIST and NSA, through the National Information Assurance Partnership (NIAP) and the Common Criteria, have created the framework for these procurement standards. The NIAP is accrediting commercial labs to conduct security evaluations and validations of security products/systems in accordance with the International Standard Common Criteria for Information Technology Security. Government policy, which provides for a practical, phased-in approach to employing validated and evaluated security products/systems, facilitates the Government-industry partnership and provides the product/system basis for information security.

- *Develop security testing and evaluation programs*: NIAP is initially focusing on three primary initiatives to promote the development and use of security-enhanced IT products and systems: Security Requirements, Security Product Testing, and Security Testing Research and Development.

  - The security requirement initiative is a series of services offered by NIAP to aid interested parties in specifying robust, testable security requirements that could ultimately be used by an accredited laboratory to test the security attributes of products or systems.

  - The security product testing initiative strives to demonstrate and increase the value of independent testing and certification as a measure of security and trust in information technology; move current government-conducted evaluation and testing efforts to accredited, private sector laboratories; help establish the elements of a robust commercial security testing industry; and establish the basis for international mutual recognition of security product evaluation results.

  - The goal of the Research and Development initiative is to foster R&D to advance the state-of-the-art in security testing methods and metrics through NIAP-sponsored partnerships with industry and internal R&D efforts.

- *Enhance oversight that Federal Agencies maintain up-to-date system patches, vulnerability closures, and other on-going actions to maintain secure systems*: The Federal Computer Incident Response Capability (FedCIRC), the NIPC's CyberNotes program, and other CERTs provide frequent notices about new systems vulnerabilities and modes of intrusion. Such information is useless unless acted upon. GSA, working with OMB, will develop procedures to ensure that all Agencies implement the recommendations of applicable FedCIRC or other CERT advisories in a timely manner. This may be modeled after the DoD Information Assurance Vulnerability Alert (IAVA) program.

- *Develop processes for certifying Federal systems administrators and other key Federal information systems officials*: There are several Federal security-related job categories for which formal certification may be appropriate. NIST, together with OPM, has prepared a training requirement guide for Computer Security Act implementation that identifies many of the job categories that may be covered.

  OPM, along with the Departments of Commerce and Defense, will identify the Federal job categories requiring certification, and the process for certifying officials as having sufficient skills to build and maintain appropriate security for information on their systems, and adequately respond to attacks onto their systems. In developing the accreditation process, existing professional certification programs will be examined for their applicability to Federal personnel.

- *Create a formal annual interagency process for revising Federal information systems recommended practices and standards:* Just as the preparation of the Federal budget follows a regular annual cycle, so to there will be a regular process of developing, evaluating, and deciding on appropriate revisions to Federal recommended practices and standards for information systems security. OMB and the CIO Council will manage the interagency process. Input from industry and outside standards and cyber-security organizations will be encouraged.

Milestones: Cyber-Security Recommended Practices and Standards

Identify or develop recommended practices and standards for cyber-security. Adopt these recommended practices and standards across the Federal Government for mission critical systems, including procurements for such systems, and create the management systems for clear responsibility and accountability for meeting these standards. Update standards and recommended practices regularly, and cooperate with industry in encouraging adoption or adaptation of these Federal recommended practices and standards for private sector use and acceptance by the international standards community.

Cyber-Security Recommended Practices and Standards Milestones		
Milestone	**Activity**	**Target Date**
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 (January 2000)
1.8	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
1.13	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.	FY 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

1.3 Public Key Infrastructure: Public Key Cryptography to Secure Critical Information Systems

Protecting critical infrastructures in the Federal Government and private sectors requires development of a public key infrastructure (PKI). A PKI enables data integrity, user identification and authentication, user non-repudiation, and data confidentiality through public key cryptography by distributing public keys in a secure, scalable, and reliable manner. The potential of PKI has inspired numerous projects and pilots throughout the Federal Government and private sectors. The Federal Government has actively promoted the development of PKI technology and has developed a strategy to integrate these efforts into a fully functional Federal PKI.

A PKI distributes keys through the generation of public key certificates and associated status information. The status information is generally distributed as a certificate revocation list (CRL). Components that generate certificates and CRLs are known as certification authorities (CAs). By

managing the certificates and CRLs, a PKI supports digital signatures and secure distribution of symmetric keys for critical infrastructures and applications.

To achieve the goal of an integrated Federal PKI, and protect our critical infrastructures, the Federal Government is working with industry to implement the following program of activities:

- *Connect agency-wide PKIs into a Federal PKI:* DoD, NASA, and other Government Agencies, are actively implementing Agency-wide PKIs to protect their internal critical infrastructures. While a positive step, these isolated PKIs do not protect infrastructures that cross Agency boundaries. Full protection requires an integrated, fully functional PKI.

  To facilitate the interconnection of agency-wide PKIs, the Federal PKI Steering Committee (housed at the Treasury Department) is developing a Federal Bridge CA. Agencies can establish a single relationship with the Bridge CA and indirectly establish relationships with all the agency-wide PKIs that are connected to the Bridge CA.

  To promote compatibility of certificates issued by Agency PKIs, the Federal PKI Technical Working Group has developed a *Federal Certificate and CRL Profile* as guidance to Government Agencies. Users from Agencies that follow this guidance will be able to process each other's certificates.

- *Connect the Federal PKI with Private Sector PKIs:* Private sector groups are actively developing their own PKIs as well. While a positive step, like in the Federal sector, these isolated PKIs do not protect infrastructures that cross government or industry sector boundaries.

  Connecting the Federal PKI to private sector PKIs presents similar challenges to the creation of a Federal PKI. The Federal Bridge CA will be the mechanism facilitating the connection of the Federal PKI and private sector PKIs. The Bridge CA will perform the analysis of external PKIs and establish the appropriate relationships. This will permit users of the Federal PKI to obtain security services with users of the private sector PKIs.

- *Encouraging development of interoperable Commercial Off-the-Shelf (COTS) PKI Products:* Communities implementing a PKI are often limited to a single vendor's solution. This can be a serious impediment, as most organizations have a heterogeneous computing environment. Consumers must be able to choose COTS PKI components that suit their needs, rather than those offered by a particular vendor.

  The Minimum Interoperability Specification for PKI Components (MISPC) includes message formats and transaction protocols, in addition to the certificate profile noted above. The definition of detailed message formats and protocols will encourage development of interoperable COTS PKI products. NIST and several PKI vendors are currently participating in a series of interoperability workshops to demonstrate interoperability of PKI components using these formats and protocols.

- *Validating the Security of Critical PKI Components:* Protecting critical infrastructures require sound implementations of the CA and related components. The strength of the security services provided to the critical infrastructures depends upon the security of the PKI components. Validation of the security of PKI components is needed to ensure that critical infrastructures are adequately protected. NIST is pursuing a validation program for PKI components.

- *Encouraging Development of PKI-Aware Applications:* Critical applications desiring to use the public key's infrastructure may not be PKI-aware. To become effective, critical applications need a choice of COTS PKIs to provide digital signature services and manage certificates. To encourage development of PKI-aware applications, the Government is working with vendors in key application areas. One example is the secure electronic mail projects that have been performed jointly with industry.

Milestones: Development of a Public Key Infrastructure

Establish profiles and infrastructure components necessary to connect agency-wide PKIs and private sector PKIs into a fully functional PKI. Publish interoperability specifications to promote interoperability of commercial PKI products. Establish validation programs to promote secure implementations of PKI components. Encourage development of "PKI-aware" applications to utilize the PKI.

Milestone	Activity	Target Date
1.6	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
1.22	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
1.26	Perform the first validation of a PKI component against the *Security Requirements for Certificate Issuing and Management Components.*	December 2001

OBJECTIVE 2: ACTIONS TO DETECT AND RESPOND

Program 2: Multi-Layered Systems to Detect Attacks and Unauthorized Intrusions Against Government Computers and Data

U.S. national security, economic well-being, and public welfare rest on strongly interconnected systems. As real-life computer intrusions like Solar Sunrise illustrate, malicious intrusions into specific systems have the potential to cripple networks, destroy or alter important public records, or even deny vital public services such as police, fire and rescue. The public also expects data that it sends to the Federal Government to be kept secure and protected from unlawful review and manipulation. At the same time, however, the public also rightly expects the Government to respect and uphold America's privacy rights and civil liberties. Accordingly, any system for protecting Federal Government computers and data must be designed with the utmost concern for these vital issues.

Since the release of Presidential Decision Directive 63 in May 1998, the Administration has methodically explored technical, legal, and policy issues associated with Government-wide computer security. As attacks on Government computers increase in scope and intensity, Federal Agencies are increasingly under pressure to defend the integrity of their cyber systems. It is particularly difficult to quantify the potential costs of a disruption given the increasing reliance of our economy and our daily lives on government data and associated computer networks. Examples of national reliance on information stored and processed on Federal information systems include:

- national security from the Department of Defense and other Agencies;
- warnings from the Emergency Alert System;
- severe weather forecasting from the National Weather Service; and,
- flight tracking/air traffic control from National Airspace Systems.

Many enterprises in both the public and private sectors already use products or services to monitor their computer network systems for computer viruses and/or for unauthorized network intrusions. Commercially available products and the approaches they take to protect computer systems from unauthorized activity vary. Nevertheless, most if not all routinely scan all network traffic to detect and identify unauthorized intrusions and criminal activity that could destroy or deny critical services important to the economic well-being of our country.

This National Plan calls for developing and deploying computer network intrusion detection monitoring systems to detect unauthorized and possible criminal activity both within and across participating Government Agencies. The Federal Government is developing a comprehensive framework for assuring both the security of such computer systems and the information they contain. In addition, the proposal will be the subject of ongoing legal review in order to assure strict compliance with constitutional and statutory safeguards.

Agency Initiative: Department of Energy Cyber Security Strategy

As a part of the Department of Energy's revamping of its cyber security program, the departmental computer security oversight has been consolidated under the CIO. At the same time, the CIO's office is being realigned under the Office of Security and Emergency Operations.

The CIO's office developed a new cyber security plan that was released in September 1999. This plan will cover the implementation of a consistent policy on classified and unclassified computing, a rapid training initiative to be deployed within six months, a cyber security architecture, and an R&D program for computer security tools.

Additionally, the Computer Incident Advisory Capability (CIAC) staffs at Lawrence Livermore National Laboratory will be increased from seven to 25 people. The CIAC will have increased responsibilities in monitoring security and providing early warning for viruses.

This heightened security effort is expected to cost $80 million during the next two fiscal years (FY2000 and FY2001) with $45 million of the total amount going toward fielding the operational security capability.

Milestone	Activity	Target Date
2.4	Release departmental cyber-security plan and realign DOE CIO office under the Office of Security and Emergency Operations.	COMPLETED (September 1999)

2.1 Defensive Systems to Detect Intrusions and Anomalous Behavior

To detect unauthorized intrusions or activities on a network, the Plan first calls for the installation and implementation of highly automated security and intrusion detection capabilities on critical Federal systems, 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.

It is important to note that these four security controls are not the only ones necessary to protect networks. However, they are becoming viewed as increasingly important elements of an overall risk-based, cost-effective security program that comprises many layers.

Some of these capabilities are currently commercially available. Most commercially available programs are first generation. In many systems that have installed some of these capabilities, extensive human monitoring and intervention are still required.

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 Federal critical information system networks. The Government may also share evaluations of such systems with the private sector and state and local governments through Information Sharing and Analysis Centers (ISACs).

2.2 Government-wide Systems for Analyzing and Correlating Attack Data

The installation of Defensive Detection Systems by themselves will not provide adequate protection for critical Federal systems. In almost all current applications, intrusion detection monitors are installed on individual systems or networks. When alarms go off, reporting procedures are often unclear or too limited in scope. When one network is attacked with a new technique, it may take days for other networks to learn of the technique and weeks to adopt software to prevent it, leaving critical systems vulnerable in the meantime. For these reasons, a Government-wide system for analyzing and correlating intrusion data, and rapidly disseminating attack information, is required.

With the current state of the art in Defensive Detection Systems, human management and analysis are essential to integrate intrusion information from the multitude of data streams available. To resolve this, the Plan calls for the networking of intrusion detection systems with analysis centers to detect attacks. As soon as any system is attacked, word of the attack would be flashed to all other sites.

2.2.1 Three Elements of the Government-wide System

The proposed Government-wide system will consist of three elements: one for the Department of Defense (DoD) and National Security communities, a second for non-DoD Federal Departments and Agencies (referred to as Federal Civilian Agencies), and a third that provides information to both systems. Two of these systems—JTF-CND and NSIRC—are already deployed.

- ***Joint Task Force-Computer Network Defense (JTF-CND)****(see p. 95 of the Plan for in-depth discussion of JFT-CND)*: The Department of Defense is already advanced in deploying a combination of network security monitors and network intrusion detection systems netted to central analytical cells.

- ***Federal Intrusion Detection Network* (*FIDNet)***: Building on existing DoD and other security technology expertise, the Plan calls for creating the Federal Intrusion Detection Network (FIDNet) to protect critical non-Defense Federal systems. Implemented and

operated by the General Services Administration (GSA) and working with cooperating Federal Civilian Agencies, the FIDNet will link together intrusion detection monitors covering critical Federal civilian systems with a central analysis capability of system anomalies at GSA.

- ***National Security Incident Response Center (NSIRC)***: The NSIRC provides expert assistance to the national security community in isolating, containing, and resolving incidents threatening national security systems.

2.2.2 Coordinated Federal R&D into common challenges facing Intrusion Detection Systems

Continued R&D to advance the tools and techniques for detecting, analyzing, and responding to intrusions is key to the long-term success of the proposed Government-wide system. The Plan calls for coordination of Federal R&D efforts underway in intrusion detection to achieve the following goals:

- *Open standards for Intrusion Detection (ID) reporting format and content*: There needs to be a way that different monitors can share information in a common format for joint analysis. Work to achieve this is already underway through the Internet Engineering Task Force (IETF), and under DARPA's Common Intrusion Detection Framework.

- *Automated and Artificial Intelligence (AI) tools for analysis*: There needs to be better-automated tools to assist skilled human analysts in quickly and accurately identifying intrusions.

- *Evaluation criteria/goodness metrics for system evaluation*: There needs to be effective means of measuring how good an intrusion detection system is.

2.3 FIDNet: A "Burglar Alarm" for Government Computers

Locks and burglar alarms protect valuable information in file cabinets. FIDNet is a burglar alarm system for sensitive information on select government computers.

FIDNet will be the 'system of systems' that provides Federal civilian-wide intrusion detection, prevention, and response services to participating Agencies. FIDNet will link intrusion detection monitoring capabilities (both technical and personnel) together with an automated system for reporting data on system anomalies to a centrally managed analysis center at GSA. In the event of suspected criminal activity, FIDNet staff will inform the FBI through the NIPC.

Federal civilian Agencies and Departments are already making investments in intrusion detection monitors and skilled personnel to protect themselves. FIDNet will link the capabilities of participating Agencies into a larger system, providing the operational scale no single civilian Agency can obtain itself. This includes:

- an analytical staff at GSA FedCIRC that will work with Agency cyber-security experts, review reports of intrusions, and provide suggested means of preventing the intrusions in the future;

- secure telecommunications between the participating Departments and the central analytical staff;

- a system for providing and verifying utilization of certified software upgrades to eliminate vulnerabilities ("patches"); and

- updates to systems users on system status, and actions required to improve system reliability and security.

FIDNet will provide Federal systems administrators with the real time capability to analyze incident data and then update system's security and reliability measures across multiple systems.

2.3.1 FIDNet Benefits

FIDNet will provide the first integrated, Federal civilian capability to protect critical Federal information infrastructure. It will help to assure the continued operation of the U.S. Government and the privacy of its communications with all Americans. Other expected benefits of FIDNet include:

- *Enhanced correlation of intrusions and suspicious events across multiple systems and Federal Agencies*.

- *Increased speed of response*: At full operating capability event correlation and response are designed to operate in "Internet time."

- *Better detection of attacks spread over time and space*: Stealthy attacks, also known as 'low flyers,' specifically avoid detection by remaining below the threshold of most Intrusion Detection Systems (i.e., by distributing their network data packets sufficiently wide). Broader data correlation and centralized data analysis and mining will greatly improve the detection of these techniques, which are becoming more common.

2.3.2 FIDNet and Protecting Privacy and Civil Liberties

An ongoing legal review is underway to ensure that FIDNet's design and implementation, as well as the overall FIDNet concept, continue to support the American citizens' privacy rights and are consistent with the Electronic Communications Privacy Act (ECPA) and other law.

A preliminary legal review by the Justice Department has found that the FIDNet concept, as presented, complies with the stringent privacy provisions of ECPA. The legal review, which includes OMB and other Federal Agencies, is ongoing.

Other key points about FIDNet include:

- *FIDNet sensors will not monitor traffic on private sector systems or on any non-Federal systems*. This system is to be the Federal Government's own computer intrusion detection network not unlike those presently operated by other large enterprises. FIDNet's mission is to provide a mechanism to better ensure the integrity of the Federal Government's *own* data systems and networks.

- *FIDNet is not run by the FBI or by any other law enforcement agency.* Instead, it is a service managed and provided by GSA to non-DoD Federal Agencies.

2.3.3 FIDNet Implementation

Deployment of FIDNet will be shaped by the following considerations:

- *FIDNet is only one component of a multi-layered, Government-wide information assurance system*: Protection of Federal systems will require many steps, including training of personnel, development of standards and recommended practices, and actions by individual departments and agencies to improve security.

- *Joint Program Management*: Led by GSA, the FIDNet Joint Program Office will include an interagency management team with representatives from the defense, intelligence, technical, legal, privacy, law enforcement and customer agency communities to refine system parameters, and work in consultation with private sector information systems security vendors to develop specific design parameters.

- *Ongoing legal review*: Continuing legal review will ensure that FIDNet design and implementation are at all times consistent with law and supportive of privacy rights and principles. An interagency working group, including the various Agencies with jurisdiction over Federal privacy laws, is similarly conducting the legal review.

- *Research and Development*: Achieving FIDNet's full operating capability will require new and updated technologies focused on automated incident analysis, visualization, data mining, and network discovery tools as they become available for use.

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)

Milestone	Activity	Target Date
2.5	Initiate searches for malicious codes 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.	October 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: Create, Maintain, and Coordinate Robust Law Enforcement and Intelligence Capabilities to Protect Critical Information Systems, Consistent With Law

Built around the National Infrastructure Protection Center (NIPC)**,** the Federal Government is developing a system to provide the Nation with timely warnings and coordinated response to the threat of cyberattack. Other key elements of this system are FedCIRC, the Intelligence Community, and NSIRC. Also part of this system is DoD's Joint Task Force-Computer Network Defense (JTF-CND). Information Sharing and Analysis Centers in the private sector are a needed complement to this system; they are discussed in the Private Sector Plan.

3.1 The National Infrastructure Protection Center (NIPC)

PDD-63 authorized the expansion of the FBI's former organization, the Computer Investigations and Infrastructure Threat Assessment Center, into a full-scale National Infrastructure Protection Center (NIPC). The PDD states that the NIPC "[s]hall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." It further states the mission of the NIPC "will include providing timely warnings of intentional threats, comprehensive analyses, and law enforcement investigation and response."

The PDD places the NIPC at the core of the Government's warning, threat investigation, and response system for threats to, or attacks on, the Nation's critical infrastructures. The NIPC is the focal point for gathering information on threats to the infrastructure as well as "facilitating and coordinating the Federal Government's response to an incident." The NIPC is also responsible for "mitigating attacks, investigating threats, and monitoring reconstitution efforts." However, the PDD further states that, depending on the nature and level of a foreign threat/attack, protocols established between special function Agencies (DOJ/DoD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DoD or the Intelligence Community. The PDD further specifies the NIPC should include "elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach, and development and application of technical tools."

The NIPC has a vital role in collecting and disseminating information from all relevant sources. Thus, the PDD directs the NIPC to "sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant Federal, state, and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity." The NIPC is also charged with issuing "attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators."

In order to perform its role, the NIPC is establishing a network of relationships with a wide range of entities in both the government and the private sector. The PDD provides for this in several ways. First, it states the Center will "include representatives from the FBI, U.S. Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, Intelligence Community, and Lead Agencies." Second, the NIPC will be "linked electronically to the rest of the Government, including warning and operations centers as well as any private sector information sharing centers." Third, all Executive Departments and Agencies are mandated to "cooperate with NIPC and provide it assistance, information, and advice that the NIPC may request, to the extent permitted by law." Fourth, all Executive Departments are also mandated to "share with the NIPC information about threats and warning of attacks and actual attacks on critical government and private sector infrastructures, to the extent permitted by law." To ensure that flow of information is unimpeded—which is imperative when dealing with cyberattacks—the PDD authorizes the NIPC to "establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector might create." The NIPC is organized into three sections: Computer Investigations and Operations; Analysis and Warning; and Training, Outreach, and Strategy.

As part of its mission under the National Plan, the NIPC will do the following:

- *Outreach to the Infrastructure Operators*: The NIPC's Training, Outreach and Strategy Section is formulating a comprehensive outreach plan, with subsidiary plans for each infrastructure sector, that will address this task as well as the specific outreach tasking in PDD 63. The plan contains a variety of outreach activities, including the use of Federal Agency, law enforcement, and DoD contacts in the private sector; new outreach to corporate leaders and industry associations; and cooperation with other government or quasi-government entities that have established relationships with the private sector. The goal of the plan is to connect the NIPC with existing mechanisms for government-private sector interaction and, where no such mechanisms now exist, focus outreach resources to create them in order to establish an efficient flow of information between the NIPC and each infrastructure. Sector Liaison Officials and Sector Coordinators will work jointly with the NIPC to implement the outreach plan.

  The NIPC is developing a "Key Asset Initiative" (KAI) whereby it will build and maintain a database of specific "key assets" within each infrastructure sector (e.g., particular power grids, telecommunications switching nodes, etc.) and points-of-contact at each asset. The objective of the KAI is to:

- identify and enter in a database the key assets of the critical infrastructure sectors;
- develop points-of-contact (POCs) and liaison with the sector asset owners and operators; and
- assist in contingency planning.

An organization, group of organizations, or system will be considered a key asset (within one of the eight critical infrastructure sectors) for purposes of KAI if it is determined that the loss of services or products provided would have a widespread and critical social or economic consequence.

Eventually, the Program will include exercises to test response plans within each jurisdiction and modeling to determine the effects of an attack on particular assets. FBI Field Offices will be responsible for developing a list of the assets within their respective jurisdictions, while the NIPC will maintain the national database. This program will be developed in coordination with Sector Coordinators, Sector Liaison Officials, DoD and other agencies. Because these assets are vulnerable to both physical and cyberattack, the KAI and related response plans, will address both. Further, the NIPC will work closely with the National Domestic Preparedness Office (NDPO) regarding physical threats to the infrastructures.

- *InfraGard*: The NIPC is in the process of establishing lines of effective communications with industry in order to share threat warnings and information. InfraGard is a program designed to address the need for a private- and public-sector information sharing mechanism at both national and local levels. Specifically, its objectives are to:

  - provide members prompt, value-added threat advisories, alerts, and warnings;
  - increase the quantity and quality of infrastructure threat information and incident reports provided to local FBI Field Offices (for coordination, investigation, and follow-up) and the NIPC (for national level analysis and warning);
  - increase interaction and information sharing among InfraGard members, and their associated local FBI Field Offices, and the NIPC, on infrastructure threats, vulnerabilities, and interdependencies;
  - ensure the protection of cyber and physical threat data shared among InfraGard members, FBI Field Offices, and the NIPC through compliance with proprietary, legal, and security requirements; and
  - provide members a forum for education and training on infrastructure vulnerabilities and protection measures.

  During FY00, the FBI will be expanding InfraGard nationwide. This expansion includes the development of a secure alert website that can provide members information about recent intrusions, research related to infrastructure protection, and the capability to communicate

securely with other members. This network will allow the NIPC to rapidly acquire information regarding attacks on U.S. industry and to quickly formulate a response. This program is intended to be complimentary to or amplify alerts issued through a threat and warning system that may be established by the Sector Liaison Official and Sector Coordinator.

- *Vulnerability assessments/Analysis and Information Sharing*: the Analysis and Information Sharing Unit (AISU) will analyze all source information. Infrastructure analysis (e.g., assessments done by the various sectors pursuant to PDD-63); threat analysis (e.g., country or terrorist group threat analysis from the Intelligence Community); and current intelligence (derived from investigative, operational, or private sector reporting) will all be combined to produce infrastructure risk assessments. These assessments form the basis for a variety of products, including alerts and advisories, an *Infrastructure Protection Digest*, and topical electronic reports. These products will be designed for tiered distribution to both government and private sector entities consistent with applicable law through the Watch and Warning Unit. The NIPC will be undertaking risk assessments in FY00, beginning with the telecommunications and energy sectors.

- *Watch and Warning*: The Watch and Warning Unit (WWU) monitors all source reporting and serves as a collection point for information. The WWU will be the focal point for the collection and dissemination of cyber intrusion and infrastructure-related information from open sources, current investigations, intelligence sources, and other agencies, as well as various CERTs and any private sector Information Sharing and Analysis Centers (ISACs) that partner with the NIPC. The NIPC will draft and disseminate warnings, alerts, and advisories involving cyber threats and incidents to Federal, state, and local law enforcement and the private sector. It will coordinate with the FBI's Terrorist Threat Warning System where terrorist groups may be the source of the threat incidents. One WWU goal will be to ensure that all critical infrastructure assets are notified of threat warnings, alerts, and advisories in a timely manner.

  Information gathered by the WWU will be quickly analyzed to determine if a broad-scale attack is underway. If the NIPC determines an attack is underway, it can issue warnings using an array of mechanisms, and send out sanitized and unsanitized warnings to the appropriate parties in Federal Government and the private sector so they can take immediate protective steps. This is a difficult process requiring the design of both procedures for reporting and sanitization, and collection and distribution mechanisms. The NIPC is currently working on these procedures and mechanisms.

  The NIPC is also working on improving lines of communications to get threat warnings out to industry and all government agencies. Currently it relies on existing mechanisms such as Law Enforcement Online and the National Law Enforcement Telecommunications System (NLETS) to reach state and local law enforcement. It is also using the NIPC's web home page, the Awareness of National Security Issues and Response (ANSIR) system, and other mechanisms to reach Federal, state, and local government, as well the general public. The NIPC will continue to work to develop ways to get warnings and threat advisories to entities

not on these systems. The long-term goal will be to develop a comprehensive warning system that utilizes as many existing mechanisms as possible.

As the NIPC matures, the WWU will continue to identify additional appropriate recipients of advisories and warnings, as well as produce a weekly report (mentioned above) highlighting the most important information collected. NIPC staff is developing guidelines for the sharing of information between private sector and government entities to achieve the maximum dissemination of relevant information and analysis consistent with applicable law and the protection of investigative equities and intelligence sources and methods. The NIPC plan includes the relocation of the WWU adjacent to the FBI's expanded Strategic Information and Operations Center; the integration of DoD and intelligence community analysts into the NIPC; and the acquisition of additional technical resources. Currently, the watch is operating 5 days a week, 16 hours a day for normal operations. It plans to have 7 days a week, 24 hours a day operation in 1999 once other Government Agency personnel are on board. In the meantime, procedures are in place to operate the watch center for 24/7 capability in the event of a crisis.

- *Planning and Coordination Activities*: The NIPC is coordinating the production of the Law Enforcement Sector Protection Plan. A Sector Coordinator counterpart has been identified and a milestone plan for the sector has been developed and submitted to the CIAO.

- *Cyber Threat Investigation and Response*: The NIPC provides the principal means of facilitating and coordinating the Federal Government's response to critical infrastructure incidents, mitigating attacks, investigating threats, and monitoring reconstitution of critical cyber assets, including the telecommunications and computer networks on which the government relies. The NIPC is the lead government component for coordinating crisis management in response to attacks on the critical infrastructures.

  The NIPC's national mission has been placed into a new investigative program called the National Infrastructure Protection and Computer Intrusion Program (NIPCIP). This program is contained within the Counter-Terrorism Division of the FBI. NIPCI squads and teams in field offices will conduct computer intrusion investigations as well as respond to threats and collect intelligence under the Attorney General Guidelines for Foreign Intelligence Collection and Foreign Counterintelligence Investigations. The FBI has Computer Crime Squads in 10 large metropolitan field offices. Further, every field division also includes a NIPCI Team. In coming years, the FBI's goal is to have a full NIPCI Team in all field offices. These initiatives are intended to compliment existing computer investigation capabilities of the U.S. Secret Service and other NIPC member agencies.

  As part of its crisis management capabilities, NIPC can respond to significant incidents involving possible violations of criminal law, threats to national security, or threats to the national infrastructures. NIPC has personnel who possess the requisite computer and information security skills and knowledge, and criminal and national security investigative experience. The goal of the NIPC is to respond quickly in the initial stages of a crisis, and to pursue the appropriate law enforcement or national security strategies, depending on the nature of the incident. In order to facilitate this, the NIPC has created a Cyber-Emergency

Support Team (CEST), which will be capable of rapid deployment once full staffing is achieved.

- *Training for Federal, State, and Local Officials on Infrastructure Protection*: The FBI plans to expand the number of technically trained investigators at the headquarters level in the NIPC and in the field offices. The NIPC trained 170 FBI agents and 17 representatives from other law enforcement agencies in 1998. Plans are to train more than 500 law enforcement personnel (Federal, state, and local) in 1999-2000. Additional training opportunities include specialized courses in information security developed by the private sector. The FBI is also expanding its computer forensics program to have at least one full-time computer forensics examiner in each field office.

  The NIPC, in conjunction with NDPO, will be conducting outreach and training efforts for local first responders and state and local law enforcement with regards to infrastructures. The NIPC is seeking to train investigators and at least one trainer from state level investigative agencies in each of the 50 states and the District of Columbia. The NIPC is also seeking to train investigators from the municipalities represented in the Major Cities Chief's and the Major Sheriff's Associations and has been consulting on this with the International Association of Chiefs of Police and the National Sheriffs Association. A larger effort to include the training of 500 state and local law enforcement personnel at a one-week, hands-on course was launched in FY99.

  The NIPC is developing its exercise program to test the operational capabilities of U.S. Government agencies and infrastructure operators to respond to an infrastructure crisis. Planning is currently underway for at least one exercise to occur during 1999.

3.2 Federal Computer Incident and Emergency Response Capability (FedCIRC)

The need for an incident handling capability crossing Agency boundaries has never been greater. Based at GSA, the Federal Computer Incident Response Capability (FedCIRC) is a collaborative partnership of computer incident response, security, and law enforcement professionals to handle computer security incidents and to provide both proactive and reactive security services for the Federal Government.

The primary purposes of the FedCIRC are to provide the means for Federal Agencies to work together to handle security incidents; share related information; solve common security problems; and to collaborate with the NIPC, JTF-CND, and NSIRC. Cooperation is focused on planning future infrastructure protection strategies and dealing with criminal activities that pose a threat to the critical information infrastructure.

FedCIRC accomplishes this effort by:

- providing Federal civil Agencies with technical information, tools, methods, assistance, and guidance;

- being proactive and providing liaison activities and analytical support;

- encouraging the development of quality products and services through collaborative relationships with Federal civil agencies, DoD, academia and private industry;

- promoting the highest security profile for Government IT resources;

- promoting incident response and handling procedural awareness within the Federal Government;

- fostering cooperation among Federal Agencies for the effective prevention, detection, handling, and recovery from computer security incidents;

- providing the means for communication of alert and advisory information regarding potential threats and emerging incident situations;

- augmenting the incident response capabilities of other Federal Agencies, and

- facilitating the sharing of security-related information, tools, and techniques.

The FedCIRC partners have entered into agreements for the exchange of information that, when collected, compiled, and analyzed, enables the Federal Government to defend its resources or quickly recover from events that target the disruption of critical information processing.

3.3 Intelligence Community Role In Information Sharing

The Intelligence Community (IC) is comprised of 13 agencies or elements of agencies and is diverse in its activities regarding the protection of information systems.

Central to the protection of information systems of the entire Federal Government and the Nation is the mission of the IC: to collect, analyze, and disseminate intelligence on foreign threats. This includes both strategic information about the plans and intentions of foreign states and non-state actors, and tactical information about impending attacks (i.e., warnings) and attacks in progress. Mechanisms to disseminate this intelligence to Defense and other Federal users, including the NIPC, are already in place. The IC supports the widest possible information sharing, and will seek to release all possible intelligence within the constraints imposed by protecting its sources and methods.

In addition, IC agencies support the NIPC in its responsibility to gather information on infrastructure threats, facilitate and coordinate Federal responses to incidents, mitigate attacks, investigate threats, and monitor reconstitution. IC officers are detailed to the NIPC to facilitate intelligence sharing and the levying of requirements. NSA, which is responsible for elements of Federal information security, further supports the NIPC with analysis of data from specific incidents.

3.4 National Security Incident Response Center (NSIRC)

The NSIRC is the NSA focal point for addressing computer incidents impacting U.S. Government national security information systems. The NSIRC provides warnings of threats against U.S. information systems in a timely manner and expert assistance to Defense and civil Agencies in isolating, containing, and resolving incidents that threaten national security systems.

The NSA is uniquely qualified to serve its customers/partners because of its ability to perform in-depth technical analysis of serious intrusions and because it is the only organization positioned to link intrusion data to foreign signals intelligence. In its effort to provide threat warning and technical response to cyberattacks, the NSIRC objective is to provide its customer/partners with network attack warning information through time-sensitive reporting, threat and vulnerability reporting based on correlated and fused information and expert technical analysis through computer diagnostics.

The NSIRC will focus its analysis and production efforts on the national-level entities of the network defense community such as the NSC, NIPC, JTF-CND, DISA, and FedCIRC. The NSIRC currently manages a database reflecting computer incidents from across the DoD and a number of civil agencies. For 1998, this NSIRC database recorded more than 5,700 computer incidents, which originated from many foreign and domestic sources. Based on this database, the NSIRC issues alerts and threat advisories that warn the Government network defense community of IP addresses that appear to be the source of system attacks (i.e., "bad addresses"), new or existing hacker groups, or unusual hacking activity.

The NSIRC is composed of four functional areas, yet will leverage any area within NSA to support network defense requirements. The Information Protect Cell is the 7-day-a-week, 24-hour-a-day operation in NSA's National Security Operations Center. The Reporting and Analysis of Network Exploitation Division provides all-source analysis of network incident activity. The Network Intrusion Analysis Capability provides computer diagnostic analysis to provide customers with greater detail of hacker techniques. Finally the Threat Assessment Division provides a more global wide-ranging perspective of threats to U.S. telecommunications and information systems.

Focusing Law Enforcement, Intelligence, and Other Federal Organizations on Sharing Information On Vulnerabilities, Threats, and Warnings 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 to 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: Rapidly Sharing Attack Warning and Incident Information

The information economy rests on highly linked systems. Malicious intrusions are not confined to a single system; viruses can spread rapidly throughout multiple networks. *To effectively address these threats, the Nation needs a system for rapidly sharing information about actual and possible intrusions, indicators of impending cyberattacks, and the means of defending against them.*

The role of the Federal Government here is both to create Federal capabilities for enhanced information sharing, and to encourage non-Federal entities (private sector and state and local governments) to organize themselves for efficient information exchange about cyberattack threats and incidents. In particular, the Federal Government will:

- continue building NIPC's role as the center for Federal information sharing;
- encourage the creation of private sector Information Sharing and Analysis Centers; and
- automate sharing of attack and highly suspicious incident data across the Federal Government through FIDNet, NSIRC, and the JTF-CND.

4.1 Building NIPC's Role As the Center for Information Sharing on Threats and Warnings

In the immediate term, we need to do a better job with the information about intrusions, unauthorized attacks, and threats that we already have available. Systems administrators, both in Federal and private sector service, are usually the first to see evidence of unauthorized intrusions and attacks. Data on unauthorized intrusions and attacks should be sent directly to the NIPC for analysis. Data on system anomalies and other incidents can be sent to ISACs (in the private sector), FIDNet (Federal civilian agencies), and JTF-CND (military entities), as appropriate. Further, per PDD-63, private sector and U.S. Government entities should also contact the NIPC or the local FBI field office directly with information.

Unauthorized intrusion and attack information provided to the NIPC can be combined with intelligence, law enforcement, open source, and other information available to the NIPC. The integration and analysis of all source information will allow for the detection of intrusion activity and patterns that simply cannot be performed by technical means alone.

Federal systems are a prominent target for attempted intrusions, and it is important that incidents involving Federal systems be adequately analyzed, and the resulting insights widely shared. The Plan calls for additional steps to ensure that indications of illegal intrusions in Federal computer systems are reported to the NIPC, and shared appropriately. Further, to implement our information sharing:

- all Executive Departments and Agencies shall share information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures with the NIPC;

- clear policy direction from Agency CIOs and OMB to provide incident information to the NIPC, combined with additional training and awareness for systems administrators, will increase the quantity and quality of information for analysis and subsequent sharing; and

- more effective coordination between and among FedCIRC, other Federal Computer Emergency and Incident Response Centers (CIRCs and CERTs), and the NIPC will also encourage full sharing of incidents involving Federal systems. The CIAO and GSA (which manages FedCIRC) will sponsor a White House conference in FY 2000 for Federal CIRCs/CERTs to further coordination and the development of common operating standards.

The NIPC continues to share the results of its analysis. These include not only InfraGard, but also daily and bi-weekly reports, and special notifications of threatening situations.

Agency Initiative: FAA Computer Security Incident Response Capability (CSIRC)

The FAA Computer Security Incident Response Capability (CSIRC) is a centralized reporting and monitoring function, which will identify, assess, and respond to information system security (ISS**)** incidents. The CSIRC function will cross various FAA lines of business by providing protection for all categories of FAA information systems (National Airspace Systems (NAS), mission support and administrative). Its three principal functions are proactive measures, incident reporting and response, and disaster recovery. An initial operating capability was established in FY99. Full operating capability for a limited number of systems will be attained in FY00. In future years, cost is expected to increase as the capability is expanded to additional FAA information systems (NAS, mission support and administrative).

Proactive Measures

Through coordination with counterparts in other agencies and organizations, the CSIRC will disseminate advisories, bulletins, and warnings relevant to FAA systems. Technical assistance to FAA offices will include implementation of appropriate countermeasures.

The CSIRC will carry out FAA-wide intrusion detection and full-time interception of all network activity that enters each FAA installation, as authorized by FAA management. The CSIRC will support FAA offices by monitoring and analyzing intrusion detection data to identify poor security practices and unauthorized activity.

Incident Reporting and Response

The CSIRC will utilize a Computer Incident Response Team (CIRT) trained in handling intrusions and incidents. The CIRT, consisting of computer specialists, computer scientists, engineers, and on-site system experts, will provide telephone assistance to system administrators and will be dispatched, as necessary, to assist in system recovery from attacks or a disaster. On-site system field personnel are experts at responding to field emergencies and outages affecting the NAS and, as such, will play an integral part of the CIRT.

Disaster Recovery

The CIRT will provide disaster recovery assistance to restore operations. An assessment of damages will be conducted and documented. Once the system is brought to an operational state, appropriate management officials will be the final authority for placing the system back into service.

4.2 Encouraging the Creation of ISACs

For the private sector and state and local governments, the Plan encourages the creation of Information Sharing and Analysis Centers (ISACs). ISACs would share information among corporations and state and local governments, and could receive warning information from the Government.

For those corporations or non-Federal entities 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' this data (e.g., by removing the name of the target). Companies are encouraged, however, to directly inform the NIPC of attacks.

The Federal Government has several roles in encouraging the creation of ISACs:

- *Unilateral sharing of Federally developed threat, vulnerability, and incident data*: The Federal Government has extensive insight and experience with identifying and fixing vulnerabilities, and responding to threatened and real malicious intrusions. This information will be shared with trusted non-Federal entities, such as ISACs, that are in a position to act on this information to improve private sector and state and local government cyber-security.

- *Legal Reforms*: Companies may wish to share information about cyber threats, vulnerabilities, and incidents with other companies, or with the Federal Government, but may be deterred because of concerns about the protection of this information, or resulting liability. Companies wishing to organize ISACs may be further deterred by antitrust concerns. A particular concern voiced by many companies is that information disclosed to the Government could become subject to a request for public disclosure under the Freedom of Information Act (FOIA). In July 1999, the CIAO and the Department of Justice sponsored a White House conference to examine this issue. A working group is currently developing solutions to ensure the confidentiality of private sector information.

  A similar process is underway to develop solutions that will address the private sector concerns regarding liability exposure and antitrust violations.

- *Support for Startup:* Recognizing that some sectors may require limited support to create an ISAC, Lead Federal Agencies will seek budget resources for FY01 to assist in ISAC creation. Any Federal support for ISAC startup will be limited in scope and duration; ISAC constituencies—the private sector and state and local governments—must be willing to provide the necessary long-term support.

4.3 Information Sharing Through FIDNet and the DoD JTF-CND

With current technology, analysis of system anomalies for indication of malicious intrusions is largely human based. So too are the mechanisms for system-wide response. Continued research and development—an important component of the FIDNet program—is intended to increase the

use of automation and artificial intelligence tools to increase the speed and accuracy of incident analysis.

In addition, with further development, more insight than just the fact of attack might be provided. It may be possible to provide information about how the attack developed, the techniques employed, and the way to blunt the attack. Analytic cells would be able to develop system 'patches' to block the attacks. Such notification and response, including the installation of patches, will eventually be largely automated.

As permitted by privacy and law enforcement requirements, FIDNet and the JTF-CND incident detection systems will share incident data between themselves, and with the FedCIRC. Incident data that suggests illegal conduct will be passed to the NIPC.

Program 4 Milestones

Milestones	Activity	Target Date
4.1	DOJ and CIAO will host a White House Conference Center meeting on the Freedom of Information Act and the need to protect 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 (ISACs).	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 ISACs.	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

Program 5: A Nationwide System for Response, Reconstitution, and Recovery

Information warfare attacks may not be limited in their scope to isolated incidents. They may be directed at an entire company 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 analyze software problems disabling the network, design work arounds, and reinitiate network operations.

5.1 Building on the Y2K Experience

Y2K computer systems conversion and critical information system protection share a need to develop rapidly a national capability to reconstitute critical cyber systems that fail. Y2K planners prepared for critical infrastructure systems that may have failed or been attacked during the Millennium transition period. A national system of joint Federal-private sector resources was created in order to monitor, coordinate, and assist, if necessary, in the reconstitution of vital cyber systems during the Y2K rollover.

This national reconstitution system complements the Federal Response Plan. Under the Federal Response Plan, the Federal Emergency Management Agency (FEMA) is designated as the Lead Agency for the full range of consequence management issues during a presidentially declared national emergency. The Federal Response Plan is associated with the Stafford Act and other related authorities; however, these mechanisms may not address reconstituting information systems affected by a cyberattack or Y2K-related systems failure. The Federal response mechanism is designed to deal only with managing the physical and social consequences of a cyber failure.

We need a national capability that complements the Federal Response Plan mechanism and supports efforts to bring vital government and private sector systems back online following a major disruption—irrespective of the origin.

The Chair of the President's Council on the Year 2000 Conversion and the National Coordinator pooled efforts to help develop this reconstitution capability. The Information Coordination Center (ICC) established by the Council works closely with the Critical Infrastructure Assurance Office, and other institutions dedicated to protecting critical infrastructure facilities and systems. PDD-63 calls for the creation of a public-private partnership to protect this Nation's critical infrastructure facilities. The CIAO is charged with coordinating the development of the National Plan, analysis of Federal Government dependencies on critical infrastructures, legislative and public affairs within the Government, as well as conducting Education and Awareness activities. Therefore, aligning the work effort between the CIAO and ICC was an integral component of this Nation's Y2K work efforts.

The principal elements of this system are as follows:

- *Information Coordination Center (ICC)*: The ICC assisted in making preparations for information sharing and coordination within the Federal Government and key components of the public and private sectors, coordinated agency assessments of Y2K activities that could have had an adverse effect on U. S. interests at home and abroad.

  - Both the public and private sectors needed certain information during theY2K transition period. The ICC reported on the status of Federal operations for vital computer systems and critical infrastructures during the Y2K conversion period. In addition, the ICC reported on the status of critical systems identified by Federal Agencies and sector working groups within key sectors at home and abroad.

  - A key feature of this reporting was the relationship between the ICC and private sector-based National Information Centers (NIC). During the conversion period, more than 14 NICs provided relevant details on activities in key industries. These NICs included retail, air transport, natural gas, food supplies, and energy. The Cyber Assurance NIC, created specifically for the Y2K conversion period, encompassed cyber components, cyber security, and the Internet. The Cyber Assurance NIC focused on the health of the Internet and its relationship to supporting the other critical infrastructures.

- If serious emergencies arose during the Y2K conversion period, the ICC would have collected Agency situation reports on the emergency, monitored sector responses, and assisted in coordinating reconstitution capability to the extent appropriate. Capabilities included creating an inventory of assets, marshaling resources, and facilitating the information sharing process. The information collection activities were structured to protect lives, property, and critical infrastructure systems. The ICC was especially concerned with Y2K emergencies that could have adversely affected national interests or public health and safety.

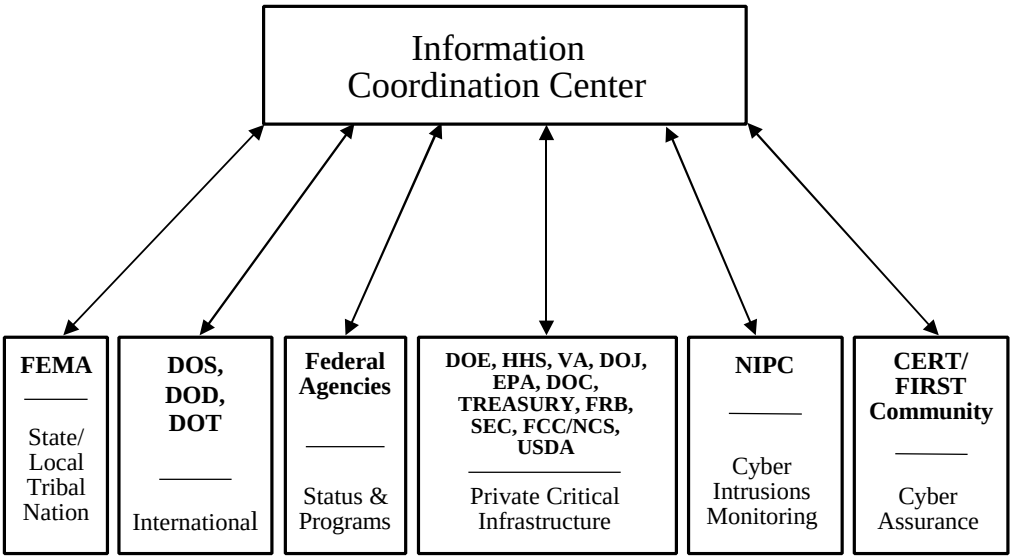
- *NIPC Response Coordination*: Working closely with the Information Coordination Center, the NIPC stood ready to coordinate intelligence and law enforcement capabilities in response to criminal or national security threats that arose during the conversion period. Should a national level event have occurred, the NIPC under PDD-63 would have monitored reconstitution to ensure that response and reconstitution were coordinated.

- *NIPC Y2K Role*: The NIPC maintained real-time awareness of cyber threats or incidents that took place around the Y2K conversion period, disseminated warnings to the appropriate government and private sector parties, and coordinated the Government's response to such incidents.

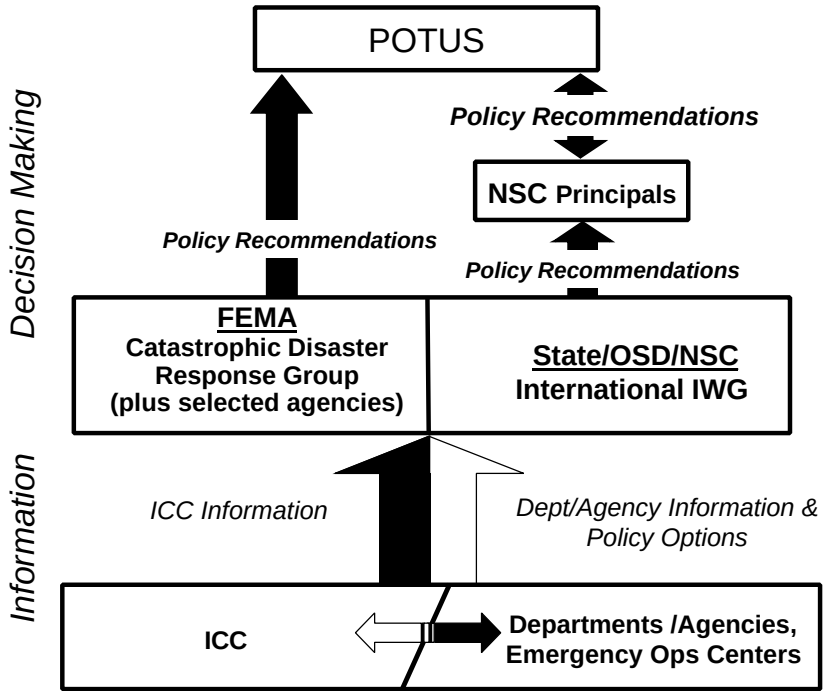
- *A Network of Resources in Key Sectors*: Working with industry associations and other groups, and building on already on-going efforts to prepare for possible reconstitution needs, the Y2K Council and the ICC encouraged the creation of centers or expert teams in each economic sector. These largely private industry Sector Response Centers provided expert assistance and resources.

- *Y2K "Yellow-pages" and Reconstitution Resources*: Building on already prepared resource materials and 'yellow pages' of Y2K assistance providers, the ICC, working in close cooperation with the CIO Council, encouraged the development of capabilities resource guides (both cyber and hard copy) for Y2K responders to assist in providing reconstitution information.

Y2K Information Collection Overview



Y2K Information Flow / Policy Decision-Making



After a thorough analysis of the Y2K "lessons learned" has been conducted, the reconstitution capabilities developed may be leveraged, through cooperation with other Government Agencies and the private sector, into a permanent national cyber-reconstitution capability for responding to major cyber events in coordination with the NIPC.

5.2 Integrating Continuity of Operations and Cyber Response, Reconstitution, and Recovery

In PDD-67, the President directed every Federal Department and Agency to submit new continuity of operations plans by the end of 1999. These plans included measures to support continuity of operations during an information warfare attack.

The Federal Sector Liaisons will work with their counterparts in industry to ensure that corporate recovery plans address information attack reconstitution as well. The 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.

Response, Reconstitution, and Recovery 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

OBJECTIVE 3: ACTIONS TO BUILD STRONG FOUNDATIONS

Program 6: Enhance R&D in Infrastructure Protection

6.1 *Critical Infrastructure Protection Research and Development Initiative*

The Critical Infrastructure Protection Research and Development Initiative (CIPRDI) expands the scope and funding for Federal research and development in critical infrastructure protection. CIPRDI also for the first time coordinates Federal work in this area through the Critical Infrastructure Protection R&D Interagency Working Group, chaired by the White House Office of Science and Technology Policy.

CIPRDI will expand Federal R&D in five key, crosscutting areas that directly support sector specific research needs in all critical infrastructures. Two of the highest priority CIPRDI projects are a program to develop automated tools for detecting trapdoors and other malicious computer code, and a technology development program to provide warnings of anomalous activity within systems.

Vulnerability and Risk Assessment

- *Fielding Enhanced Vulnerability Detection, Assessment and Analysis Tools*: The first objective for this research is to identify, collect, organize, and disseminate infrastructure vulnerability information. The second objective is to develop technologies and methodologies to avoid, reduce, or eliminate vulnerabilities during the development of infrastructure equipment and systems, including hardware and software, and during the integration of such equipment into infrastructures. This research is anticipated to result in a lexicon of threat and vulnerability information, methodologies and information databases on vulnerability and attack taxonomies, and technologies and methodologies to analyze vulnerabilities.

- *Development of Advanced Tools for Risk Management, Performance Assessment, Security Testing, and Metrics*: This research will develop new metrics and measurement tools to gauge such things as infrastructure performance in real time, which is needed to assist detection of performance degradations before they become significant or cascade.

- *Characterization and Notification of Threats*: This research addresses data collection and analysis for the Information and Communications infrastructure. Specifically, data will be collected to assist in characterizing threats in terms of motivation and origin, and to develop tools and technology that would profile attackers and pinpoint attack origins.

Information Assurance

- *Development of Advanced Information Assurance Tools*: This research will develop tools and techniques for rigorous design, implementation, testing, and formal verification of hardware and software components and their subsequent integration into larger systems.

- *Development of Advanced Security Architectures*: This research will organize security components and services to provide confidentiality, integrity, and availability for information and communication systems, and focus on developing the tools and procedures for building the information and communications (I&C) infrastructure with minimal vulnerabilities. Topics covered will include public key infrastructures for public key cryptography; directory and certificate management; interoperability among security components; policies for security implementation in emerging technologies; advanced firewall technologies; packet-switching technologies; secure operating systems for the Internet and automated distribution of patches and information related to security upgrades; scalability and optimization of security architectures; and vulnerabilities in remote control systems.

- *Development of Tools for Automated Distribution, Installation, and Tracking of Software Patches*: This program is designed to develop a set of software tools that will automatically distribute and install software patches in computer systems and networks, track the use of patches, and detect systems in which patches are not properly installed or in use.

- *Understanding Human Factors in Information Assurance*: This program is designed to address the human factors relevant to information assurance and develop strategies and recommended practices to reduce the associated infrastructure security risks. Expected research products are mitigation strategies, recommended practices, and personnel standards.

Interdependencies Among Infrastructures

- *Identification and Characterization of Interdependencies*: This program will identify and characterize the interdependencies among the infrastructures. In particular, the program will address the manners by which disturbances and failures propagate across multiple infrastructures. This program will build upon ongoing programs to further develop a science-based understanding of linkages among, their effects upon, and their implications for critical infrastructures.

- *Development of Advanced Modeling and Simulation Tools*: This program will develop systems analysis techniques, modeling and simulation tools, and databases required to assess vulnerabilities arising from the Nation's interconnected infrastructures. National-level geographic information system (GIS) databases of the infrastructures will be required to fully simulate and analyze the vulnerabilities arising from scaling, complexity, and interdependencies. Test beds may prove critical to analyze effects that cannot be adequately simulated in software models.

- *Consequence Analysis, Risk Management, Protection, and Mitigation Technologies*: This program will develop the methods and tools for assessing the consequences (e.g., national security, economic, and social) of interdependency-related disruptions and for managing risk. This program will also identify existing protection and mitigation measures and technologies that could reduce vulnerabilities arising from interconnections among the infrastructures. The roles of such measures will be characterized from an interdependencies perspective. New protection and mitigation technologies will be developed and pilot tested.

Security of Automated Infrastructure Control Systems

- *Development of Advanced Secure Supervisory Control and Data Acquisition (SCADA) Systems*: This research program will address security issues and vulnerabilities specifically associated with SCADA systems in order to improve security features and protocols, as well as develop new architectures to increase redundancy and reliability.

Intrusion Detection and Monitoring

- *Development of Advanced Artificial Intelligence Software Tools for Trap Door Analysis and Malicious Code Detection*: This program is designed to develop advanced software tools and techniques that can detect and eliminate trap doors and other malicious code in software. Although detecting subtle but intentional alterations to computer code is problematic, these tools will increase the integrity of software products, and thereby reduce the probability of future penetrations and compromises of computers and networks.

- *Development of Advanced Intrusion and Incident Detection and Warning Techniques*: This research will develop tools and procedures to detect, respond to, and recover from incidents, losses in service, or attacks. It will focus on the development of metrics for evaluating false-alarm rates, strategy-based intrusion detection technologies, tools and technologies for use on high-speed networks, scaleable intrusion detection systems, and tools to trace intrusions back to their sources.

Milestones: Critical Infrastructure Protection Research Initiative

Develop a Federal Government critical infrastructure protection R&D agenda, subject to multi-year planning and taking into account private sector research, which will minimize vulnerabilities on a rapid but achievable timetable.

Critical Infrastructure Protection Research Initiative 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

Milestone	Activity	Target Date
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

6.2 Institute for Information Infrastructure Protection (I^3P)

In R&D and other key technical areas, neither private sector market demands nor Agency mission objectives fully meet the Nation's requirements. The Institute for Information Infrastructure Protection (I^3P) will fill these gaps, supporting research and technology development to protect our critical information and telecommunications infrastructures from attack or other failures.

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 institute to address R&D issues associated with information infrastructure protection. PCAST concluded that not only are there no technical organizations dedicated to developing the knowledge and common technology base required to successfully address this problem, but that the private sector does not have sufficient market incentives to fully address these issues on its own. The President agreed with the importance of this mission, and he directed OSTP and the NSC to review the PCAST proposal and provide him with their recommendations. This review concluded that there is both substantial need, and widespread private sector support, for an Institute.

Concept of Operations

The Institute's success depends on effectively meeting the needs of multiple constituencies: concerned Government Agencies and Departments; information infrastructure owners and operators; information technology providers; academia; and companies and communities that rely on critical infrastructures. To meet these needs, the Institute would be structured as follows:

- *The Institute would have only a small expert staff.* The Institute would carry out its missions by funding and tasking existing organizations or groups, similar to how DARPA operates. This operational mode has several advantages:

- It promotes flexibility, quality, and speed. The Institute can direct research funding to the most talented information technology professionals, whether they are located in industry, academia, or government. Furthermore, research priorities can be rapidly adjusted by reallocating funds, without having to overcome the "inertia" of a large, in-house effort.

- "Brick and mortar" start-up costs are avoided, as no new, large laboratory facilities would be required. Core staff would be relatively small, particularly during the start-up phase.

- *The Institute would supplement, not absorb, existing research*. It would coordinate its information infrastructure protection activities closely with ongoing efforts in the U.S. Government, the private sector, and academia. The Institute would also provide demonstration and development support for key foundations of cyber assurance such as benchmarks and standards, provision of "test beds," and curriculum development. This support would assist Federal and private sector CIOs as well as the Information Sharing and Analysis Centers that are being established to serve state and local governments and industry.

  I^3P would concentrate primarily upon funding, coordinating, and integrating research on high-quality science and technology areas not being addressed through existing industry or government programs—it would not compete with industry. It would fund top-quality basic research, and it would also fund and/or conduct more applied activities such as modeling and identifying vulnerabilities in U.S. information infrastructure systems and providing "test beds" for information assurance technologies. Some of these applied activities might be sensitive and may have to be classified. The Institute could emphasize R&D and Analysis into vulnerabilities of broad, systems-of-systems that cross sectors and industries and create risk of large-scale consequences under a concerted attack. Furthermore, the Institute would fund research related to interdependencies between the information infrastructure and other critical infrastructures.

- *Operated through the Commerce Department's 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 Deputy Director/OMB, the Director/NSA, the Director/DARPA, the Director/NIST, the Director/NSF, 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.

Mission and Functions

The missions and functions of the Institute will include, but are not necessarily limited to:

- engaging industry for I^3P's top-level strategy development and program definition;

- funding, coordinating, and integrating research in "shortfall areas" and transferring the results of this research to those institutions in a position to apply them;

- sponsoring a two-way street for public-private collaboration and information sharing;
- providing product evaluation benchmarks, test beds, and tools. In this respect, I^3P would have an Underwriters Laboratory®-like role; and
- supporting academia with training and educating a body of researchers and educators to work in the information assurance field. Support in this area could include, for example, assistance with curriculum development and research grants.

Research Areas

In close consultation with Government and industry, and under the guidance of Federal Coordinating Council, I^3P will determine—and continually refine—its research agenda and its allocation of R&D resources. Consultations to date with private sector, academic, and Government experts have pointed to a number of important candidate research areas for the institute, including:

- physical/cyber/human interfaces;
- intrusion monitoring and response;
- malicious code prevention and detection;
- reconstitution;
- characterizing infrastructures as end-to-end systems;
- establishing information assurance as an engineering discipline, including development of engineering principles and metrics;
- prototyping and testing end-to-end trustworthy systems;
- robustness and resilience of highly complex, nonlinear networks;
- analysis of infrastructure interdependencies, including modeling, simulation, and database development; and
- other shortfalls (e.g., public key infrastructure, testing, security architectures).

Milestones

Milestone	Activity	Target Date
6.6	Creation of the Institute for Information Infrastructure Protection (I^3P) with funding of multiple research projects.	FY 2001

Program 7: Developing a Cadre of Highly Skilled Computer Science and Information Security Personnel—Federal Cyber Services (FCS) Training and Education Initiative

Highly trained information systems security experts are the foundation of the Federal Government's information systems protection program. Unfortunately, these information security experts are in short supply throughout the Federal Government, academic, and private sectors today. The need to ensure an adequate supply of highly skilled Federal information systems security specialists requires a new program—the Federal Cyber Services (FCS) training and education initiative. This initiative encompasses five broad programs that will identify the IT personnel shortfalls; develop new recruitment, education, and retention efforts; provide continuous training and certification for the many dedicated information security specialists already in government service; and provide information security awareness for all Federal workers. The Federal Government will also be working with the private sector, including industry and academic institutions, to determine how best to foster development of the necessary faculty to educate the experts to meet our information security needs.

The information systems personnel shortfall has been previously documented by numerous sources. A 1997 Government Accounting Office report documented the Federal shortfall and concluded that the Federal Government had "a shortage of personnel with the technical expertise to manage controls." On the national level, it is estimated that our economy will require nearly 1.3 million new IT workers during the next 10 years. Surprisingly, the number of computer science degrees went down nearly 30% from 1985-1996, a trend which only recently abated. There is much to be gained through a comprehensive effort to train and educate our IT workforce and provide basic awareness programs for the entire Federal workforce.

In developing the FCS initiative, we can leverage many existing Federal education, training, and awareness programs. In education, the National Security Agency (NSA), has a program to designated universities as Centers of Academic Excellence in Information Assurance Education, based on established criteria rooted in the National Security Telecommunications and Information Systems Security Committee (NSTISSC) training standards. Additionally, the General Services Administration (GSA) has sponsored a CIO University initiative to improve the knowledge and skills of the senior Federal IT workforce. In training, the Defense Information Systems Agency (DISA) has developed information assurance training tools for use in the Defense Department, and then tailored these products for other Federal Agencies. Some Agencies have developed these training tools on their own. The DoD's Defense Information Assurance Program (DIAP) has developed a program to certify DoD information assurance workers based on formal training, on-the-job training, and work experience. The NSTISSC's Education, Training and Awareness focus group's work on national information assurance training standards is also an important effort to leverage. In the awareness field, several Agencies, including DISA, have developed superb INFOSEC awareness training tools. The CIO Council has two committees addressing this issue, the IT Workforce and Security committees, and their inputs are incorporated into the initiative. We will also solicit the expertise of the Federal Information Systems Security Educators' Association (FISSEA) and the Federal Computer Security Program Manager's forum in developing knowledge and skill competencies.

The National Institute of Standards and Technology (NIST) sponsored an excellent interagency review of this issue in April 1998. The report, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST SP 800-16), is a conceptual framework for providing information security training. This report clearly demonstrates the need to conduct *awareness* programs, information security *training*, and *education* of the IT workforce. This report provides the framework on which much of the FCS initiative will be constructed.

7.1 Government-Wide Information Technology Occupational Study

The first step in developing the FCS initiative is the completion of the OPM information technology occupational study. The study will provide a better estimate of the types of IT jobs (for example, Network Administrator, Security Specialist, etc.) in the Federal Government, and more properly define the information security competency requirements of IT jobs. This study is essential to validate the numerous 'anecdotal' evidence of IT security personnel shortfalls in many Government Agencies. Additionally, this study will help identify the training needs of Federal IT personnel.

OPM will conduct an accelerated review of the Government's overall approach to the management of IT occupations, and will develop a competency-based job profile pilot to replace the current minimum qualifications used to select IT personnel. OPM will also develop a new IT job family and specialty titles to replace the outdated IT classification standards. OPM will work with interested Agencies to develop a proposal for any additional authorities and funding that may be required to ensure the Government's ability to recruit, train, and maintain the IT personnel necessary to protect critical U.S. Government information systems. Results of the occupational study will also be used to enhance the recruitment, selection, and training of "Scholarship for Service" and high school program candidates. Data from the IT occupational study will be incorporated in the review and design of the IT compensation system.

7.2 Center(s) for Information Technology Excellence (CITE)

The Center(s) for Information Technology Excellence (CITE) will provide high-caliber, cutting-edge information security training and certification for current Federal IT security employees, Federal contractors, and FCS candidates. The Centers will offer the capability to:

- provide web-based and/or classroom training on the technical competencies for IT occupational specialization required by Federal employees;

- provide training and certification to college and high school students in the Federal Cyber Services career education program; and

- refine, enhance, and maintain currency of the technical competencies of Federal employees and Federal Cyber Services candidates already meeting the certification requirements.

Initially, development of the CITE will focus on providing training for Systems Administrators and Information Systems Security Officers (ISSOs) using existing training standards for these

occupations. Such standards include those used by NSTISSC, the Certification for the Information Systems Security Professional (CISSP), and other national and international bodies. Future expansion of the Centers will focus on the training of System Certifiers, Risk Managers, Computer Scientists, Computer Engineers, Computer Programmers, and Systems Analysts. The certification and re-certification process for current Federal employees and Federal Cyber Services candidates will be modeled after the evolving Department of Defense's certification process for its critical IA personnel, those developed by the CISSP, and other international and national certification bodies. We will recognize the certifications already achieved by those employees who have participated in programs that meet or exceed the minimum standards developed by the CITE. Tracking of certified specialists could be done through the Central Personnel Data File (CPDF).

Developing the Centers for IT Excellence will require the utilization of existing facilities, curriculum, and faculty/instructors. *Any* organization successfully demonstrating the capability to provide knowledge and skills to Federal workers and train Federal Cyber Services candidates on the specific technical competencies required for certification will be considered for inclusion into the Center network. Such organizations may be colleges and universities, existing government training facilities, or private sector based technical training centers. The training organization certification process will be modeled after the evolving NSTISSC courseware and curriculum certification process. We will rely on the CIO Council, the NIST Security Training report, and the OPM occupational study to provide specific guidance and input into what the training and certification standards should be. The goal is to establish a nationwide network of Centers that will provide standardized training to OPM's required Federal IT employee technical competencies.

One promising area for leveraging the work of the Department of Defense is evaluating the newly developed "Advanced Distributive Learning Network" that will deliver web-based and/or computer-based Information Assurance knowledge and skills to DoD's workforce. This network will use the IT security employee training products already deployed, or in development by DISA. DoD has already demonstrated a willingness to work in partnership with civilian Federal agencies to expand the network to cover the entire Federal IT workforce. Delivery methods for this knowledge and skills training can include classroom-based, computer-based, web-based, and distance learning instruction.

7.3 Scholarship for Service Program

The main effort to educate and hire new Federal IT workers and security managers is a "Scholarship For Service (SFS)" program for college students. In this program, the Government would pay for either graduate or undergraduate studies meeting established information assurance standards in return for a pre-determined commitment to Federal Government service.

The SFS program will provide two-year scholarships for M.S. or Ph.D. candidates; two-year scholarships for promising juniors and seniors working towards a B.S. in an accredited information security program; and scholarships for IT security personnel working towards an A.S. or A.A. in an approved two-year IT program.

The SFS program will provide more then just tuition and a modest living stipend. The students will participate in summer work and internship programs at Federal Agencies and participating Government laboratories. For students, this experience will provide guidance on where they may request to be permanently assigned, and it will broaden their knowledge of what skills they need to develop during their academic experiences. For the Federal Agencies, this summer work will contribute to ongoing IT security efforts, and allow for evaluation of the performance of colleges participating in the SFS program. The summer work and internships will also allow for the completion of Federal IT security training programs and subsequent certification at a CITE, permitting students a more rapid and efficient transfer to Federal service upon completion of the SFS program. The SFS students will also participate in periodic conferences, including the National Colloquium on Information Systems Security Education, to encourage sharing of academic and technical experiences. The summer work and internship programs will be managed in cooperation with the high school initiatives discussed in Section 7.4 below.

A key element in the success of the SFS is the identification and accreditation of universities and colleges with information security curriculums for program participation. There are currently few information security graduate programs at American universities. This small number of graduate programs results in a lack of professors and active graduate students in the information security field. The shortfall of information security programs is equally dramatic in the undergraduate curriculum. This lack of information security programs reflected the general decline of computer science degrees where, from 1985-1996, the number of degrees awarded has dropped from 50,000 to 36,000 per annum. The Federal Government must work with the academic institutions and industry to rectify this shortfall.

There are several models in Government for a similar partnership with universities in information assurance program development, including the NSA's National INFOSEC Education and Training Program (NIETP). The NIETP provides standards and guidance for INFOSEC curriculum development, helps develop INFOSEC education infrastructure, and recognizes universities that meet the established criteria for designation as Centers of Academic excellence in Information Assurance Education. To date, eight universities have completed a rigorous application and review process and have been designated as Centers of Academic Excellence. An equal number of universities are expected to apply for consideration during the program's second year. We can work closely with the NIETP and its Centers of Academic Excellence in Information Assurance Education program to identify schools for the SFS initiative.

The larger Federal community must agree to the criteria for accreditation, which are established for identifying and recognizing leading universities in the information assurance arena. (The criteria for the NSA Centers of Excellence in Information Assurance Education program are based on NSTISSC training standards agreed to by 21 Federal Departments and Agencies.) The centers must have the capability to deliver state-of-the-art IT security skill development. Existing and future centers must be evaluated for their ability to provide a source for information assurance faculty development and enrichment. This capability would include:

- delivering Federally certified curriculum;

- teaching entry- and advanced-level teaching skills; and

- augmenting and refining a Federally certified curriculum with appropriate lab exercises, AV programs, distance learning technology, and programs with results in non-proprietary materials.

Three- to five-year evaluations must be instituted in order to promote and assure currency in "excellence." This program will require built-in incentives (i.e., preferential access to grants, etc.), which may require changes in Federal procurement practices. These standards would then be discussed with the broader industry and academic communities in the National Colloquium on Information Systems Security Education.

The CIO Council and GSA have developed a complementary education program for senior executives, the CIO University, a virtual consortium of four universities which offers graduate level programs that directly address the executive core competencies adopted by the CIO Council. The purpose of the CIO University is to improve government information systems management through enhancing the skills of its top IT executives. The program, which ranges from eight weeks to three semesters of course work, can lead to a CIO certificate and possibly an M.S., depending on which university program is chosen.

The identification of universities to partner with the SFS will also contribute to a more consistent and rapid commitment of universities to IT faculty and information security program development, increasing the number of undergraduate and graduate students who would be effectively educated in this field. Some of those graduates would transition into government and industry, while others would remain in the academic programs to meet the growing national need. The partnership could also include Federal assistance in "seeding" the establishment of faculty positions and IT security laboratories at the universities with SFS programs. This will include program efforts at historically black and Hispanic colleges and universities. Clearly the NIETP and CIO University programs offer opportunities for leveraging existing Federal effort in identifying possible universities for partnering.

7.4 High School and Secondary School Outreach Program

One clear trend in the IT field is the ability of young citizens to participate and compete in this world. This opportunity has prompted us to develop a High School and Secondary School Outreach program. The primary goals of this program are to:

- increase the *awareness* of students and teachers at the junior high school level about IT security and the Federal Cyber Services;

- *educate* high school students and teachers about information security and the Federal Cyber Services educational and employment opportunities; and

- *identify* talented students at the high school level, who may want to pursue information security programs at the college level.

The high school outreach program will sponsor conferences, summer camps/work programs, and internships with teachers and students to encourage their participation in information protection curriculum; identify and recruit promising workers for immediate hiring into Federal Government IT positions after high school graduation; and recruit future SFS program candidates. The summer camps could be integrated with Federal training programs (CITEs) to allow for certification of attendees as system administrators, heightening their exposure to Government work and standards, and increasing their value to a Federal Agency as a potential employee.

Educating secondary school students and teachers on information security issues has both academic (i.e., personal awareness, privacy protection, employment, research techniques) and ethical (i.e., school security, personal responsibility) benefits. The Department of Education is already working closely with academia and private industry to develop and promulgate standards and publications on educating our school children on computer security responsibilities. For example, in 1998 the Department worked with the International Society for Technology in Education and various government and civil organizations to develop the National Education and Technology Standards (NETS) program. This program provides four types of standards for early IT education. Additionally, the Department of Education published *Safeguarding Your Technology, Practical Guidelines for Electronic Education Information Security*, a comprehensive primer for developing secondary school education programs. We will continue to evaluate a variety of secondary school computer education programs and consider a Federal website to support curriculum development and distribution.

7.5 Promoting Federal Workforce IT Security Awareness

PDD-63 and the President's Commission on Critical Infrastructure Protection both called for the Federal Government to serve as an example of IT readiness to the private sector. In order to have an effective program to counter threats to Federal information systems, it is necessary to ensure that all Federal workers who may be in a position to identify cyber threats and initiate appropriate action are aware of the threats and briefed on what actions to take. This program is designed to ensure that *all* Federal employees are aware of threats to Federal systems that arise from cyber intrusions; to be able to recognize such events; and to know the steps to follow in response. The strategy is to develop and implement a baseline program of cyber literacy, including briefings and related activities (e.g., CD-ROMs, videos, exercises, workshops, demonstrations, etc.) that can be adapted by each Federal Agency for its own uses. There would also be a range of "awareness acknowledgments" developed and offered for Agency use. The acknowledgments would provide a way of documenting the fact that periodic cyber awareness initiatives were conducted.

This program would be conducted in close coordination with the CITE, using its infrastructure to develop and distribute IT security awareness products. As with the IT security training products, the tools could be web-based, CD-ROM-based, videos, or briefing materials. DISA has already developed several useful "INFOSEC Awareness" CD-ROMs for both DoD use, and tailored products for non-DoD Agencies. We will leverage this existing content development effort. The IT awareness and literacy tools will have to be carefully scrutinized to ensure they are being periodically updated as required.

Milestones: Developing a Cadre of Highly Skilled Computer Science and Information Security Personnel

Institute programs to create and maintain a highly trained workforce of information technology security professionals within the Federal Government. To accomplish this goal, we need to:

- complete a comprehensive Government-wide IT occupational study which will identify all IT security positions, and ascertain the competencies needed to fill the position;
- establish a program to train and certify existing Federal information technology employees in information systems security;
- create a Scholarships for Service program to provide scholarships in information systems security in exchange for Government service (at accredited universities), and develop information security faculty and curriculum;
- design an outreach and awareness program for high school and secondary school students and teachers to encourage future Federal IT workers, and educate all students on computer security ethics; and
- develop and implement a Federal INFOSEC awareness curriculum.

The Federal Cyber Services (FCS) Training and Education Initiative
Information Security Personnel Milestones

Milestone	Activity	Target Date
7.1	Begin university outreach effort to promote SFS program. Develop certification for SFS candidates and develop 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.	May 2000
7.6	Establish the standards that institutions will have to meet to be designated as CITEs.	June 2000
7.7	Design and implement the high school and secondary school outreach programs to include conferences, summer work and internships.	July 2000

Milestone	Activity	Target Date
7.8	Designate the universities selected to participate in the first year of the SFS program.	Summer 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 the Federal IT workforce.	Summer 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: Outreach and Awareness

8.1 Partnership for Critical Infrastructure Security

Keeping critical information systems secure from serious malfunction and outside attack will take an unprecedented partnership between private citizens and businesses, state and local governments, and the Federal Government. To succeed, this partnership must be based on public awareness and an understanding of the threat and how to meet it.

The *Partnership for Critical Infrastructure Security* will be a national collaborative effort between industry and Government, to focus attention on the urgent need for industry and Government to work together to assure delivery of critical services over our Nation's infrastructures.

The Partnership will feature the support of the highest levels of Government and the heads of many of America's major corporations. It will establish a framework and umbrella for a wide array of awareness activities and initiatives.

To this end, the Partnership will sponsor a series of conferences, meetings, and working groups composed of industry and government executives for the purpose of:

- promoting awareness and understanding among owners and operators of critical infrastructures, the risk management community, the general business community, state and local governments, and, ultimately, the American public;

- facilitating future industry contributions to the National Plan; and

- identifying and addressing issues of mutual concern, including but not limited to information sharing arrangements, legal and regulatory reform, standards and best practices, education and training, and research and development initiatives.

The Partnership will proceed based on open and voluntary membership; mutual trust; regular interaction; full understanding of each participant's values, expectations, needs, concerns, and individual objectives; and achieving clear, focused, and well-defined goals.

The CIAO will coordinate the Federal Government's participation in the Partnership. It will work with the Federal Lead Agencies and their private sector counterparts to develop strategies and plans to increase the effectiveness of the Partnership and provide program guidance and materials to support its efforts and participants.

8.2 CyberCitizens Initiative

The Information Technology Association of America (ITAA) and the Justice Department have created a complementary national campaign to educate, raise awareness, and provide resources for additional joint public-private action. The CyberCitizen's Initiative will:

- engage and educate children, young adults, and the wider user community on the basics of critical information protection and security, and the limits of acceptable online behavior. The initial focus will be on child users in grades K through 8, explaining the importance of computer usage ethics;

- publish a computer and network security directory to help public and private sector organizations quickly find the computer security resources they need to protect information assets; and

- establish a formal personnel exchange program between industry and the Federal Government to promote education and awareness, enhanced product development, and greater cooperation.

Just as America's decision-makers must understand and take action to protect our cyber-systems, so too must all Americans understand the importance of appropriate behavior on the Internet and other information systems.

8.3 Training for Federal Employees

If the Federal Government is to be a model for information systems security, then all Federal employees must carry that message. An important first step in achieving this goal is to ensure that the message of cyber-security and good information systems practices reaches the several million dedicated civil servants—and is reinforced by the actions of their managers.

Every year, all Federal employees are educated in important national priorities, such as the importance of ethical behavior in their positions of public trust. Similarly, we will seek to ensure that all Federal public servants are made aware through regular training sessions of the need for information systems security, and the simple but necessary steps that they must adopt to ensure that Federal and national systems are not compromised.

Milestones: Outreach and Awareness

Outreach and Awareness Milestones		
Milestone	**Activity**	**Target Date**
8.1	Educate America's children about appropriate behavior and ethics in using computer systems through 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*.	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: Legal and Legislative Analysis and Reform

Federal Government efforts to advance critical infrastructure assurance require a careful review of law and policy. For more than four years, this Administration has methodically examined various approaches to legal reform. With regard to the legal reform process, seven principles have consistently surfaced.

First, legal reform must evolve as part of a focused dialogue and a diverse partnership. Critical infrastructure assurance policy cuts across private sectors, as well as political and geographic boundaries.

For these reasons, any successful legal reform effort must engage:

- a wide range of Executive Branch agencies;
- institutions that are part of the Executive Branch, such as the CIO Council and the President's Council on Integrity and Efficiency;
- Congress, including its Agencies, such as the U.S. General Accounting Office;
- the Federal and state judiciaries, as well as state and Federal prosecutors and the U.S. Sentencing Commission;
- state and local law makers, regulators, and first-responder communities;

- academia, including think tanks and research institutes; and

- private industry, including trade and professional associations.

Second, the Administration does not intend to create and implement a wide range of new legal regimes. Both Congress and Executive Branch agencies have already created law to address many of the critical infrastructure needs discussed in this Plan.

Third, the Administration will build upon existing policies and institutions in lieu of creating new legal and political structures. As an example, banking regulators have converted existing reporting mechanisms to incorporate cyber-related intrusions; previously, the Suspicious Activity Report covered physical, but not necessarily cyber-related threats. A recently issued Bulletin from the Office of the Comptroller of the Currency raises awareness of threats and vulnerabilities created by cyber-terrorism to the financial services industry. Other agencies are similarly harmonizing available programs to encompass both cyber and physical issues.

Fourth, where new laws are needed, the Administration should focus on solutions that reduce impediments to critical infrastructure assurance without increasing regulatory burdens for government and industry. Existing law, for example, may complicate information sharing between government and industry. Legal adjustments should foster greater information sharing without adding new layers of regulation or complicating the government's existing missions.

Fifth, legal reform strategies must leave room for technological change and development. Technological advancements may, in effect, supersede Congressional statutes, as well as Agency regulations. For this reason, lawmakers have a responsibility to understand technology—especially its impact on existing law. Critical infrastructure policy formation may suffer until government officials accept this responsibility and work with technicians, systems administrators, and others who best understand our cyber networks and critical systems.

Sixth, legal reform must build on specific studies and findings in the area of critical infrastructure assurance.

This Administration embarked on a careful study of infrastructure assurance in 1995, with the commissioning of the Critical Infrastructure Working Group (CIWG). Chaired by Jamie Gorelick, who served as Deputy Attorney General at the Department of Justice, the CIWG discussed and debated optional long-term strategies for addressing threats to infrastructures. Significantly, the CIWG created a methodology based on "critical infrastructures" and both physical and cyber threats. The President subsequently incorporated this approach in Executive Order 13010, which formed the President's Commission on Critical Infrastructure Protection (PCCIP).

The PCCIP studied legal reform options for 15 months. This extensive and comprehensive examination included outreach directly with numerous government communities, including law enforcement, general counsel, intelligence, chief information officers, and defense. Commissioners, who represented a broad segment of government and the private sector, vetted

legal methodologies and topics extensively. The PCCIP's findings and conclusions—published as *Legal Foundations*—represent knowledge and experience that should be used further to develop legal reforms. Since May 1998, the National Coordinator has managed an extensive interagency review of critical infrastructure recommendations. This knowledge should be considered in implementing the Administration's initiatives.

Seventh, legal reforms must identify and foster wholesale respect for privacy rights and civil liberties. On this issue, the Administration has been clear and consistent: critical infrastructure assurance polices must continue to enhance privacy rights and other Constitutional protections, as well as the proprietary rights of American businesses. This Plan includes a separate section on civil liberties, which describes this commitment in greater detail.

9.1 Reviews Are Necessary Before National Plan Implementation

Within this context, the Administration will review existing legal authorities and requirements to implement the Federal Information Assurance Plan. The Department of Justice will have the lead responsibility to coordinate legal reform developments. The review, and as appropriate the Administration's legislative package, may include the following elements:

9.1.1 Enable the Federal Government to demonstrate its commitment to the protection of critical infrastructures and lead by example.

- *Procurement Reform*: The Federal Government should, where feasible, incorporate infrastructure assurance concerns into substantial and pending procurements. The availability of waivers and other gaps in procurement policies and regulations may, however, undermine significant infrastructure assurance objectives.

  Legal reform will examine whether assurance objectives are being considered; indicate how such objectives may be adapted; and propose revisions for future procurements. Legislation, including the Paperwork Reduction Act of 1995 and Clinger-Cohen Act of 1996, requires that Agencies focus on information technology procurements and information resources management. Any legal reform should build on these foundations, in addition to institutions such as the CIO Council.

- *Standards and Certifications*: The Federal Government should serve as a model for the private sector with respect to information security standards and compliance with those standards. Standards can provide a foundation for government-sponsored certification programs to signal compliance with security-related objectives. Government-sponsored certification programs will be created that do not require large bureaucracies to oversee implementation and enforcement and which make available various incentives to encourage private sector participation.

- *Performance Measurements*: The Government Performance and Results Act (GPRA) requires five-year strategic plans and performance measures for major functions and operations of Federal agencies to be reviewed by the Office of Management and Budget in the budget process. The Clinger-Cohen Act of 1996 requires that performance measures

relate to the use of information technology. The required performance measures do not, however, specifically include information security.

Federal Agencies should be encouraged to include assigned infrastructure assurance functions within their GPRA strategic planning and performance measurement framework. Proposals will be discussed to amend Clinger-Cohen to require that Agency Chief Information Officers develop performance measures for the security of their information systems and to submit evaluations to OMB as required by law. National security elements may be exempted from submission of quantitative performance measures for selected systems, if it jeopardizes national security. Legal reform efforts should engage the Government Accounting Office, which has carefully studied these issues and offered various corrective recommendations.

- *Intrusion Detection*: Developing systems to assess, warn, isolate, and reconstitute essential information is fundamental to the long-term success of this plan. Deployment of Intrusion Detection Systems (IDS), as outlined in this plan, raise various legal and policy issues, all of which the Administration must address carefully.

  Principally, the Department of Justice, as part of the interagency process, will explore these issues. Significant legal reform topics include:

  - the extent of government involvement in the development of IDS products;
  - Federal Government liability for failure to protect database contents adequately;
  - procedures for monitoring, accessing, using, and disseminating information;
  - policies for distinguishing voluntary disclosures from those obtained without consent; and,
  - a comprehensive list of privacy and civil liberty issues associated with IDS.

INSPECTORS GENERAL

Future Role of the Inspectors General
Cyber Intrusions, Auditing, and Law Enforcement for Critical Infrastructure Protection

Since 1978, Federal Agency Inspectors General have played an important role in developing, auditing, and enforcing Federal Government management and security practices. Legal reform and National Plan implementation (as they develop) will incorporate roles, responsibilities, and the active participation of Federal Agency Inspectors General.

At this time, the President's Council on Integrity and Efficiency (PCIE) and the Economic Council on Integrity and Efficiency (ECIE), formed by Executive Order 12805 in 1992 (*Integrity and Efficiency in Federal Programs*), are exploring models for participating actively in the critical infrastructure protection process. According to the PCIE, overall objectives include examining the adequacy of:

- Agency *planning and assessment* activities for protecting critical, cyber-based infrastructures;
- Agency *implementation* activities for protecting their critical, cyber-based infrastructures;
- Agency *planning and assessment* activities for protecting their critical, non-cyber infrastructures; and
- Agency *implementation* activities for protecting their critical non-cyber infrastructures.

Specifically, the Inspectors General have announced that they are additionally reviewing the adequacy of agency activities in the following risk areas: risk mitigation; emergency management; interagency coordination; resource and organizational requirements; and recruitment, education and awareness.

9.1.2 Enable the establishment of an effective government-industry partnership.

- *Legal impediments to information sharing*: The success of an information sharing mechanism for infrastructure assurance will, in large part, depend on the creation of a trusted environment where participants—both government and the private sector—are encouraged to share sensitive information on a voluntary basis. Several legal impediments currently exist that may prevent or discourage such participation. These include apprehension over potential liability (e.g., antitrust, tort), national security concerns, classification of information, legal processes compelling public disclosure, and concerns over the protection of proprietary and trade secret information.

  The Freedom of Information Act and other related laws control the conditions under which information in the possession and control of Federal Government Agencies can be made available to the public. Potential participants in an information sharing mechanism may

require some degree of assurance that the sensitive information they contribute will remain confidential if shared with the Federal Government. Federal Agencies may require some degree of assurance that the sensitive vulnerability information they develop and share to protect the infrastructure will not be subject to full public release. The Administration's legal review will focus on legal or process reforms that may effectively overcome these and other similar obstacles.

9.1.3 Eliminate unnecessary legal impediments to facilitate the recruitment and retention of a sufficient cadre of information technology expert personnel to assure the protection of the Federal Government's own critical systems.

The Administration will support OPM in its examination of relevant issues. Legal reform may require interagency discussions on the full range of solutions.

9.1.4 Federalism issues require review of partnership framework

Federalism issues pervade critical infrastructure assurance policies and programs. This Administration consistently defines critical infrastructure assurance as a partnership—whether between public and private sectors, different government Agencies, or between state and Federal actors. It is possible, therefore, that many complex jurisdictional issues will be settled within the partnership framework, while others will require further study.

- *State laws impact on critical infrastructure assurance*: Following the principles and policies outlined in Executive Order 13132, "Federalism," of August 5, 1999, the Administration will identify areas where state laws may interact—positively and negatively—in achieving the objectives outlined in this plan. As discussed in the introductory principles to this section, critical infrastructure assurance must include a wide range of partners and discussions. Dialog with significant representative organizations, such as the National Association of Attorneys General, National Governors Association, Council of State Governments, U.S. Conference of Mayors, National Association of Counties, National Conference of State Legislatures, state sentencing commissions, and emergency management associations may lead to model codes. There are other state and local entities that must be engaged to develop and foster critical infrastructure assurance legal reforms.

9.1.5 Jurisdiction: Conflict, Overlap, and Clarification of Roles and Responsibilities

The interagency review will include a comprehensive examination of Agency jurisdiction issues. Agencies' roles and responsibilities are creatures of the Agencies themselves and the charters given by Congress, or the President through the Reorganization Act. Thus, although Congress and the Executive Branch define the legal and policy-making functions of different agencies, the critical infrastructure mission adds a layer that does not necessarily fit into existing molds.

Legal reform discussions include jurisdiction overlap, resolution of potential conflicts, and identification of gaps in policy implementation. Specific examples include:

- cyber intrusions and roles and responsibilities of the Inspectors General;

- effective and comprehensive implementation of Computer Security Act policies;

- Defense Department, Intelligence, Law Enforcement and Civilian government cooperation to address cyber intrusions and related investigations;

- overlapping missions of the Security Policy Board and the National Security Telecommunications and Information Systems Security Committee; and

- implementation of national security and emergency preparedness telecommunications authorities in the context of various information systems.

9.1.6 Emergency Response Plans and Mechanisms

Critical infrastructure assurance emergencies may invoke existing emergency response plans and mechanisms. Similarly, Congress, the President, and Executive Branch Agencies have written emergency response authorities to support these mechanisms.

The interagency process will consider how existing authorities and plans already exist to support critical infrastructure issues. Where there are gaps, the review should result in suggestions for amending existing authorities and plans. State and Federal planning mechanisms should be reviewed to ensure that all appropriate measures are taken to prevent waste and confusion. Several examples include:

- Federal Response Plan & Emergency Support Functions (all purpose)

- National Plan for Telecommunication Support for Non-Wartime Emergencies

- FBI Incident Contingency Plans

- HHS Health and Medical Support Plan for the Federal Response to Acts of Chemical/Biological Terrorism

- Federal Radio navigation Plan (GPS)

- National Contingency Plan (Oil Spill)

- Federal Radiological Emergency Response Plan (radiological emergencies)

- State and private sector plans.

9.1.7 Other: Legal Reforms

The Administration will carefully monitor discussions in the interagency process for other areas requiring examination and possible legal reform.

4C: THE DEPARTMENT OF DEFENSE INFRASTRUCTURE ASSURANCE PLAN

The Department of Defense will ensure the availability, integrity, survivability, and adequacy of those assets, both domestic and foreign, whose capabilities are deemed critical to DoD force readiness and operations across the military operational spectrum. The Department of Defense's strategic goal is to ensure that national and international infrastructure dependencies do not adversely affect its ability to fulfill its mission of national defense and global force projection.

Nowhere in the Federal Government is our reliance upon information technology (IT) more apparent than in the Department of Defense. The DoD utilizes IT to provide more reliable intelligence, radically improve command and control, standardize business practices, and develop more powerful weapons systems. The DoD, because of its national defense missions, has led the charge to protect our critical infrastructures from cyberattack and other events that threaten our national security.

Critical Infrastructure Protection (CIP) is about ensuring those infrastructure assets that DoD needs to execute its missions and functions are available when needed. CIP looks at what we use to meet our defense mission (e.g., facilities, equipment, information systems, networks, people, contracts), determining the critical assets, identifying their associated vulnerabilities, recognizing interdependencies, and taking measures to protect them. CIP takes a defensive view of the world, not an offensive one. While the DoD has long been concerned with protecting its individual facilities (e.g., bases, installations), both here and abroad, looking at how those facilities depend on each other and on services from the private sector requires a slightly different point of view.

Formulating the Plan

The Defense Infrastructure Assurance Plan includes three unique elements that provide a useful framework to help build the Federal Government plan and private sector framework. DoD has created organizational structures to identify and fix vulnerabilities; developed and deployed intrusion detection systems; and launched key innovative research and development projects.

The DoD plan encompasses the physical and cyber dimensions of CIP. It is the basis for a continuing process, which addresses the entire national defense operational spectrum, including business continuity processes; recognizes and understands critical infrastructure interdependencies; engages and integrates traditional security disciplines and information assurance; leverages recent DoD initiatives and the ongoing activities needed to meet current and future DoD, National Infrastructure, and Information Assurance challenges; and necessitates a DoD-private sector partnership.

The DoD achieves critical infrastructure protection through the application of the following six activities:

- Analysis and Assessment;
- Remediation;
- Indications and Warning;

- Mitigation;
- Response; and
- Reconstitution.

Valuable Application:	***Both physical assets and information-based activities are protected through these six protection activities.***

Scope of the Defense Infrastructure

In today's global information environment, the IT revolution is permeating every corner of the Defense missions of the United States.

- Soon our soldiers on the battlefield will have communications that allow their commanders to know precisely the individual soldier's position, situation, and even heart rate, i.e. almost complete "battlespace awareness."

- We are using the Internet to meet a wide variety of our requirements from travel payments to satellite communication to electronic commerce.

The Defense Infrastructure (DI) is a complex, interdependent, and decentralized network of systems, services, people, and processes—including private sector and other Government functions—that cross Defense organizational boundaries providing goods and services to meet Defense requirements. The DI is categorized into 11 sectors (e.g., finance, logistics, transportation, personnel). These sectors are composed of assets that may be either simple (a facility or a single information system in one geographic location) or complex (a set of geographically distributed facilities, systems, links and nodes). For example, DoD operates a multitude of military bases, including ships, which are much like small towns with a power grid, heating systems, air filtration, automatic locking devices, local area networks, information systems, and chronometers on ships and planes.

To expand on the DI description, it consists of the web of information and communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of Defense users across the range of military operations.

The DI encompasses sustaining bases, tactical, and defense departmental information systems; command, control, communications, computers, and intelligence interfaces to weapons systems; and the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery.

The applications and data engineering tools, methods, and processes to build and maintain the software for command and control; intelligence; surveillance and reconnaissance; and mission support users who access and manipulate information in fulfillment of their requirements also make up a portion of the DI. In addition, the DI is anchored with the standards and protocols that

facilitate interconnection and interoperation among networks; and the people and assets, which provide the integrating design, management, and operation.

The DI rests on a foundation of effective information and communications. The DI shares the vulnerabilities of the National Information Infrastructure (NII), but due to its defense mission, has additional vulnerabilities to deal with. These are also subject to the same business forces that exploit those vulnerabilities in the private sector.

CREATING THE FOUNDATIONS FOR (1) PREPARE AND PREVENT, and (2) DETECT AND RESPOND (Programs 1-5)

The DoD was among the first Federal Government entities to develop a plan of action to assess and eliminate significant vulnerabilities to infrastructure and information attacks on its critical systems, missions, and installations. The Defense Critical Infrastructure Protection Program through the Critical Infrastructure Protection Integration Staff will provide oversight, leveraging current DoD efforts and capabilities, and integrating related programs (e.g., DIAP, Critical Asset Assurance Program, Infrastructure Assurance Protection Program) to ensure success. Also, DoD is taking the lead in training its personnel on how to deal with critical infrastructure protection.

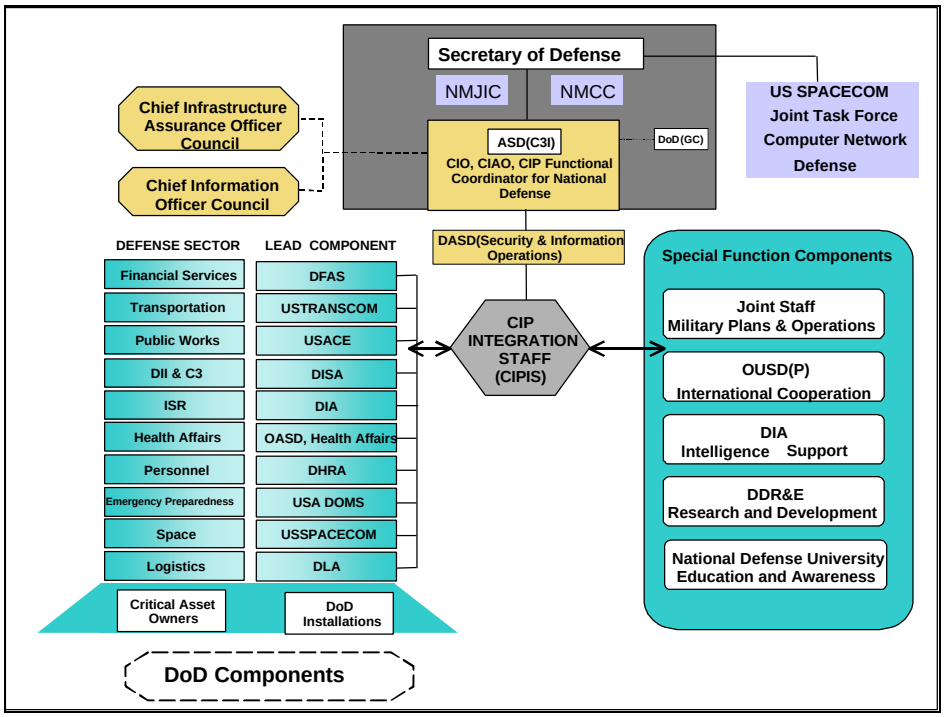
The elements of the Defense Critical Infrastructure Protection Program advance both the *Prepare and Prevent* objective of the Plan, and the *Detect and Respond* objective.

Critical Infrastructure Protection Program (CIPP)

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence [ASD (C^3I)] develops DoD CIP policy and serves as the CIP Functional Coordinator for National Defense and DoD representative to the Critical Infrastructure Coordination Group (CICG); and the DoD's Chief Information Officer (CIO) and Chief Infrastructure Assurance Officer (CIAO).

The DoD Director for Infrastructure and Information Assurance chairs the CICG National Defense Coordination Sub-Group. Proposed membership includes National and Defense Sector Liaisons and Special Functions Agencies. This is a permanent sub-group to the CICG for coordination of national defense-related issues. Its purpose is to assist the Functional Coordinator for National Defense in the planning and provision of infrastructure services required for national defense under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

The Department's Critical Infrastructure Protection Plan is the vehicle by which it will meet PDD-63 requirements and institutionalize critical infrastructure protection. DoD's desired end-state is that all aspects of critical infrastructure protection will be institutionalized. The following depicts DoD's organizational structure for Critical Infrastructure Protection.



The Deputy Secretary of Defense assigned DoD Lead Components Defense Sector responsibilities. The assignment of Lead Components for a set of infrastructure "horizontal processes" represents a major institutional change in the way the DoD does business. Through this structural change, the Lead Components take responsibility for developing a comprehensive institutional focus on the assurance of each Defense Infrastructure.

The Defense Sectors and Lead Component are identified below:

Defense Infrastructure Sector	**Lead Component for Sector Assurance Coordination**
Financial Services	Defense Finance and Accounting Service
Transportation	U.S. Transportation Command
Public Works	U.S. Army (Corps of Engineers)
Defense Information Infrastructure Command, Control, & Communications (C^3)	Defense Information Systems Agency (DISA)
Intelligence, Surveillance and Reconnaissance	Defense Intelligence Agency (DIA)
Health Affairs	OASD, Health Affairs
Personnel	Defense Human Resources Agency
Emergency Preparedness	U.S. Army (Director of Military Support)
Space	U.S. Space Command
Logistics	Defense Logistics Agency

To ensure the planning and assurance activities of the Lead Components are integrated and not "stovepiped," the Deputy Secretary of Defense, in response to PDD-63 and the Department's CIPP, established the Critical Infrastructure Protection Integration Staff (CIPIS). The CIPIS focuses on Defense Sector integration, facilitation, and integrated decision support. The integrated decision support is an active part of the Defense CIP as it permits "focused assurance" when and where the assurance is needed.

Critical Infrastructure Protection Integration Staff (CIPIS)

The CIPIS achieved Initial Operating Capability in July 1999. It provides oversight, leverages current DoD efforts and capabilities, integrates related programs, and establishes partnerships with the private sector. The CIPIS is composed of Defense Sector Liaison officials from throughout the Department and representatives from the Joint Staff, Services, and Joint Program Office–Special Technology Countermeasures (JPO-STC).

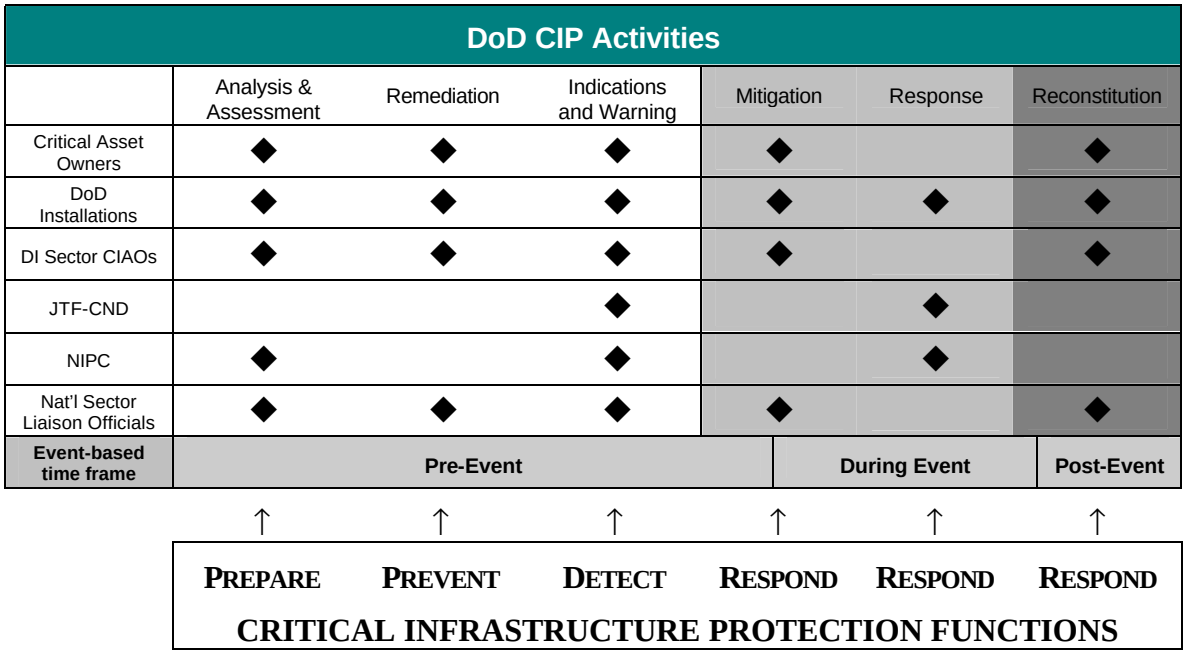
CIPIS functions identify infrastructure assets critical to DoD in the context of existing military operational plans, including business continuity; map Defense Infrastructure to the National and International Defense Infrastructures; ensure qualitative vulnerability and interdependency analysis are performed on designated assets; conduct risk management assessments on designated critical assets and recommend to DoD Chief Infrastructure Assurance Officer and components justifiable security enhancement measures; and coordinate CIPIS findings with appropriate national Lead Agencies identified in PDD-63.

The formulation of all Departmental planning (e.g., Defense Sector Plans, continuity of operations, DII/C^3 continuity of operations integration), policy, and procedures for CIP-related remediation, indications and warning, mitigation, response, and reconstitution efforts are also coordinated through the CIPIS. CIPIS provides the necessary expertise for the development of CIP-related National Defense, National Security, and International Cooperation efforts as stated in PDD-63; and maintains expertise and awareness with the private sector support for respective Defense Infrastructures.

Methodology

The DoD will achieve CIP through the six protection activities that map to the **Prepare**, **Prevent**, **Detect**, and **Respond** functions. Effective management of these activities will ensure that they can be coordinated and reconciled among all entities; recommended practices can be exchanged; and DoD Critical Asset Owners, DoD Installations, Sector CIAOs, and military planners and operators continuously share a coherent and information-rich, risk-based decision framework. The protection activities are aimed at assuring the ability of the DoD to conduct operations and meet mission objectives. The activities integrate physical protection and information assurance into a comprehensive structure.

Six Critical Infrastructure Protection Activities



Infrastructure *Analysis and Assessment, Remediation,* and *Indications and Warning* primarily occur before any event. *Mitigation* occurs both before and during events. *Response* occurs during events, and *Reconstitution* may start during events, but will generally be concentrated afterward. Each protection activity can be independently applied to assure the functioning of physical assets that the DI relies upon and the information-based assets that essentially make up the nervous system of those infrastructure assets. The figure also shows which entities within the DoD and national organizational structures have primary assurance or protection responsibilities in which phases. The Defense Sector Leads will build the protection profile of all critical assets during every phase of their protection activity cycle and during the transition from one phase to the next.

The activities and functions of several entities cross all six life-cycle activities. The DoD CIAO Council provides oversight, resources, and sets priorities for all activities. The DoD CIO Council sponsors development of IT remediation solutions and their incorporation into information systems, enables mitigation activities through IT, and incorporates and leverages IT advances in reconstitution.

The CIP Functional Coordinator for National Defense identifies assets critical to national defense within the national infrastructure sectors, and advocates remediation, indications, mitigation, and reconstitution activities for these assets throughout the DoD protection life cycle. In addition, the Coordinator will monitor sector remediation for those assets and represent DoD requirements and equities in the reconstitution of the national infrastructures. The Coordinator will advocate mitigation planning within national sectors and sponsor "joint" planning, training, and exercise of the coordination and interface between DoD and national activities at all levels.

National Sector Liaisons concentrate their efforts on coordinating the development and implementation of the national sector assurance plans and on maintaining national sector

infrastructure characterization, performing vulnerability assessments, and implementing monitoring and reporting activities. In addition, they will lead in the planning, training, and exercise of mitigation activities, and monitoring reconstitution activities within each sector. They will also share information with the NIPC as appropriate.

Analysis and Assessment

Encompasses a continuum of activities: Critical Asset Identification; Defense Infrastructure Characterization; Operational Impact Analysis; Vulnerability Assessment; and Interdependency Analysis.

A critical asset is defined as any facility, equipment, service, or resource considered essential to DoD operations in peace, crisis, and war that warrant measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration (paragraph E2.1, DoDD 5160.54). Continental United States (CONUS) assets will be identified before Outside Continental United States (OCONUS) assets. Asset ownership (public sector, private sector, U.S., foreign, multinational) will not be a factor in the selection process. Critical assets will change and in some cases, time and context determine asset criticality.

Accomplishment:	***DoD has developed the Registered Asset List (RAL)—a geographic information system containing most of the physical sites and defense sector assets upon which it depends.***

Note that this is the identification of only DoD-dependent assets and this list will not equate to a complete compendium of all national defense and security assets.

Analysis & Assessment Milestones		
Milestone	**Activity**	**Target Date**
1.9	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
1.10	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

DoD Critical Asset Owners have the responsibility, in coordination with DI Sector CIAOs, Military Plans and Operational Functional Coordinator and CIPIS, to conduct asset-level vulnerability assessment; and coordinate with Sector CIAOs, Functional Coordinator for Military Plans and Operations, and the CIPIS. The DoD Functional Coordinator for Military Plans and Operations will conduct operational impact analysis; and identify military operations critical assets.

The CIPIS will conduct defense infrastructure interdependency analysis; operational impact analysis; and defense-wide vulnerability assessment. It will also ensure currency of the defense infrastructure characterization; assist in critical asset identification; sponsor Defense-wide analysis and assessment; and provide technical and systems support and integration for all other levels.

Remediation

Precautionary actions taken before undesirable events occur to improve known deficiencies and weaknesses that could cause an outage or compromise a defense infrastructure sector or critical asset.

For example, the DoD Information Assurance Strategy—**DEFENSE IN DEPTH**—centers on a series of layered defenses, varying in strength and assurance levels, each one designed to meet a specific need. These layers include:

- *DoD Wide Area Networks*: harden against cyberattacks; produce and deploy robust encryption products;
- *DoD Local Area Networks*: deploy boundary protections (e.g., firewalls, guards, virus scanners, intrusion detection);
- *DoD Hosts, servers, applications and operating systems*: employ measures to deter and detect unauthorized actions and implement strong access controls;
- Key management implementation services;
- Mandatory employee training and certification;
- Standardized IT and information assurance job categories; and
- Integration and analysis of physical and cyber incident reports.

This strategy also allows for the implementation of key management services; employee training and certification; standardization of IT and information assurance job categories, and enhanced integration and analysis of physical and cyber incident reports.

Remediation Milestones		
Milestone	**Activity**	**Target Date**
1.18	DoD Critical Asset Owners with their Sector CIAOs will provide remediation plan and resource the plan. In addition, DoD Installations will provide installation-level remediation plans with the Sector CIAOs and resource the plans.	November 2000
1.20	DI Sector CIAOs will resource and perform sector-level remediation and integrate and reconcile asset-level remediation plans within each sector.	December 2000

Milestone	Activity	Target Date
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
1.28	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 causal relationships; determining likelihood and range of consequences; assessing extreme events; constructing risk of extreme events; identifying tradeoffs; and identifying and analyzing options.	December 2002

Indications and Warning

Indications and warning include the preparatory actions or infrastructure conditions that signify that an incident is likely, is planned, or is under-way.

DoD Critical Asset Owners and DoD Installations will participate in defining, monitoring, and reporting infrastructure incidents while Sector CIAOs develop and implement sector monitoring and reporting processes. National Military Command Center (NMCC) and the Joint Task Force-Computer Network Defense (JTF-CND) will receive, consolidate, and assess sector reports; develop DoD indications through the fusion of sector reports with traditional intelligence information; report DoD indications to the NIPC; issue DoD warning; and receive, assess, and disseminate national warning.

The CIPIS provides technical integration, support, and process improvements. The DoD Functional Coordinator for Research and Development provides improved materials, tools, methods, and models for detection. The DoD Functional Coordinator for Intelligence Support provides expert advice, assistance, and support to Sector CIAOs in developing and implementing monitoring and reporting processes.

The NIPC will lead the development of national indications requirements; participate in the design and development of national sector monitoring and reporting; receive, consolidate, and assess national sector reporting; develop infrastructure indications through the fusion of national sector reporting and traditional intelligence; and issue national warning.

Accomplishment:	***By installing intrusion detection systems on key system nodes and establishing a 24-hour watch, DoD has increased its situational awareness and fused traditional intelligence information with sector monitoring.***

Mitigation

The actions taken by DoD Critical Asset Owners, DoD Installations, DI sectors, and military operators in response to an infrastructure warning of incident.

DoD Critical Asset Owners and installations will develop, train for, and exercise asset- and installation-level mitigation activities. They will initiate these activities in response to warning, emergency, or infrastructure incident; and report mitigation status to the NMCC, JTF-CND, and affected Sector CIAOs. Sector CIAOs will integrate and reconcile asset-level mitigation planning and activities within the sector, and report mitigation status to the NMCC and JTF-CND. NMCC and JTF-CND will monitor emergencies and incidents and provide mitigation status to affected DoD entities and Component(s); and recommend or direct mitigation activities. CIPIS will provide technical integration support to the NMCC, JTF-CND, and Sector CIAOs.

NIPC will monitor national emergencies and incidents; provide mitigation status to affected national entities; and recommend mitigation activities.

Accomplishment:	***Established positive control over the identification and repair of information systems at risk with the Information Assurance Vulnerability Alert (IAVA).***

Incident Response

Activities undertaken to eliminate the cause or source of an event, including emergency measures from dedicated third parties (i.e., not the asset owners/operators themselves), such as law enforcement, investigation, medical, and fire and rescue.

Incident Response Milestones		
Milestone	**Activity**	**Target Date**
1.19	DoD Sector CIAOs will monitor response activities, coordinate appropriate sector mitigation and reconstitution activities, and provide support to the NMCC.	November 2000

DoD Critical Asset Owners and DoD Installations will coordinate with appropriate response entities, and plan, train for, and exercise local emergency responses. The JTF-CND will respond to incidents impacting assets under its defense. The CIPIS will provide technical support to the NMCC, the JTF-CND, and Sector CIAOs and monitor the status of response activities. The NMCC will monitor status of response activities.

Accomplishments:	***Expanded computer emergency response teams to perform alerts, critical triage, and repair; and developed contingency plans to mitigate the degradation or loss of networks.***

Reconstitution

Actions required to rebuild or restore an infrastructure after it has been damaged.

DoD Critical Asset Owners, supported by DoD installations, will reconstitute assets and report status to the Sector CIAOs. Sector CIAOs will monitor reconstitution activities and share information with the NMCC, the JTF-CND, the NIPC, and the CIPIS; conduct sector level reviews and sponsor or initiate CIP process improvements; and update DI sector characterization.

The JTF-CND will monitor and advise on reconstitution of assets under its defense; and provide input from response after action analysis to Sector CIAOs and affected Component(s) for consideration in reconstitution. The CIPIS, supported by its private sector partnerships and industry expertise, will provide technical support to the NMCC, the JTF-CND, affected Component(s) and Sector CIAOs. The NIPC will provide incident response review results as input to reconstitution planning, and monitor significant national infrastructure reconstitution efforts.

FEMA will function as the Lead Agency for Consequence Management of national emergencies in accordance with the Federal Response Plan.

Defense Critical Infrastructure and Information Assurance-Related Programs

The CIPIS, under the direction and oversight of the Director, Infrastructure and Information Assurance, will integrate and provide oversight to these related programs.

Defense-wide Information Assurance Program

Given the risks and the fact that weakness in any portion of the DII is a threat to the operational readiness of all Components, the Department is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information and the protection of its information infrastructure. Recent assessments, exercises (Eligible Receiver ’97), and real-life events clearly demonstrate that Defense-wide improvement in Information Assurance (IA) is an absolute and continuous operational necessity. We can no longer be satisfied with reactive or after-the-fact solutions. As the Department modernizes its information infrastructure, it must also continuously invest in the research, development, and timely integration of products, procedures, and training necessary to sustain its ability to defend it. Providing for the protection of the DII is one of the Department’s highest priorities and most formidable challenges.

Critical to achieving the Department’s IA objectives—to continuously provide for the availability, integrity, authentication, confidentiality, non-repudiation, and the rapid restoration of mission essential elements of the DII—is the implementation of a DoD-wide planning and integration framework. To that end, in January 1998, the Deputy Secretary of Defense approved the creation of the Defense-wide Information Assurance Program (DIAP), to provide for the planning, coordination, integration, and oversight of the Department’s IA activities and resources.

The DIAP forms the Department's core organizing element for achieving a more comprehensive, coherent, and consistent IA program. It includes a process designed to give central oversight while retaining decentralized execution to realize continuous improvement in our IA posture. The DIAP's central coordination and oversight activities enable the Department to accurately develop, validate, integrate, and prioritize DoD-wide IA requirements; determine the return on our IA investments; and objectively assess our Defense-In-Depth efforts to protect the DII and critical elements of NII and Global Information Infrastructure (GII). Properly constructed and executed, the DIAP process can achieve both necessary and sufficient responsiveness to current and future IA issues, threats, and vulnerabilities. While the DIAP provides a common management framework and central oversight for the Department, the execution of individual Component programs remains the responsibility of the Commanders-in-Chief (CINCs), Services, and Agencies.

Information assurance requires an approach that goes beyond the "classic" protection of DoD's information based principally on national security classification. The approach must consider how critical the information is to mission accomplishment and provide the means, commensurate with that criticality, to ensure that information is authentic, uncorrupted in transmission and available when needed and to ensure the availability of supporting critical infrastructures. IA is also an evolutionary and dynamic discipline that requires flexibility, adaptability and responsiveness to new technologies, and changing threats and vulnerabilities. Creation of the DIAP reflected an increased understanding across the Department that IA is an operational readiness issue and that increasing dependence on interconnected and interdependent systems and services created a shared risk environment, necessitating an unprecedented level of coordination and unity of effort across the Department.

The DIAP resides within the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence [OASD (C^3I)], and is staffed with personnel from the Defense Agencies, the active and reserve forces, and the Intelligence Community. The DIAP Staff is supported through several DIAP liaison positions: the Intelligence Community Coordinator, Critical Infrastructure Protection (CIP) Integration Liaison, and Joint Staff Liaison. The DIAP achieved Initial Operating Capability (IOC) in June 1998 with the assignment of the Staff Director.

The DIAP is composed of two teams: the Functional Evaluation and Integration Team (FEIT), and the Program Development and Integration Team (PDIT). The FEIT contains eight functional areas where program activity initiation, coordination, and oversight occur. Each of the eight functional areas has a Team Leader who initiates, coordinates, and assesses the activities of performing organizations both within and across functional areas. The Functional Areas are: readiness assessment; policy oversight and implementation; human resources development; architectural standards and system transformation; acquisition support and product development; security management; operational monitoring and incident response; and research and technology. Each functional area is supported by its own Department-wide team, which relates the results of its activities to the DIAP's PDIT for use in the DoD's Planning, Programming, and Budgeting System (PPBS).

The PDIT provides oversight, coordination, and integration services for the Department's IA program resources. Using program guidance and other information provided by the FEIT, the PDIT ensures promulgation of this information among the Components. The PDIT monitors the IA plans, activities, and resource investments of the Components and assesses the adequacy of resources necessary to ensure the continuous operational readiness of the DII and its dependencies on the NII and GII. The PDIT is also responsible for documenting a baseline of IA spending across the Department, including those funds identified in the Information Systems Security Strategy (ISSS) as well as additional IA funding appearing in other DoD Program Elements.

The Infrastructure Assurance Program

The Infrastructure Assurance Program (IAP) is a research and engineering program established in 1995 and sponsored by the Office of the Secretary of Defense (OSD) and the Joint Staff. The U.S. Navy is the Executive Service. The Joint Program Office administers the program for Special Technology Countermeasures (JPO-STC). The IAP represents the majority of DoD's investment to-date, both in time and resources, to address DoD dependencies on critical commercial infrastructures. This effort has resulted in an established and proven process tailored to DoD mission needs with important insight regarding other approaches. The process proposed for DoD's Critical Infrastructure Protection will build on the system developed to support the JPO-STC's Infrastructure Assurance Program, and extend it to address DoD infrastructures.

The IAP contributes the following to the DoD CIP effort:

- engineering methods, metrics and tools for all activities in the CIP analysis and assurance life cycle phase (critical asset identification, defense infrastructure characterization, operational impact analysis, vulnerability assessment, and interdependency analysis) customized for all levels (asset, installation, defense infrastructure sector, military operation, and defense-wide);

- centralized DoD expertise in and responsibility for infrastructure interdependency analysis and mapping DoD critical assets and Defense Infrastructure to National and International Defense Infrastructure;

- infrastructure information security research and standards; analytic and integration support to Military Plans and Operations and Intelligence Support; and information engineering.

Public Key Infrastructure

A Public Key Infrastructure (PKI) is comprised of the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates. A PKI is necessary for the wide-scale, interoperable use of public key technology to support digital signatures, confidentiality, and other security services, which facilitate the trusted electronic exchange of information. As PKI products and services have developed in the commercial marketplace, the Department of Defense (DoD), like other federal departments and agencies, has adopted and adapted, the technology to maximize the use of these commercial capabilities and

minimize expensive government developments. The Department established a number of pilot initiatives to place the technology in the hands of the user community and to further understanding of the issues and challenges in fielding a large scale PKI.

To ensure interoperability among DoD users and to minimize operational costs, the DoD will employ a PKI that is under a centralized management structure yet supports outsourcing and distributed Service/Agency operation of some of the PKI components. The enterprise-wide PKI will address a variety of security token technologies, support both commercial and federal standards, and meet overall DoD objectives for secure electronic transactions within DoD and with elements of the private sector.

To better focus the Department's PKI efforts, a PKI Roadmap and X.509 Certificate Policy were developed. These documents help both the user and vendor communities to understand the Department's PKI goals and objectives, a strategy for implementation, and the timeline associated with the availability of critical technology and processes. In April, 1999, to provide the management attention and oversight required to achieve these objectives, the Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) assigned program management responsibility for the DoD PKI to the National Security Agency (NSA) and Defense Information Systems Agency (DISA). The Program Manager is from NSA, while the Deputy Program Manager is from DISA. The Program Management Office is located at NSA.

In addition, on May 6, 1999, the Deputy Secretary of Defense established a Department-wide PKI policy to provide the underpinning of Service and Agency strategies in support of the Department's PKI goals and objectives. The DoD PKI Policy:

- emphasizes the importance of achieving Information Superiority by requiring that DoD IA capabilities address the diversity and pervasiveness of information, information systems, and infrastructures, to support warfighting and business operations;

- seeks to maximize the use of commercial-off-the-shelf (COTS) technology, as appropriate, in order to keep up with technology evolution, and develop Government-off-the-shelf (GOTS) solutions only when necessary; and

- establishes critical milestones to aggressively implement a DoD PKI that meets the requirements for all Information Assurance services, encourages widespread use of public key-enabled applications and provides specific guidelines for applying PKI services throughout the DoD.

DoD PKI Implementation Milestones		
Milestone	**Activity**	**Target Date**
1.25	Signed Electronic Mail: All electronic mail will be signed; encryption of mail is encouraged, throughout DoD.	October 2001
1.27	DoD will issue its most secure Certificates/Tokens to all users in implementing its PKI.	January 2002

OBJECTIVE 2: DETECT AND RESPOND *(CIP Efforts Highlighted) (Programs 2, 3, 4, 5)*

The most dramatic difference between DoD's CIP efforts to date and the rest of the Federal Government and the private sector appears in DoD's deployment of intrusion detection systems (IDS) to all critical nodes, continued development of advanced IDS, and the standing-up of the JTF-CND organization to manage this effort.

Intrusion Monitoring Systems (Enhanced Capabilities)

Several types of Intrusion Detection Systems are in use throughout the Defense infrastructures in the management of its networks and information systems. These are Government off-the-shelf (GOTS) and commercial off-the-shelf (COTS) products. GOTS products that are currently being used are network security monitors, network intrusion detection, and joint intrusion detection system(s).

- Network security monitor products observe network traffic, detect unauthorized network activity, and provide real-time alarms.

- Network intrusion detection monitor products are a suite of software tools that help detect, analyze, and identify intrusive behavior on networks.

- Joint intrusion detection systems combine the best features of the network security monitor products and network intrusion detection products.

Another area where work has begun is in the Automated Intrusion Detection Environment-Advanced Concept Technology Demonstration (AIDE-ACTD). This project is intended to demonstrate the ability of various intrusion devices to detect, visualize, and report intrusion activities. The objective is to develop the capability to determine whether information systems are under attack. The program will provide automated detection, correlation, warning, and reporting for integrated threat warning and attack assessment. Information systems sensor devices at various locations will be targeted using attack scenarios collected from the Services and Agencies. This addresses the challenges associated with techniques to recognize coordinated attacks and filter out "normal" hacker intrusion attempts. The next step will be to integrate this capability across service lines with a disparate set of sensors.

Joint Task Force-Computer Network Defense

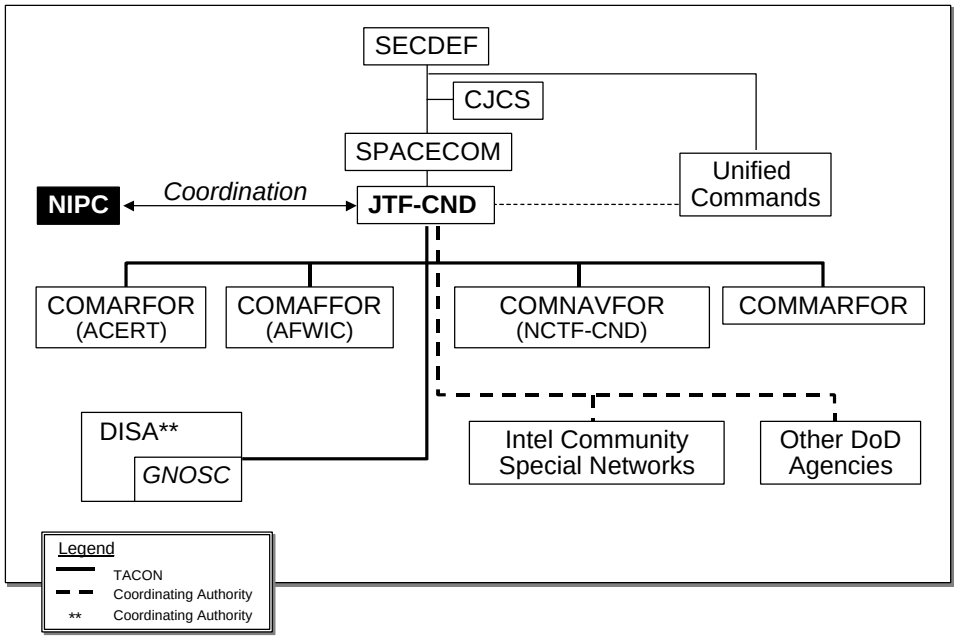
The Joint Task Force Computer Network Defense (JTF-CND) monitors incidents and potential threats, and coordinates across the Department to formulate and direct actions to stop or contain damage and restore network functionality.

The main functions of the JTF-CND are to synchronize technical, operational, and intelligence assessments of computer network attack; assess impact to military operations and capabilities and notify the National Command Authority (NCA) and user community; coordinate and direct

appropriate DoD actions to stop the attack, contain damage, restore functionality, and provide feedback to the user community; assess the effectiveness of defensive actions and maintain current assessment of operational impact on DoD; and coordinate, as required, with the National Communications Systems (NCS), the NIPC at the FBI, DoD Law Enforcement Agencies (LEA), DoD counterintelligence organizations, civilian law enforcement, other interagency partners, the private sector, and allies.

The U.S. Space Command assumed command authority for the JTF-CND on 1 October 1999. The following diagram depicts the JTF-CND command relationships:

Command Relationships



The JTF-CND is not a policy-making body, but it will make inputs as appropriate. The JTF-CND is not staffed to handle a major computer network attack crisis, but rather has minimum personnel to monitor daily operations and provide initial workload in a developing crisis.

Accomplishment: ***IOC for JTF-CND was established on December 30, 1998.***

Department of Defense National Roles

The Director, National Security Agency, as directed in Executive Order 12333 (EO12333), executes the responsibilities of the Secretary of Defense for the communications security of the U.S. Government. In National Security Directive 42 (NSD-42), the Director, NSA executes the responsibilities of the Secretary of Defense as the Executive Agent of the Government for National Security Telecommunications and Information Systems Security and as the National Manager for National Security Telecommunications and Information Systems Security.

The Director, Defense Information Systems Agency, is the National Communications System (NCS) Manager. The NCS was constituted and given its mission in a Presidential Memorandum signed by President Kennedy on August 21, 1963. In April 1984, the signing of Executive Order (E.O.) 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," changed the mission focus of the NCS from planning and coordinating a single unified Government communications system to its present mission of assisting the President and the Executive Office of the President (EOP) in exercising wartime and non-wartime emergency telecommunications, and in the coordination of the planning for and provisioning of NS/EP communications for the Federal Government under all circumstances.

Computer Emergency/Incident Response Capabilities

As Defense networks began experiencing an increasing number of security computer-related incidents several years ago that threatened its information systems and networks, it responded by initiating efforts to report and monitor the incidents. In addition, in order to maintain operational readiness, it assembled teams of experts who could respond to these incidents and repair any damage caused by them. Since then, a number of Computer Emergency Response Team (CERT) and Computer Incident Response Team (CIRT) centers have grown up throughout the Defense environment.

Within Defense, there is a relationship among the individual Services and Agency CERT/CIRTs and the Global Network Operations and Security Center (GNOSC), which acts as the enterprise-level CERT for DoD and interfaces with other government and private sector CERTs. There are processes and procedures among the Defense CERTs for the defining and reporting of incident data and the sharing of information and response capabilities. Within the JTF-CND structure, the GNOSC provides the CERT/Coordination Center (CC) services to maintain the health of the Internet and interconnected segments of the DII and NII.

Most of the CERTs within Defense are members of the Forum of Incident Response and Security Teams (FIRST)—an international coalition, composed of a number of government and private sector organizations around the globe.

Accomplishment: Multiple CERTs are established throughout the DoD and the Services.

National Infrastructure Protection Center (NIPC) Support

The DoD contingent to the NIPC is responsible for ensuring the integration of intelligence, counter-intelligence, and law enforcement in support of DoD critical infrastructure protection. As part of the NIPC, the DoD contingent will conduct national interdependency analysis; perform nationwide vulnerability assessment; develop national indications requirements; receive, consolidate, and assess national sector reporting; monitor national emergencies and incidents; and monitor significant national infrastructure reconstitution efforts and coordinate within Defense, as appropriate.

Accomplishment: Through DoD's efforts with the NIPC and law enforcement agencies, a procedure to share critical infrastructure protection information with the private sector has been developed.

OBJECTIVE 3: BUILDING STRONG FOUNDATIONS

With new technologies come new dangers. There is little argument that our information infrastructures are critical. DoD has already seen the first wave of cyber threats in both exercises and actual attacks. The Department has had a long-term R&D interest in this area; recent events have spurred greater focus on responding to the threat.

Information System Security Strategy (ISSS)

The Information Systems Security Strategy is the core of the DIAP and represents a multidimensional approach directed towards implementing new or enhanced IA operational capabilities, deploying advanced IA technologies and systems solutions, and enhancing the IA skills of DoD personnel.

Within a framework of information systems security and information assurance policy, standards and architectures, the DoD ISSS provides for integrated layers of a Defense in Depth of the DII. The areas in this initiative include securing the applications; protecting hosts and enclaves; and protecting the network. In addition, the *Security Technical Implementation Guide* and the *Security Handbook* are maintained and updated; network intrusion detection systems are fielded and deployed.

NSA, DISA, and the Services have other programs in these development areas. In addition, the proper deployment, use, and maintenance of information assurance solutions are essential to secure our networks and systems.

Defense-related Research and Development (Program 6)

The CIP DoD R&D agenda will leverage ongoing research in DoD and the Federal Government to develop and manage an infrastructure and information assurance and protection research and development portfolio that complements and leverages the national portfolio.

The Office of Director, Defense Research and Engineering (ODDR&E) will coordinate with the DoD CIAO, CIP Integration Staff, Sector CIAOs, and Service/Agency research and development activities to formulate a CIP DoD R&D agenda responsive to the Defense Sector and critical interdependency R&D needs. It will coordinate with R&D activities ongoing within the DIAP, CAAP, IAP, and other CIP-related programs.

As the DoD representative and deputy co-chair to the National CIP R&D Interagency Working Group, ODDR&E provides feedback and advice to the CIAO and Council regarding national issues and initiatives, reconciles the DoD agenda with the national R&D agenda, and provides DoD input to the national agenda.

DARPA Research Initiatives

Since 1995, the Defense Advanced Research Projects Agency/Information Technology Office (DARPA/ITO) has pursued a long-term strategy for investment in Information Systems Survivability technology. The first phase of this strategy was the Information Survivability Program (FY1995-99), which closed critical technology gaps in four areas: Indications & Warnings (I&W); Assurance & Integration (A&I); High Confidence Networking, and Computing.

The second phase of ITO's sustained investment in this area is called Inherent Survivability. The program builds on the successes of Information Survivability, adjusting the technical focus of the four major themes to address the next layer of challenges. The technical focus of Inherent Survivability has evolved from local intrusion detection to global intrusion assessment and from enhanced barriers to penetration to tolerance of attacks that manage to breach those barriers.

Information Assurance Program

The DARPA Information Assurance Program focuses on the growing dependence on information systems and the pressing need to get the right information to the right person at the right time. It becomes critical in such an environment to deliver and protect information and assure the availability of associated services. Information assurance technologies will be integrated into future versions of the DII Leading Edge Services (LES) to provide a robust architecture across a wide range of DoD information systems. The resulting security framework will reduce information vulnerability, allow increased interoperability and functionality, and provide the operational commander greater assurance that he will have the information he needs when he needs it.

The new Strategic Cyber Defense builds upon the above and pursues six key component areas including information assurance science and engineering principles; exploitation of cyber sensors and intrusion detection systems; cyber situation understanding; cyber system command and control tools; defensive mechanisms; and cyber defense strategies.

Solution Generation and Development

In order to address the challenges presented by the network environment and the use of commercial off-the-shelf (COTS) products, Defense research activities have embraced industry as a full partner in activities that include development of a network security framework; generation and development of network security products; and continuing maintenance and enhancement of traditional security product suites where commercially produced solutions are unavailable.

NSA Research Initiatives

The security of DoD systems and networks depends upon the ability to know and understand their vulnerabilities. NSA has extensive expertise in the area of vulnerability discovery that provides support to analyze vulnerabilities related to current and projected threats. The NSA can

also determine the adequacy of security measures; assess security deficiencies; provide data from which to predict the effectiveness of proposed security measures; confirm the adequacy of such measures after implementation; and provide a capability to uncover, investigate, and document security vulnerabilities in current and emerging network technologies.

The goal of NSA research programs is to ensure that IA solutions keep pace with leading edge information technology, and provide to the customer essential security services. The technology areas include active network defense, secure network management, and network security engineering—all supported by enabling research in cryptography and secure communications.

Active network defense provides a source of research and advanced technology development in Defensive Information Operations (DIO). Ongoing and future research efforts will develop new tools and techniques for analyzing types of attacks, their source and objectives, and technology to support manual and automatic responses. Future work in visual analysis of network attacks will develop prototypes that display multi-variable data in forms that can cope with massive data sets associated with very large-scale systems. New work has been initiated which will determine appropriate automated network responses under different intrusion scenarios. Research in mobile agents will investigate the applicability of that technology to the problem of network attack detection and response.

Secure network management is the technology area that supports the operation of a security management infrastructure (SMI) through the development of secure protocols for information sharing, network control, and monitoring of events within information systems. Future research will produce security-enhanced Internet protocol specifications, reference implementations, and support in worldwide standards bodies. Other ongoing research will develop proofs-of-concept for multicast security key management, fractional keying for multicast security, secure but non-cryptographic techniques for multicast, multicast routing security mechanisms, and group key management services.

Network security engineering addresses many of the issues critical to the development of secure hardware, software, and networked systems. Work in boundary definition is addressing the problem of identifying and protecting network borders in order to establish points for monitoring, controlling, and defending against cyberattack. Boundary protection is currently managed primarily by firewalls that filter communications based upon addressing data. New research will develop high assurance, high performance boundary protection devices that will add a capability to filter on the data itself or on specific protocols. The goal is higher efficiency and effectiveness, with much higher data rates than currently possible. An assessment of the security implications of advanced ATM network switching technology, such as IP Switching, in order to develop appropriate IA solutions is also an initiative. This research area is also addressing security issues associated with the use of object technology working through the Object Management Group (OMG).

All of the Services and Defense Agencies work closely with DARPA and NSA in order to apply the results of their research in real world operational environments. The operational environments range from command, control, communications and computers; to intelligence, surveillance, and reconnaissance; to weapons systems; to theater-level network management; to

tactical warfighter capabilities; to network and infrastructure survivability. The Services, NSA and DISA all have additional programs that support research, technology, infrastructure, and personnel development.

Education, Training, Awareness, and Professionalization (Program 7)

A vital element in improving the Department's Infrastructure and Information Assurance posture is trained and motivated personnel. Because of the shared-risk environment created by highly connected and interdependent DoD information systems, all individuals using, administering and maintaining these systems must understand the threats to the Department's systems and the policies, procedures, and equipment designed to mitigate such threats.

Training for all employees using DoD computer systems is already mandated by statute and Departmental regulation. Training and professional needs are addressed through an IA and IT skills base-line assessment. A coherent set of formal IA training and certification plans and programs are in place for certification compliance. The Military Services, NSA, and DISA all have training centers of excellence, which work together to provide extensive training in support of these, defined requirements.

Accomplishments:	***Classified systems users, system administrators, and maintainers must be certified by January 1999, unclassified, by December 2000.***
	The DoD Infosec program has created a series, 17 to date, of interactive CD-ROMs and videos for use throughout the Federal Government. The topics include DoD Infowar Basics, DoD and Federal INFOSEC Awareness, Information Age Technology (Overview of IT infrastructures), Information Assurance for Auditors and Evaluators, Networks at Risk, and Bringing Down the House (Hacker intrusion descriptions).

Exercises and Red Teams

Similar to several other key components of this Plan, the Y2K crisis "fast tracked" the initial implementation schedule of exercises envisioned in the PDD. Under the joint leadership of DoD and FEMA, an aggressive series of exercises addressed critical infrastructure and information warfare scenarios in the context of a Y2K environment.

These exercises tested among other things potential Y2K impacts on National Security; potential for policies in conflict; procedural currency and relevance; how to address allocation of scarce resources; and compatibility of individual Departmental/Agency plans.

The National Plan fully endorses this effort that ensured these exercise scenarios challenged senior leaders, both public and private, in managing and operating in the ambiguous environment of information warfare. Additionally, all elements of the Federal Government in conjunction with private industry Sector Coordinators participated in regular exercises that focused on system security, intrusion response, reconstitution methods, and overall management in a cyber crisis.

DoD Red Teams will continue to be used to test security measures. Through the Red Team implementation, the Department will develop consistency of purpose, commonality of structure, and meaningful and comparable results. In addition, the Red Team process will conduct periodic independent assessments of the IA processes, systems, and organizations to provide an impartial appraisal of some of the vulnerabilities.

Key national security systems or networks may be exempted from the requirement that an "outside expert" conduct vulnerability assessments. For security reasons, internal teams may conduct such tests.

Building the Public-Private Partnership (Program 8)

Information sharing with the private sector is indispensable in this Government and industry partnership to protect our Nation's critical infrastructures. The CIPIS is centrally located in the DoD organizational structure where the critical infrastructures and assets are assessed defense wide. The DoD installations, on the other hand, serve as "the Department's primary interface with host nation, Federal, state and local law information, emergency service personnel and *commercial infrastructure providers*." Private sector interface and information sharing serve as is needed at both levels.

The CIPIS staff will work with the ISACs through the lead non-DoD Agencies to build the partnership with these supporting infrastructures. Within the DI, the CIPIS, in partnership with the private sector representatives, will define the Government and the private sector information (classified, business confidential, etc.) exchange process, including the means to which it should be shared, documented, and updated routinely. The exchange of information at this level may be through a contractual agreement, an open forum via on-call/part-time industry representatives, or virtual interface with the private sector.

At the DoD Installation-level, Government and private sector DI representatives will work together to meet the needs and requirements the Lead Components/CIPIS identify in its planned assessments. Government/industry representatives will provide recommendations based on input from the state, county and local governments and private sector counterparts as to what the installations need in order to accomplish their missions. These representatives will also develop the procedures for exchanging information using one of several current government/industry and academia "partnership" models such as the National Security Telecommunications Advisory Committee.

Promote International Cooperation

In order to pursue international cooperation in CIP issues and information exchange in coordination with the national CIP program with other nations, international organizations, and industrial security officials of nations with multinational corporations within their borders, we need to improve infrastructure assurance and emergency planning at military and supporting sites outside the United States; support intelligence activities; improve cooperation for incident response; understand the impact of globalization on U.S. infrastructure; and ensure that Defense

Security Service (DSS) implementation mechanisms are appropriately included in existing and future international agreements whenever CIP and/or Information Assurance are addressed.

The CIPIS will incorporate international agreements into the DoD CIP process and coordinate new requirements. DSS will participate in the CIPIS to provide advice and support for implementing international industrial security-related arrangements.

5. FRAMEWORK FOR CRITICAL INFRASTRUCTURE ASSURANCE BY PRIVATE SECTOR AND STATE AND LOCAL GOVERNMENT

The Need for Public-Private Partnership

The Federal Government alone cannot protect U.S. critical infrastructures. Private industry and state and local governments directly own, effectively control, or greatly influence the large majority of the infrastructures that are vital to our national security and economic well-being. Therefore, the Federal Government can only help defend these critical infrastructures through effective cooperation with industry, and state and local governments. Attempts by the Federal Government to do the job alone will fail.

This is not to say that the Federal Government has no role or only a limited role in protecting private sector infrastructures, but the Federal Government must act through cooperative means. The Federal Government must develop a relevant case for action to urge the private sector into motion, share information with the private sector about threats and potential remedies, support the private sector to design its own defensive programs, provide incentives for the private sector to implement those programs, remove obstacles to private sector action, spur important research and development, and, at times, provide overall national leadership. The relationship between the Federal Government and private sector infrastructure providers should be a full and complete partnership.

Principles of Partnering

- Voluntary
- Mutual concerns, with achieving clear, focused, well-defined goal(s)
- Key complementary capabilities and roles exist between the participants
- Mutual understanding of each participant's values, expectations, needs, concerns, and individual objectives
- Persistent/frequent interaction
- Mutual trust on action
- Starts with planning

The relationship among industry, state and local governments and the Federal Government should be one of positive, voluntary cooperation, shaped by all participants. Officials at all levels of government and private sector representatives should interact frequently, perhaps continuously, in order to ensure mutual understanding of concerns, needs, and expectations. The Government should not seek to direct private sector compliance, either through law or regulation. Most importantly, it means that the Government should not take any action that would undermine civil liberties.

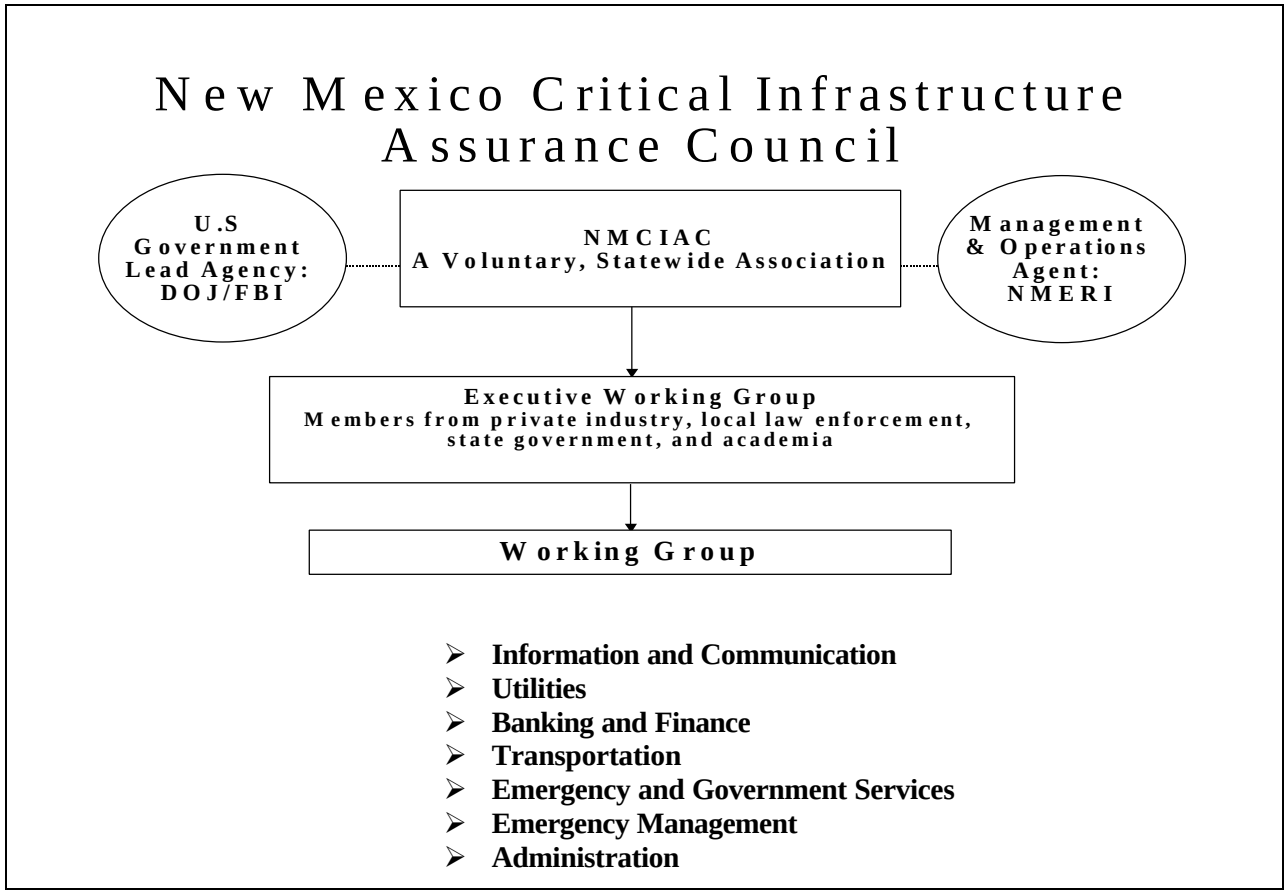
American efforts to protect our critical infrastructures will be a product of this public-private partnership. Therefore, this chapter of the National Plan is not a plan at all, but a framework for

building the partnership, an outline of how the Federal Government can contribute and encourage development of public-private cooperation. As such, the chapter considers the private sector and state and local government together, recognizing that there are clear differences between these two sectors. If we are successful, future editions of this section of the National Plan will move beyond the framework described here, and describe a full spectrum of specific actions and programs that have been jointly agreed upon by industry and all levels of government.

The Role of State and Local Governments

State and local governments are at the forefront of the Nation's defense of our critical infrastructures against deliberate attack. They both directly own and operate certain infrastructures, and have the physical proximity and closest governmental interaction with privately owned and operated infrastructures. As such, state and local governments may appropriately be considered to constitute a separate sector in the CIP effort.

State and local governments and private industry cooperated to prepare for Y2K, and several are already organizing to deal with longer-term critical infrastructure protection issues. A close relationship already exists between state, local and Federal counterparts in law enforcement and other relevant areas. The Federal Government is working to increase this cooperation and expand the necessary relationships between the Federal Government and state and local governments, and foster such relationships between these entities and the private sector.



Within at least one state, New Mexico, industries, academia, and government agencies have voluntarily mobilized to form the New Mexico Critical Infrastructure Assurance Council (NMCIAC) to protect that state's critical infrastructures from physical and cyber threats.

The interaction between state and local governments and the private sector to protect our Nation's critical infrastructures is discussed throughout this chapter. Future versions of the National Plan may also contain separate chapters for the efforts by private sector and state and local governments, in cooperation with the Federal Government, to protect our Nation's critical infrastructures.

The Role of Private Industry

For private industry, computer security can have a direct effect on business success, and even survivability. Private firms know they have an obligation to their customers, both public and private, to maintain robust and reliable service delivery systems. In order to maintain customer confidence and to survive in an increasingly competitive marketplace, successful companies have implemented programs to assure service when their systems and operations are disrupted. The increasing dependence on information technology, and the new threats and vulnerabilities that can come with its use, represent a new dimension of concern for these assurance efforts.

There is a long history of American business leaders stepping forward to organize their industries to contribute to solving national challenges. In doing so, they acted in the national interest. However, they acted not as altruists, but because they also helped ensure the reliability of the services they provide their customers. Actions that served the interest of the Nation, also served the interests of the shareholders.

Examples include the establishment of the North American Electric Reliability Council (NERC) and the National Security Telecommunications Advisory Council (NSTAC). The NERC focusing on the national electric grid, and the NSTAC, focusing on national security issues regarding U.S. telecommunications networks, represent models of industry commitment to their customers and to the public good. Both have the common theme of assuring reliability, availability, and integrity of their respective systems.

National Security Telecommunications Advisory Committee (NSTAC)

- The NSTAC is a Presidential Advisory Committee that was established in September of 1982 to provide advice and expertise to the President.
- The NSTAC consists of up to 30 senior corporate leaders representing major telecommunications related industries.
- The NSTAC formed subgroups to analyze national security and emergency preparedness issues pertaining to communications.
- The NSTAC works closely with the National Communications System (NCS) to serve as a focal point for joint industry/government planning.

North American Electric Reliability Council (NERC)

- Not-for-profit ownership by 10 regional reliability councils.
- All segments of the electric industry, including privately owned companies, state, local, and Federal Agencies.
- Accounts for virtually all the electricity supplied in the United States, Canada, and a portion of Mexico.
- Promotes the reliability of electricity supply for North America by reviewing for lessons learned, monitoring compliance with policies, standards, principles and guides, and assessing the future reliability of the Nation's bulk electric systems.

Y2K and the Role of Industry and State and Local Governments

Sometimes the private sector serves as a catalyst for public-private cooperation to defend against a common threat. Early in the Y2K effort, many in industry and the public believed that inadequate concern was being paid to a very real issue. They urged the Federal Government to elevate national awareness and action. Building on the work already underway, the Federal Government quickly established a process for improved cooperation. Although we will only know the true effectiveness of this effort after a thorough examination of what went well and what did not is completed, there is a general belief that improved public-private cooperation made the problem manageable.

Y2K was the first test of the Nation's infrastructure assurance programs in the Information Age. Possible systems failures due to Y2K highlighted the need to include a cyber-reconstitution component in owners' and operators' infrastructure assurance programs. The Federal Government's role is to assure that various programs across industry and local and state governments can be implemented in a coordinated and effective manner nationwide.

Lessons learned from the Y2K conversion effort are relevant to a public-private partnership for information security. Incorporating the information dimension into service and product delivery assurance programs requires that each industry and company:

- assess dependency of critical business operations on information technology;

- review impact and consequences to business operations and customer relationships when information flow is disrupted or corrupted from intentional or accidental acts;

- evaluate change in corporate risk profile and take remedial action as required by prudent management and due diligence to assure delivery of services or products per customer and public expectations; and

- continue to appraise future information technology investments to include security risks to critical business operations.

Business leaders recognize the health of their industries affects the health of their individual companies. Consequently, these actions, naturally encouraged and expected as prudent management business practices, are the same measures needed to protect against the new threats to national security and to assure the economic security of their industries.

Federal Organization for a Public-Private Partnership

The White House and key Federal Agencies are organizing themselves to directly work on shaping the National Plan with key private sector and state and local government leaders and organizations. Under PDD-63 and subsequent decisions, Lead Federal Agencies were designated to work with selected infrastructure sectors to encourage their organization. In the past year, a number of sectors, with the support of their respective Lead Agencies, have begun organizing themselves by designating Sector Coordinators:

Critical Infrastructure Sector	Private Sector Coordinator	Federal Lead Agency And Sector Liaison
Information and Communications	Information Technology Association of America; Telecommunications Industry Association; United States Telephone Association	Department of Commerce Greg Rohde, Assistant Secretary for Communications and Information
Banking and Finance	Banking and Finance Coordinating Committee	Department of Treasury Greg Baer, Deputy Assistant Secretary
Water Supply	Association of Metropolitan Water Agencies	Environmental Protection Agency J. Charles Fox, Assistant Administrator, Office of Water
Aviation, highways (including trucking and intelligent transportation systems), mass transit, pipelines, rail, and waterborne commerce	TBD	Department of Transportation Rear Admiral Bert Kinghorn, Director, Intelligence and Security Office
Emergency law enforcement services	Committee of State and Local Law Enforcement	Justice/FBI Michael Vatis, Director, NIPC
Emergency fire service; continuity of government services	National Association of State Fire Marshals	FEMA Denis Onieal, Superintendent, National Fire Academy; Catherine Light, Director, Office of National Security Affairs
Public health services	TBD	Department of Health & Human Services John Callahan, Assistant Secretary
Federal Sector	N/A	General Service Agency Thomas Burke, Assistant Commissioner, Information Security Office
Electric power; oil and gas production and storage	North American Electric Reliability Council; National Petroleum Council	Department of Energy General (Ret.) Eugene E. Habiger, Director, Office of Security and Emergency Operations

Working together, the Federal Government and private industry have opened the dialogue on critical infrastructure protection within each sector.

- A November 1998, Energy Forum sponsored by the Department of Energy, the Gas Research Institute, and the Electric Power Research Institute (EPRI) for the energy industry, was attended by more than 100 electric, gas and oil industry, and Government representatives. A second Energy Sector Forum was held April 1999 in Houston, Texas, and a third by the EPRI for 150 attendees in November 1999.

- The banking and finance industry through its Sector Coordinating Committee has met several times and established action plans to address risk assessment, industry information sharing, a research and development agenda, and outreach to industry senior leadership.

Banking Industry Technology Secretariat
Financial Services Security Laboratory and Testing Process to Promote Safety and Soundness in Electronic Banking and Commerce

The Banking Industry Technology Secretariat (BITS) is the technology group for the Financial Services Roundtable. BITS fosters the growth and development of electronic banking and e-commerce in an open environment that will encourage greater choice and efficiency in financial software, access devices, networks, and processing capabilities for the benefit of financial institutions and their customers. BITS promotes safety and soundness in payments systems and in electronic banking products. BITS is governed by a Board of Directors comprised of 14 Chairmen and CEOs of the largest U.S. bank holding companies, as well as representatives of the American Bankers Association (ABA) and the Independent Community Bankers of America (ICBA).

Recently, BITS announced the creation of its new Financial Services Security Laboratory. With funding from participating vendors, this laboratory will be operated by a private consulting firm that specializes in information protection, electronic commerce security, and information systems engineering. The major objectives of the facility are:

- early product influence;

- risk reduction;

- cost reduction; and

- security functionality.

The Security Lab will ultimately test products for their ability to meet specific criteria pertaining to security attributes such as authentication, integrity, confidentiality, privacy, auditability and authorization. A BITS-tested mark will be given upon successful completion of the testing cycle, indicating the overall security level for the product. Mark issuance will be posted on the BITS Web site.

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 FS/ISAC 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.

The Federal Government has a plan to develop the necessary relationships with state and local governments. Working through organizations such as the National Governors Association and the United States Conference of Mayors, as well as with individual state and local governments that have begun their own critical infrastructure protection programs, the Federal Government is encouraging these efforts towards building the crucial partnership between government and private industry to protect the Nation’s infrastructures against deliberate attack. For example, state and local law enforcement has designated their Sector Coordinator and completed the initial draft of their plan for action.

Other actions are also underway. The National Coordinator and other senior Federal officials are building an active dialogue to address cross-sectoral concerns. For-profit companies have recognized the market and have begun to work with private industry clients to organize for information systems protection.

Actions to Protect and Defend Private Sector and State and Local Government Critical Infrastructures

With a growing awareness of the need for protection of our critical infrastructures, among the first questions most business people ask when they learn of this issue is: How does this impact my business?

The Federal Government cannot answer that question alone. Through public-private partnership, and working with state and local governments, we may be able to develop more detailed answers. However, even at this early stage, we can suggest that the private sector and state and local governments consider participating in several of the programmatic initiatives set forth in the plan, including identifying and fixing vulnerabilities, (Program 1), organizing to share information about vulnerabilities, threats and attacks (Program 4), investing in R&D (Program 6), and reaching out to raise industry awareness about the need for improved cyber-security (Program 8).

Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities *(Program 1)*

The Federal Government will encourage the periodic review and evolution of industry's infrastructure assurance plans, with greater attention to the role and dependency on information systems, industry structures, and best business practices.

Many industries already conduct risk assessments, take remedial action, and put in place internal response mechanisms as part of their operational responsibilities to their customers and to the public. The Federal Government collects, studies, and analyzes vast amounts of information related to cyber-security technology, practices, and trends. These are areas of opportunity for consideration by private industry. An example of the latter is a highly regarded *Information Security Management, Learning from Leading Organizations* report by the General Accounting Office. Information that can be easily exchanged should be readily exchanged. Appropriate two-way communication and support relationships should also be established with state and local governments.

The Federal Government will also provide support for sector risk analysis. Expert resources have been developed by various Agencies. The Federal Government will identify and offer the use of resources, as appropriate, to private industry and state and local government entities to conduct their risk assessments. For example, GSA and the CIAO have prepared a *Framework for Vulnerability Analysis,* which is being widely used in preparation of departmental critical infrastructure protection plans. This, or similar frameworks, are available to private industry and state and local governments for use in advancing their work. In addition, the FBI is compiling a list of critical infrastructure providers within each sector, and district offices are developing working relationships with these providers.

In addition to conducting and acting as risk assessments, private industry in particular can take the lead in two critical activities:

- *Share and Promote Recommended Practices:* The definition of standard, effective information systems security needs to be developed, evolved, and shared in the marketplace. Historically, industry plays the defining role in developing and identifying recommended practices and standards. The Federal Government has sometimes served to accredit outside institutions to develop standards and accreditation processes. However, when the market cannot itself evolve fast enough to serve the needs of the users, the Federal Government can act as a catalyst.

  The Federal Government will work with existing standards bodies and industry to create or identify an organization that can serve as a government-industry coalition for developing and encouraging the use of recommended practices and standards. This organization may consider accrediting information systems security service providers and laboratories doing evaluations, focusing a research agenda, and sponsoring a continuing national program of awareness and education on recommended practices for information assurance and security. It may coordinate its work with "change agents" such as accounting and insurance bodies. These activities in no way place requirements on the private sector. As the Government's

contribution, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) will evaluate extending the activities conducted under the National Information Assurance Partnership (NIAP) and System Security Engineering-Capability Maturity Model (SSE-CMM).

As part of these activities, NIST and NSA will survey currently operating organizations to determine if an existing organization can serve as a model. NIST, NSA, and the Office of Management and Budget (OMB) will survey relevant existing standards, recommended practices, and accreditation programs as a baseline for work. Furthermore, NIST and NSA will develop accreditation procedures for outside groups to certify that processes, human resources, and hardware/software comply with recommended practices and standards. NIST and NSA will undertake research to develop a benchmarking process and to establish general stand-alone information security metrics so that critical information system users will know how to measure effectiveness and compare themselves to others. OMB will work with Financial Accounting Standards Board, the Securities Exchange Commission, and other groups to encourage their participation. And the Defense and Commerce Departments will work through the Federal Lead Agencies to encourage each infrastructure sector to adapt or adopt the recommended practices and standards, and if necessary, work to create sector-specific standards bodies.

- *Engage Risk Management Professions to Make Information Systems Security Part of Good Business Practices:* Introduction of information technology into core business processes also presents a new dimension of risk when controls managing and securing systems are inadequate. The growing dependency of business operations on information systems inevitably means that information systems security needs to be part of prudent management controls and practices. Some in the auditing and risk management professions fully understand and acknowledge these new considerations in assessing risks for their companies, agencies, and clients. With the concerns raised in conjunction with the Y2K conversion, many more are just becoming aware. Within many companies and state and local agencies, these professionals serve in positions that report risk issues directly to senior management. Working with these professionals to communicate urgency and the national agenda will enhance overall awareness in the general business and local and state communities. This awareness—along with sharing of information on threats, tools and techniques, resources, practices, and standards applied across industries—will enhance their ability to identify and communicate the true nature of their risk to the business and operations managers within their organizations.

Organize to Share Information About Vulnerabilities, Threats, and Attacks (Program 4)

PDD-63 suggests that the private sector, in cooperation with the Federal Government, establish Information Sharing and Analysis Centers (ISACs) to facilitate public-private information sharing on vulnerabilities, threats, intrusions, and anomalies. These Centers could serve as the mechanism for gathering, analyzing, appropriately sanitizing, and disseminating private sector information to both industry and possibly the National Infrastructure Protection Center. They could also gather, analyze, disseminate, and distribute information from the NIPC to the private sector. In time, the ISACs could develop into analytic centers of excellence, establishing baseline

statistics and patterns on the various infrastructures; becoming a clearinghouse for information within the various sectors; and providing a library for historical data to be used by the private sector and, as deemed appropriate by the ISACs, by the Government.

Private industry will ultimately decide whether to participate in ISACs and what form those entities will take. The National Coordinator and the Federal Lead Agencies, who serve as Sector Liaisons, will coordinate available Federal Government assistance in response to the needs of the private sector through such initiatives as discussion forums, possible seed money, and physical facilities. The Federal Government will also help develop criteria for information sharing between the NIPC and private sector ISACs, through deliberations with the Sector Liaisons and Sector Coordinators. In the interim, Government will encourage better communication within and between the sectors utilizing existing organizations, such as the InfraGard chapters and the CERTs.

A great deal of work has been completed to encourage the creation of private sector ISACs. In January 1999, the Critical Infrastructure Assurance Office sponsored a conference for more than 70 private sector, state, local, and Government officials to discuss necessary next steps to advance information sharing.

The Federal Government is in the process of developing Government-wide intrusion detection capability for both its national defense and civilian core information systems in order to provide timely warning of threats, attacks, and major vulnerabilities. It is also focusing greater collection and analytical efforts on infrastructure security issues through the Computer Emergency Response Teams (CERT) and departmental plans. These systems will provide the Government with a better understanding of threats and vulnerabilities present in its information systems. They will also result in products that should be shared with private industries and state and local governments.

Computer Emergency Response Team/Coordination Center

If a new virus attacks your computer network, whom should you call? Carnegie Mellon Software Engineering Institute's Computer Emergency Response Team Coordination Center (CERT/CC) provides accurate, up-to-the-minute information to help solve computer security incidents.

From January through December 1998, the CERT/CC received 41,871 email messages and 1,001 hotline calls reporting computer security incidents or requesting information. During this period, it received 262 vulnerability reports and handled 3,734 computer security incidents, which affected more than 18,990 sites.

When a security breach occurs, the CERT/CC incident response staff helps affected sites identify and correct problems in their systems and develop system safeguards and security policies. It coordinates with other sites influenced by the same incident and, when an affected site explicitly requests, it facilitates communication with law enforcement and investigative agencies.

The CERT/CC works closely with technology producers and vendors to analyze reports it receives for potential system vulnerabilities. It advises manufacturers of security deficiencies in their products, helps to resolve the problems, and facilitates the distribution of corrections to other response teams and to the Internet community at large.

These products will include information developed by the intelligence community. Identifying new threats, or recognizing changes in threats, will help focus current investments in the right place, making better use of finite resources for both Government and industry. The National Coordinator, together with the NIPC, the intelligence community, and Federal law enforcement agencies, is establishing a process to provide regular briefings on threats and vulnerabilities to key private sector and state and local decision-makers. This will help non-Federal entities make more informed judgments as they evaluate risks and necessary remedial actions.

Centers for Disease Control and Prevention (CDC) as Model for ISAC

- Needs-based, evolutionary structure
- Technical focus and expertise
  - non-regulatory, non-law enforcement mission
  - establish baseline statistics and patterns on the various infrastructures
  - clearinghouse for information
- Public-private; local, state and Federal participation
- Decentralized governance
- Multi-functional
  - shares real time incident data as well as summary and "vulnerability information"
  - multiple avenues for sharing that protect information and confidentiality of disclosures

Invest in Research and Development (Program 6)

An obstacle to the wider use of information security systems is their perceived high cost of purchase, operations, and maintenance. Increased Government investment in applied research and development in this technology will stimulate the market to provide better and more affordable tools, particularly where the market cannot do so itself. Enhanced affordability of more effective tools will broaden their dissemination and use.

Moreover, following completion of the national infrastructure risk assessments, the National Coordinator and the Federal Lead Agencies will develop, as needed, recommendations for the President and Congress concerning the use of incentives such as tax incentives, direct subsidies, and insurance requirements to further spur private sector research and development.

Outreach to Make Americans Aware of the Need for Improved Cyber-Security (Program 8)

The Partnership for Critical Infrastructure Security focuses on communicating the urgent need to protect our Nation's critical infrastructures, and highlights how industry and Government can work together to secure these infrastructures from cyber disruptions.

The Partnership will explore ways in which industry and government can work together to mitigate the risks to the Nation's critical infrastructures. To this end, the Partnership will sponsor a series of conferences, meetings, and working groups with industry and government executives for the purpose of:

- promoting awareness and understanding among owners and operators of critical infrastructures, the risk management community, the general business community, state and local governments, and, ultimately, the American public;

- facilitating future industry contributions to the National Plan; and

- identifying and addressing issues of mutual concern, including but not limited to information sharing arrangements, legal and regulatory reform, standards and best practices, education and training, and research and development initiatives.

The Partnership will proceed based on open and voluntary membership; mutual trust; regular interaction; full understanding of each participant's values, expectations, needs, concerns, and individual objectives; and achieving clear, focused, and well-defined goals.

- *Focused Critical Infrastructure Sector Outreach and Awareness Programs*: The Federal Government, through designated Lead Agencies, is meeting and briefing members of critical infrastructure sectors on the importance and urgency of information security. Awareness and understanding are prerequisites to willingness to engage in active planning and action to implement protection. Lead Agency Sector Liaisons will help identify and work closely with the private sector coordinators. Jointly, liaisons and coordinators will sponsor a series of White House conferences and other workshops with the sectors.

- *NIAC:* The National Coordinator, in consultation with appropriate Government entities, will work to establish a National Infrastructure Assurance Council (NIAC) as an advisory council to the President. The Council will demonstrate the Government's commitment to partner with industry, and will consist of up to 30 industry and state and local government officials nominated by Lead Agencies and Sector Coordinators. This forum will allow critical stakeholders the opportunity to provide infrastructure assurance policy advice to the President.

Ensure Strong Legal Foundations for Joint Action (Program 9)

To support the partnership, the Administration is working closely with businesses, state and local governments, and all Americans to review existing laws and regulations and propose a legislative agenda. Based on discussions to date with private industry and state and local governments, elements of such an agenda may include:

- *Mitigating legal impediments to effective information sharing*: Enhance predictability of legal consequences for corporations to share information with each other and with the Government. The Government will address confidentiality, antitrust, and liability concerns in a legislative agenda in order to build trust across the public and private sectors.

  The Department of Justice will define circumstances under which industry may share information by developing two mechanisms: business review letters and Department of Justice Guidelines. Both will outline how to share, what to share, and other particulars.

  The Administration, working with state governments, will identify areas where state laws complicate the missions outlined in this Plan. Discussions with important representatives, such as the National Association of Attorneys General, may lead to model rules covering information sharing liability issues that can then be considered by each state. Coordinating liability solutions requires input from all members of the critical infrastructure partnership. States have their own laws governing liability; and court decisions interpreting and applying them add an additional layer of complexity. Legal reform measures must merge private sector input with state and Federal Government concerns.

- *Effective sentencing for criminals by engaging the judiciary*: Provide a deterrent and reflect more commensurately the harm caused by attacks to infrastructures.

  The Administration is working with the U.S. Sentencing Commission to ensure that the *U.S. Sentencing Commission Guidelines* account for the seriousness of harm caused from an attack on infrastructures. For example, the *Sentencing Guidelines* may address the severity of consequential damages, such as losses resulting from the "downstream" effects of a denial-of-service attack. The Administration will also encourage the Sentencing Commission to communicate critical infrastructure assurance issues to each of the states, through the state sentencing commissions or directly, as part of Federal judiciary training exercises.

- *Computer crime—International civil remedies*: Cyberattacks know no border. The Administration recognizes that existing international mechanisms to seek civil redress from attacks on infrastructures are limited. Many countries do not criminalize computer intrusions. We seek to increase the availability of civil remedies for computer-related violations through appropriate multilateral and bilateral agreements and mechanisms.

  Legal reform will draw on existing studies, such as the Federal Trade Commission's inquiry into similar issues affecting e-commerce. The review will additionally consider existing institutions, such as the World Trade Organization, for possible models.

- *Employer-employee relationships*: Define more clearly the framework within which industry can defend itself from insider attacks.

  Insider threats provide the most frequent avenue of attack to the Nation's critical infrastructures. The PCCIP outreach included extensive discussions with private sector owners and operators, state and local governments, Federal lawmakers, and privacy advocates. Further legal reform must incorporate a wide range of opinions and findings in crafting solutions that are responsive to this complex problem—especially where employees are hired to fill highly sensitive positions. We must recognize that an insider may really be an outsider. In addition, the Administration will encourage experts to undertake a review of state and Federal laws governing the employer-employee relationship and other privacy laws. This review will focus on how laws afford the maximum degree of privacy protection while not unduly impeding certain employers' needs for enhanced security.

- *Emergencies: Clarification of reporting requirements, government approvals*: Reduce confusion over jurisdictions. The Administration will review Federal Government reporting requirements that lead to confusion within the private sector; it will clarify Agency jurisdictions for industry—especially during emergencies or crises. It will assure that any new reporting requirements are not duplicative.

Looking Ahead: The Private Sector, State and Local Governments, and the Next National Plan

Building upon this framework, Federal Government officials and industry, and state and local government representatives can work together to produce the next edition of the *National Plan*. As this version includes specific directions for Government actions, it is hoped that the next edition will include a list of specific actions that private industry has chosen to take. This list will be the product of cooperative, voluntary deliberations building toward a true public-private partnership.

ANNEX A

KEY FEDERAL CIP OFFICIALS AND POINTS OF CONTACT

Name	Title	Agency	Contact Information
Richard A. Clarke	National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism	National Security Council	202-456-9351
Jeffrey A. Hunker	Senior Director for Critical Infrastructure	National Security Council	202-456-9361
Michael Vatis	Director	National Infrastructure Protection Center	202-324-0307
Art Money	Assistant Secretary of Defense for Command, Control Communication, Intelligence	Department of Defense	703-695-0348
John S. Tritak	Director	Critical Infrastructure Assurance Office	202-589-3200
Liz Verville	Deputy Director	Critical Infrastructure Assurance Office	202-589-3200
Greg Rohde	Sector Liaison, Information & Communications	Commerce Department	202-482-1840
Greg Baer	Sector Liaison, Banking and Finance	Department of the Treasury	202-622-2610
J. Charles Fox	Sector Liaison, Water Supply	Environmental Protection Agency	202-260-5700
Rear Admiral Bert Kinghorn	Sector Liaison, Aviation, Highways, Mass Transit, Pipelines, Rail, and Waterborne Commerce	Department of Transportation	202-366-6525
Denis Onieal	Sector Liaison, Emergency Fire Service	Federal Emergency Management Agency	301-447-1117
Catherine Light	Sector Liaison, Continuity of Government Services	Federal Emergency Management Agency	202-646-2979
John Callahan	Sector Liaison, Public Health Services	Department of Health and Human Services	202-690-6396
Thomas Burke	Sector Liaison, Federal Sector	General Service Agency	202-708-7000
General (Ret.) Eugene Habiger	Sector Liaison, Electric Power, Oil and Gas Production and Storage	Department of Energy	202-586-5000

ANNEX B

BUDGETARY TRENDS

Overview

The FY2000 Budget provided $1.737 million for Government-wide efforts to protect critical infrastructure. This represents an increase of more than $300 million, or 20 percent, over the FY1999 enacted base. Figure 1 depicts this increase. The budget includes funding for new programs to address key vulnerabilities, as well as for ongoing efforts to assure the security of interconnected infrastructures such as telecommunications, banking and finance, energy, transportation, and essential government services.[1]

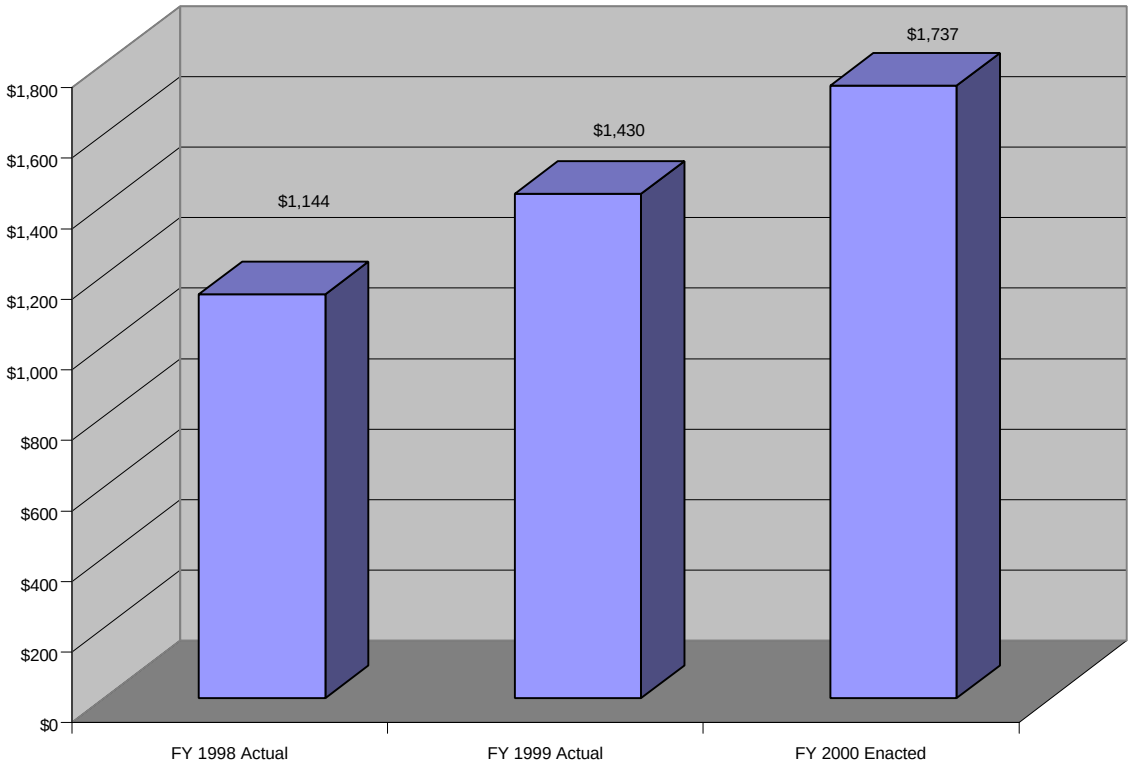


Figure 1. Total Funding for Critical Infrastructure Protection (in millions of then-year dollars)

Critical Infrastructure Spending by Agency

Within almost all major Executive Branch Departments, CIP expenditures increased between 1998 and 1999. The FY2000 budget continues that trend. This is shown in Table 1.

See page 5, *Interagency Process to Identify and Fund Critical Infrastructure*, regarding the integrity of the data in this annex.

*Table 1. Funding for Critical Infrastructure Protection (in millions of dollars)**

Agency	FY1998 Actual	FY1999 Actual	FY2000 Enacted
National Security	975	1,185	1,403
Treasury	23	49	76
NASA	41	43	66
Transportation	20	25	51
Justice	26	54	46
NSF	19	21	27
Commerce	9	22	18
HHS	22	12	13
Other	9	18	37
Total	**1,144**	**1,429**	**1,737**

The relative distribution of Critical Infrastructure Protection funds across the Government is illustrated in Figure 2.

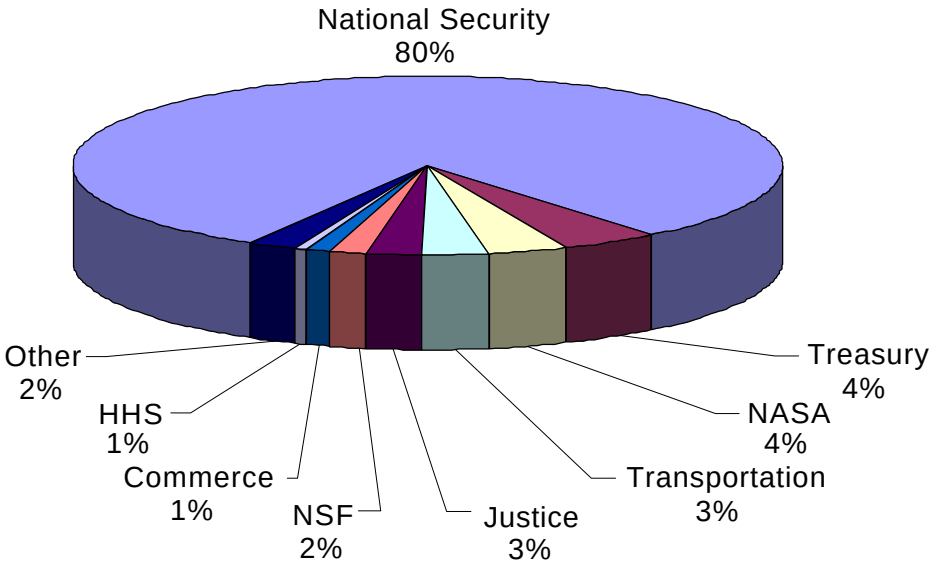


Figure 2. Funding for Critical Infrastructure Protection by Departments and Agencies

Critical Infrastructure Spending by Program Operation and Research & Development

Program operations describe different measures used on a routine basis to protect critical infrastructure. Figure 3 shows relative spending for program operations (for national security and other Federal programs) and research and development.

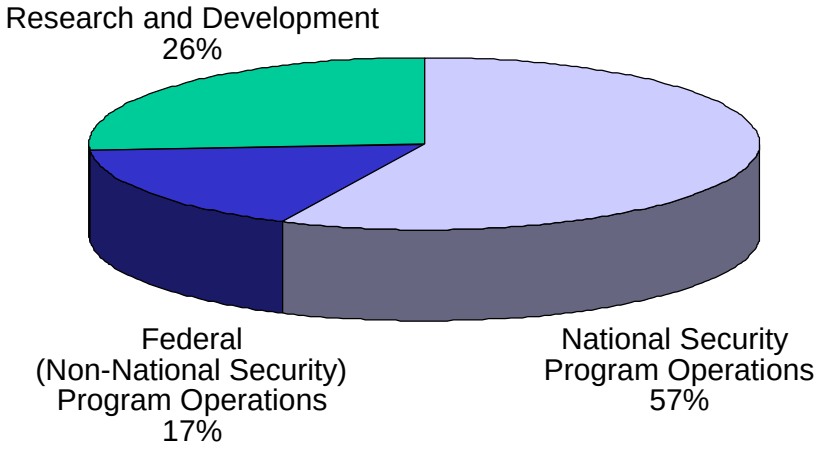


Figure 3. Critical Infrastructure Protection Spending by Function

As depicted in Figure 3, CIP spending is divided into program operations (for national security and Federal) and R&D. Program operations can be broken down into the following areas:

- vulnerability assessment;
- risk management;
- protection and mitigation;
- intrusion detection;
- incident response and reconstitution; and
- education and awareness.

Not all Agencies have sufficient granularity in their data to permit us to characterize budget data by these various program operations. Beginning this year, however, we will collect and be able to examine the data in detail.

Critical Infrastructure Spending by Sector

Table 2 lists funding for critical infrastructure protection by sector, funding for initiatives to better understand the interdependencies between sectors, and for efforts to establish Information Sharing and Analysis Centers (ISAC).

Table 2. Funding for Critical Infrastructure Protection by Sector (in millions of dollars)

Critical Infrastructure by Sector	FY1998 Actual	FY1999 Actual	FY2000 Enacted
Government and Emergency Services	1042	1282	1565
Information and Communications	41	57	58
Transportation	25	32	57
Electric Power, Oil and Gas Production and Storage, and Water Supply	22	35	30
Banking and Finance	12	17	15
Interdependencies	2	7	5
ISACs	0	0	8
Total	**1,144**	**1,429**	**1,737**

A description of how the funding will be executed for the critical infrastructure sectors, the interdependency initiative, and ISACs is provided below.

- *Government and Emergency Services*. Funds for this sector increased by more than 20 percent over the previous Budget, the majority of which support national defense Agencies' efforts to protect critical infrastructures.

- *Information and Communications*. $33 million is provided to seven Agencies for computer security research and development proposals.

- *Transportation*. To address Federal Aviation Administration facilities and information systems, and for programs to reduce vulnerabilities in the National Airspace System and surface transportation systems, the Budget significantly increases funding for this sector from $32 million to $57 million.

- *Electric Power, Oil and Gas Production and Storage, and Water Supply*. The $30 million budgeted for this area supports ongoing programs in the Department of Energy, Department of Interior, and Environmental Protection Agency to advise energy companies and metropolitan water agencies in CIP planning, and for basic research. These efforts advance the goal of public-private partnerships to meet common CIP needs.

- *Banking and Finance*. The Treasury Department received $16 million to coordinate protection of critical facilities, equipment, and operations in the banking and finance sector. As directed by the PDD, Treasury actively leads sector CIP efforts as well as serving as a model for other sectors.

- *Interdependencies*. The Budget provides $5 million to DoD, Commerce, and the National Science Foundation to study relationships among infrastructures, and to build our capability to ensure a reliable, interconnected, and secure information system infrastructure.

- *Information Sharing and Analysis Centers*. $8 million for sector liaison Lead Agencies is provided in the Budget to help establish Information Sharing and Analysis Centers (ISAC). ISACs are designed to foster private sector development and to share recommended practices and standards.

New and Ongoing Critical Infrastructure Initiatives

This section discusses specific initiatives that advance the goals of the Presidential Decision Directive to protect critical infrastructure. The initiatives listed below may support several critical infrastructure sectors. These initiatives represent only a portion of the total of the $1,737 million CIP program.

- *Computer Security Research and Development Initiative*. $80 million is allocated for R&D to study safeguarding networks and databases, and detection of anomalous activities, "trap doors," Trojan Horses, and other malicious code.

- *Information Sharing and Analysis Centers*. As noted earlier, ISACs are designed to foster private sector development and share recommended practices and standards. $8 million is set aside in the Budget to help establish ISACs.

In addition to the above-noted new programs, the President continues to support the following ongoing efforts:

- *National Defense Infrastructure*. The Budget increases resources to protect critical infrastructures that support national security requirements, bringing this funding to over $1.4 billion.

- *Federal Aviation Administration and National Airspace System*. FAA funding for CIP doubled, from $23 million to almost $50 million, to better protect FAA facilities and information systems, and for programs to reduce vulnerabilities in the National Airspace System.

- *Fighting Cybercrime*. The Budget provides $46 million to enhance the investigative and prosecutorial efforts of the FBI, the U.S. Attorney, and the Justice Department's Criminal Division.

- *Critical Infrastructure Assurance Office (CIAO)*. The CIAO received $3 million to support efforts to develop a national infrastructure assurance plan and coordinate a national education and awareness program.

Interagency Process to Identify and Fund Critical Infrastructure Initiatives

The Office of Management and Budget (OMB) began collecting Critical Infrastructure Protection budgetary data as a result of Presidential Decision Directive 63, signed in May 1998. While the budget data in this Annex shows the impact of the President's initiatives with useful accuracy, the quality of data does not meet OMB's typical expectations for several reasons.

As CIP is a new Presidential priority, Agency budget systems don't readily support collection of CIP data. Until these systems are modified, collection of information on CIP programs and budgets will be manual and inexact. The newness of CIP also means that the Government is still on the steep part of a precipitous learning curve. Individual Agencies are still grappling with the issue internally, and the interagency process is still coming together. For example, our lack of familiarity affects the uniformity of assumptions and the relative prioritization agencies make. When OMB issued its first CIP Budget Data Request (BDR) last year, it sought information at an *activity level*. But because of inadequate activity descriptions and data presentation problems, it was unable to consolidate the data, making it difficult to identify programmatic duplications and gaps that point up inconsistencies needing analysis and remedy. All this reduced confidence in the data.

To resolve the problems we had in recent years, last spring OMB and the National Security Council launched a new process to review high-priority national security programs that cross Agency lines. The process includes critical infrastructure protection and other crosscutting programs (i.e., combating terrorism, weapons of mass destruction preparedness, and continuity of operations). The crosscut ensures that recommendations for these programs are made in a Government-wide context rather than Agency by Agency. The new process involves four phases:

- *Program Review.* Interagency working groups, chaired by the National Security Council or the Office of Science and Technology Policy, review the crosscutting issues in a Government-wide context. The groups identify gaps and duplications in the national effort and develop detailed programmatic initiatives to increase our effectiveness in countering unconventional threats.

- *Budget Review.* For each issue area, a budget subgroup consisting of Agency program staff, Agency budget staff, and OMB examiners develop budget-quality cost estimates for the programmatic initiatives. This phase is not an endorsement of funding for the initiatives, but instead is an effort to provide realistic, well-justified cost estimates.

- *Agency Action on Recommendations*. The working groups then prioritize the initiatives and transmit them as funding recommendations to the Agencies. Agencies will address the recommendations in the context of other priorities and fiscal constraints in their fall budget submissions to OMB.

- *Review of Agency Action*. OMB will review Agency action on the recommendations and make any necessary course corrections in Passback based on information from the working groups, other Agency priorities, and available resources.

These efforts to improve collection and analysis of CIP data were evident in the development of the President's Proposed Budget for FY2001. The process was completed under an accelerated schedule for the FY2001 budget, and will be used to develop the FY2002 budgets for crosscutting issues. Figure 4 depicts that schedule.

Activity	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Develop IWG Programmatic Recommendations											
Develop IWG Budget Recommendations											
Integrate IWG Recommendations into Agency Budgets											
Review Agency Action on Recommendations											
Resolve Outstanding Concerns											

Figure 4. CIP IWG FY2001 Schedule

This schedule ensures participants in the process have adequate time to identify reasonable requirements and ensure there are no gaps or redundancies among Agencies. In addition to the improved schedule, OMB requested that the programmatic and budgetary recommendations follow a consistent format and provide adequate detail to facilitate budgetary analysis. The programmatic template is depicted in Figure 5.

- **Initiative Description**—What is the initiative, what does it buy or do?
- **Execution**—Which Agency(s) would carry out the initiative?
  - Which Agency(s) would provide funding for the initiative? Explain the basis for these choices.
- **Background**—Briefly state the history, if any, of similar initiatives.
- **Rationale**—Provide the reasoning for the proposed initiative.
- **Relationship to Current Program**—Is this a new initiative or an enhancement to ongoing effort? Is it a change in the approach to this issue?
- **Relationship to PDDs and other Administration guidance**—Is this initiative a national policy requirement/how does it support national policy requirements?
- **Relationship to Lead Agency guidance**—How does it support Lead Agency guidance for that activity? Did Lead Agency request this initiative?
- **Relationship to host agency guidance**—How does this relate to the Agency mission and strategic plan? Is it logical for this Agency to undertake the program? Does the initiative support the results of Agency vulnerability studies/threat assessments?
- **Relationship to private sector**—Why should the Government do this instead of the private sector? What data shows the need for Government involvement? What does the relevant industry say about the Government's role here?
- **Program Effectiveness**—What performance indicators and/or assessments are planned to measure the performance and effectiveness of the program? How will program effectiveness and accomplishments be measured?

Figure 5. Programmatic Recommendation

The budget template is depicted in Figure 6.

- **Initiative Description**
  - What is the initiative, what does it buy or do?

- **Funding Location**—Note the Agency/organization in which the initiative will be funded, budget account, the line item within the account, and the program office that would administer the program.

- **Funding Stream**
  - How much does it cost? Is the cost a one-time expense and/or recurring expenses?
  - For initiatives that affect ongoing programs, what were the program funding levels in prior years? Note any expected Congressional action on last year's budget request for this program.

- **FTE Stream**
  - Does the initiative require additional FTEs? How many, and at what levels?
  - For initiatives that affect ongoing programs, what were the program's FTE levels in prior years?

- **Proposed Source of Funding**
  - Continuation of prior year base funding?
  - Offsets or new fees?

Figure 6. Budget Recommendations

Data Call for Critical Infrastructure Protection Funding and Program Information

A critical element of the interagency review process is the annual OMB data call on programs to counter unconventional threats. The information provided in the data call will inform the program and budget reviews conducted by the interagency working groups as well as OMB's budget review. To conduct the data call, OMB issues a Budget Data Request (known as the National Security Crosscut for Unconventional Threats) for information, including funding levels, on Government-wide programs for critical infrastructure protection, combating terrorism, defense against weapons of mass destruction, and continuity of operations. The data is used to determine whether existing requirements are appropriately funded; to identify potential gaps, duplication, and synergies across the Government; and, to monitor the progress of particular initiatives of interest to the White House and the Congress.

The data call now utilizes databases to collect funding levels, narrative descriptions, and characterization information at the activity level. For each relevant activity included in their budgets, Agencies report actual or enacted funding for prior and present years, and requested funding for future years. In addition, Agencies report funding for any initiative recommended by the relevant NSC-chaired interagency working group charged with reviewing these programs.

ANNEX C

WORKING TOWARD A FEDERAL R&D AGENDA IN CRITICAL INFRASTRUCTURE PROTECTION

Background

In PDD-63, the President directed that within 180 days, a schedule for a National Infrastructure Assurance Plan be submitted to him from the CICG Principals Committee with milestones for accomplishing,

> *"Research and Development: Federally sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable."*

To respond to this tasking, the National Science and Technology Council's Committees on National Security and Technology, and the Critical Infrastructure Coordination Group established under PDD-63, directed the Critical Infrastructure Protection Interagency Working Group (CIP IWG) to prepare a Federal research and development strategy as one element of a broader Federal response to the challenge of critical infrastructure protection (CIP). The strategy highlights five priority R&D issues. Three—vulnerability and risk assessment studies, information assurance R&D, and interdependency analyses—are common to all the infrastructure sectors. The other two issues are more specific, but require immediate attention: intrusion detection and monitoring, and the security of automated infrastructure control systems.

The IWG defined five critical infrastructure sectors: Banking and Finance; Information and Communications; Energy; Transportation; and Vital Human Services. It also defined a composite sector that it calls Interdependencies.

Achieving PDD-63's goal of an initial 2001 and full 2003 capability of attaining and maintaining the ability to protect America's critical infrastructures from harm is a daunting challenge. Maintaining those protective capabilities will be a dynamic challenge, as the rapid evolution of technology assures that there will be an ever-evolving stream of new vulnerabilities in new technologies to our ever-evolving infrastructures. Realistically, achieving an initial 2001 capability will, of necessity, draw primarily upon existing technologies, and a full 2003 capability of protecting our infrastructures will, at most, draw upon new technologies to only a limited extent. Yet the critical infrastructure protection challenge will remain even as those future years melt and become the distant past. The verities of human nature, as well as the capriciousness of Mother Nature, will ensure that measures to protect our infrastructures will be challenged by countermeasures trying to overcome them. We will face the *Alice-in-Wonderland* task of running as hard as we can just to stay in the same infrastructure protection place, which will require ongoing R&D to address this never-ending challenge.

Vision and Objectives

A vigorous and effective program of Federal R&D in critical infrastructure protection should seek to enhance the security of our Nation's critical infrastructures by rapidly identifying, developing, and facilitating the fielding of technological solutions to existing and emerging infrastructure threats and vulnerabilities. The process to achieve this should embody:

- an awareness of the state of new technological developments as they become embedded in infrastructures and the new avenues they present for hostile and non-hostile disruption of these architectures;

- an ability to produce an affordable menu of R&D programs in critical infrastructure protection in time to be useful to those who make resource allocation and infrastructure protection planning decisions in Government and the private sector;

- a functioning, effective two-way interaction with the private sector, academia, and other countries so that R&D overlap is minimized and programs are pursued that best meet the needs of the private sector and Government; and

- an innovative management structure that is sufficiently flexible and responsive to a rapidly changing infrastructure environment in terms of technology and threats.

A successfully functioning R&D program will require intrusion detection systems that ideally have high detection rates and low false alarm rates. It will also require systems that can isolate problem portions of infrastructures and either "heal" them quickly or rapidly bring substitute capability online, all while protecting the rest of the infrastructures from harm. It will not be enough to meet the PDD-63 deadlines of 2001 and 2003. Evolving technologies that provide new avenues for critical infrastructure disruption will necessitate a continuing R&D program to maintain our critical infrastructures in a robust condition. The IWG thus believes that in order to maintain the goals of PDD-63, a vigorous and effective R&D agenda in critical infrastructure protection is an essential prerequisite.

Based on the direction from PDD-63 and guidance from the Committees on National Security and Technology, as well as the Critical Infrastructure Coordination Group (CICG), the IWG established the following objectives:

- *Develop and coordinate the Federal Government's critical infrastructure protection R&D agenda in accordance with guidance from PDD-63*: The comprehensive menu should include information about ongoing Federal programs, short- and long-term research plans, budget information, and proposed R&D policy.

- *Monitor and coordinate ongoing and planned Federal CIP R&D*: The IWG provides a forum to identify and resolve issues in recommending a national R&D agenda, policy, and programs.

- *Foster conditions for the development of a close partnership with the private sector, academia, and international community*: Given the volume of CIP R&D performed by and the expertise resident in industry, academia, and the international community, the Federal program must be developed in close conjunction and partnership with these communities.

- *Facilitate the smooth and timely transfer of technology among Government Agencies and between them and the private sector*: Technology developed in Government laboratories should be rapidly transferred to the private sector, particularly if the Federal Government concentrates primarily on research and the private sector on development.

- *Respond to the needs of the NSC, National Coordinator, CICG, and infrastructure stakeholders as appropriate*.

Sector R&D Needs

A review of existing and potential infrastructure vulnerabilities, and current capabilities, has identified numerous R&D needs in each sector, as described below.

Banking and Finance

Financial institutions are in the forefront of developing and utilizing security methods for reasons of competitive self-interest. Considering the strong role of Government regulation and the influence of other types of scrutiny to which the financial system—particularly banks—is subject, this sector maintains an advanced pace of vigilance, network control, and tools development. Overwhelmingly, the private sector performs the R&D for the security of the banking and finance infrastructure. However, Government has a vital interest not only in the overall health and integrity of the U.S. financial system, but specifically in the essential parts of it that are Government-owned and operated—such as the FedWire payment system of the Federal Reserve. Also, there are serious law enforcement and national security concerns regarding use of the national and global information infrastructures centered on such issues as encryption.

The requirements between current ongoing infrastructure security research and development within the financial service industry and the macro-level vulnerabilities of concern to the Government fall into the following basic areas:

- Authentication technologies
- Physical and electronic protection technologies
- Test facilities
- Simulation model development
- Information security analysis
- Intrusion indications and warnings tools
- System reliability enhancement
- Information system standardization
- Electronic commerce security enhancement

Information and Communications (I&C)

New R&D efforts are needed to address new vulnerabilities in this critical sector of the U.S. economy. The following nine research areas need special attention to address recognized vulnerabilities:

- *Modeling and Simulation Tools for the I&C Infrastructure*: Will develop a set of representative models and simulation tools of the I&C critical infrastructure necessary to create and evaluate the technologies required to protect it.

- *Vulnerability Detection, Assessment, and Analysis*: Will identify, collect, organize, and disseminate system, network, and infrastructure vulnerability, as well as develop applied techniques to avoid, reduce, or eliminate vulnerabilities during the development of hardware and software products and their integration into systems.

- *Response, Recovery, and Reconstitution*: Will develop methodologies to contain, stop, or eject intruders and to mitigate damage or restore information-processing services in the event of attack or disaster.

- *Reliability, Survivability, and Robustness*: Will address applying technologies to the I&C infrastructure to increase network reliability, system survivability, and the robustness of the infrastructure's systems and components, as well as the infrastructure itself.

- *Risk Management, Performance Tools, Security Testing, and Metrics*: Will address new metrics and measurement tools, e.g., real-time network performance.

- *Core Research Capabilities, Benchmarking, and Recommended Practices*: Will address the capabilities required for needed core research on the I&C infrastructure, as well as those needed to promulgate benchmarking and recommended practices throughout the I&C infrastructure.

- *Security Architectures*: Will organize security components/services to provide confidentiality, integrity, and availability for information and communication systems.

- *Assurance Technologies*: Will develop tools and techniques for rigorous design, implementation, testing, and formal verification of hardware and software components and their subsequent integration into larger systems.

- *Intrusion and Incident Detection and Warning*: Will develop tools and procedures to improve capabilities to detect, respond to, and recover from incidents or attacks. These efforts will include, artificial intelligence-based systems that automatically detect patterns indicative of network intrusions.

Energy

The increasing complexity of America's energy system and the economic forces driving the industry to operate with smaller reserve margins may reduce our ability to respond quickly to major infrastructure outages. The research areas below would address both current vulnerabilities and those that may arise as the industry changes:

- Conduct of vulnerability assessments
- Critical consequence analysis
- Development of real-time control mechanisms
- Development of high-security SCADA systems
- Development of efficient, adaptable encryption
- Development of robust authentication and authorization
- Sensor and warning technology
- Transmission and distribution systems in the electric power industry
- Emergency response and recovery procedures
- Evaluation of policy effects
- Directed energy technology countermeasures
- Analysis of scale and complexity
- Online security assessments
- Dispersed generation
- Decision support systems
- Evaluation of institutional barriers
- Threat assessment for risk management

Transportation

It is essential the major elements of the transportation infrastructure—including all modes and both physical and electronic aspects—be able to withstand both deliberate and natural disruptions and return to normal levels of service as rapidly as possible. Even though the U.S. enjoys the best transportation and distribution system in the world, the system is not immune from such disruptions. DOT has been working closely with transportation users and researchers in the private sector, academia, and other Federal, state and local agencies to identify broad-based security needs and develop programs to help fill in these 'gaps.' As a result of these efforts, DOT has developed the following list of R&D initiatives and estimated funding for FY2000-2005 related to the security of the transportation infrastructure:

- Development of a high-accuracy inertial navigation system and landing backup system for aircraft to use if normal systems (GPS, WAAS and LAAS) are disrupted.

- Improved capabilities to model, detect, and mitigate the impact of toxic chemical and biological agents released in transportation facilities.

- A comprehensive approach to all aspects of security at passenger and freight terminals, including passengers, cargo, facilities, energy supplies, and electronic and communications systems.

- A vulnerability analysis comparing open vs. closed and distributed vs. decentralized transportation operating systems models.

- An assessment of the human factors role (preparedness, prediction, response) in transportation systems to determine future training and education needs.

- An assessment of the electromagnetic compatibility and vulnerability of the electronic systems implemented in the Intelligent Transportation Systems and Positive Train Control programs.

- An assessment of the impact of GPS disruptions on civilian transportation users and refining the National Differential GPS service for improved navigation.

Vital Human Services

The CIP R&D needs for the water supply sector were identified by referring to two reports of the President's Commission on Critical Infrastructure Protection (PCCIP): *Critical Foundations: Protecting America's Infrastructure* and *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National infrastructures.* These references are supplemented with information from EPA staff.

Potential topics and activities for R&D in the water supply sector include:

- identifying and characterizing biological and chemical agents;

- developing biological and chemical agent detectors;

- implementing SCADA systems that integrate measures for preventing intrusions and disruptions;

- developing tools for conducting vulnerability assessments of water supply systems; and

- creating a center of excellence for risk assessment of water supply systems.

Interdependencies

Interconnections among infrastructures have long been recognized. In the 1930s, the Army Air Corps Tactical School developed its "industrial web" theory, which postulated the infrastructures of an industrialized nation were interconnected. An air campaign planner could exploit these interdependencies by searching for and attacking bottlenecks—those crucial points that would disrupt the entire fabric of an enemy's economy. The American economy today, however, is vastly more interconnected than those of industrialized nations a half a century ago. Accelerating computer and information technologies have increased the interdependencies among the infrastructures. The cyber nation of our infrastructures has created an intense reliance upon an underlying fabric of telecommunications and information networks. The infrastructures also rely

heavily upon the Nation's energy production and distribution networks, especially through the I&C infrastructure's energy requirements. The net result is that our modern infrastructures are tied together, sometimes in ways that are not obvious. The overall impact of these linkages is not well known or understood, although there is a body of anecdotal evidence that provides some insight. Recommended research areas include:

- *Characterization of Interdependencies*: Would examine what the interdependencies are and how they should be characterized.

- *Complexity Theory*: Infrastructures are complex adaptive systems. Further research into the complex and adaptive behaviors of U.S. infrastructures is needed, especially if we are to better understand how infrastructures will respond and degrade in the face of a physical or cyberattack.

- *Modeling and Simulation*: Modeling and the simulation of large, interconnected, complex infrastructures are rudimentary today. More advanced models, employing actual regional or national infrastructure data, physical network layouts, and operating conditions are needed to help uncover critical nodes, emergent behaviors, and vulnerabilities.

- *Vulnerability Studies*: We do not currently have a good understanding of interdependencies or the vulnerabilities they introduce into our national infrastructures. Analysis is needed to better understand the vulnerabilities, locate key nodes and linkages, and develop strategies to lower or eliminate such vulnerabilities.

- *Mitigation Technologies*: In the event of an infrastructure attack or other failure, it will be important to isolate the affected portions of the infrastructure, prevent the further propagation of disturbances, and remedy damages. These steps will require accurate accounting of linkages among the infrastructures and behaviors arising from such interdependencies.

- *Policy Research*: Policies for one infrastructure may have unintended consequences in others, due to the linkages among the infrastructures. Little is know about this phenomenon and how to reduce the likelihood of its impact on critical infrastructures as a whole.

Developing a Federal R&D Menu

The Federal CIP R&D IWG used a direct approach to developing a Federal Government R&D menu. The IWG identified the major vulnerabilities of each sector, as well as the existing CIP R&D work and programs already funded by the Federal Government. The IWG then sketched out an ideal, fiscally unconstrained set of programs to address these vulnerabilities. The gaps between the ideal and what was currently being undertaken then formed the raw material from which to develop an R&D menu for FY2000 and beyond.

A "Work-in-Progress" Comprehensive Federal CIP R&D Menu

Given the dynamic nature of the technologies involved, any comprehensive set of programs that are presented as a complete menu for addressing critical infrastructure protection is at best a

snapshot in time. Any program set will need to be updated on an almost continuous basis. A comprehensive menu of CIP R&D initiatives consists of 71 programs, and include:

- 9 in the Banking and Finance sector;
- 19 in the Information and Communications sector;
- 17 in the Energy sector;
- 8 in the Transportation sector;
- 12 in the Vital Human Services sector; and
- 6 in the Interdependencies category.

Two of these programs were not pursued further because the Weapons of Mass Destruction Protection Group is planning to recommend funding these initiatives in its program. The list, while comprehensive, should not be considered fully complete, as Agencies are still uncovering new areas of R&D opportunity. Keeping this list current will require continuing interagency attention. The IWG also believes relative priorities among the various initiatives, as well as initiatives that will be identified in the future, will change over time.

These are program proposals only for the Federal Government and do not directly address the R&D the private sector is conducting. The Federal Government attempted to identify private sector R&D programs, but found great reluctance to reveal any but the most general descriptions of their work.

Understanding the Menu

A review of the extensive list of initiatives that the IWG identified illustrates the extent to which cyber nation has embedded itself in U.S. critical infrastructures. Of the 71 initiatives that the IWG identified for inclusion in its CIP R&D comprehensive menu, 50—more than two-thirds—are either partly or fully addressed to information-related issues. Less than one-third of these initiatives are not cyber-related. These initiatives represent less than 20% of the funding of the comprehensive menu.

In reviewing these sector initiatives, the IWG found that there are several needs common to most or all of the sectors including: vulnerability and risk assessment studies; information assurance; and interdependency analysis.

The crosscutting nature of these needs, and the overall importance of the initiatives that embody them, give those initiatives highest priority among those identified by IWG. In addition, the IWG judged two specific issues as serious enough that they require immediate attention: intrusion detection and monitoring, and the security of automated infrastructure control systems.

While some work has been done on the intrusion detection problem, it has been insufficient to provide the level of detection needed. The Government review also found that automated infrastructure control systems, especially Supervisory Control and Data Acquisition Systems (SCADA), are important throughout the U.S. economy, and they appear especially vulnerable based on studies to date. Accordingly, initiatives to address these two issues also merit priority attention. Of the 71 initiatives overall, 31 address these priorities:

- *Vulnerability and Risk Assessment Studies*
  - I&C Vulnerability Detection, Assessment and Analysis
  - I&C Risk Management Performance Tools
  - I&C Risk Analysis
  - Energy Vulnerability Assessments
  - Energy Threat Assessment for Risk Management
  - Transportation System Vulnerability Analysis
  - Space Infrastructure Vulnerability Analysis
  - Transportation Vulnerability Assessment of GPS-Dependent Systems
  - Transportation Generic System Vulnerability to Cyberattacks and EMI
  - Vital Human Services (VHS) Water Supply Vulnerability
  - VHS Emergency Medical Services Vulnerability Assessment
  - Interdependencies Vulnerability Assessment of Interdependent Systems

- *Information Assurance*
  - B&F Authentication Technology
  - B&F Information Security Analysis
  - B&F Electronic Commerce Security Enhancement
  - I&C Assurance Technologies
  - I&C Patch Use Detection
  - I&C Encryption Technology
  - Energy Sector Efficient Adaptable Encryption
  - Energy Online Security Assessment

- *Intrusion Detection and Monitoring*
  - B&F Intrusion I&W Tools
  - I&C Intrusion and Incident Detection and Warning
  - I&C Artificial Intelligence Software Trapdoor Analysis

- *Secure Automated Infrastructure Control Systems*
  - I&C Secure Supervisory Control and Data Acquisition (SCADA) Systems
  - Energy Sector High Security SCADA Systems

- *Interdependency Analyses*
  - Identification and Characterization of Interdependencies
  - Analysis of Scale, Complexity, and Trends
  - Systems Analysis and Simulation Tools
  - Consequence Analysis and Risk Management Methodologies and Tools
  - Vulnerability Assessment of Interdependent Systems
  - Protection and Mitigation

Estimated funding for all 71 initiatives totals $750 million. This high-end funding would increase Federal CIP R&D spending by 150% in one year, an unlikely and probably inefficient step. It funds a large number of new starts and assumes that the Federal Government would plunge into the defined programs without the usual "ramp-up" process. This would probably ensure quicker results, but with higher funding inefficiency in achieving those results. The projected six-year funding of just the new initiatives would total $6.16 billion.

Partnership

One of the most important CIP challenges facing the Federal Government is to establish and maintain a viable two-way dialogue on critical infrastructure protection with the private sector, academia, and other countries as appropriate. Partnership is not too difficult on a one-way, outgoing basis, and the IWG made a number of overtures to different non-Federal groups during the course of its work. Establishing a true two-way dialogue, on the other hand, is far more difficult.

Industry-sponsored R&D is almost exclusively directed at either developing new marketable products and services or solving internal problems. Industry is understandably reluctant to share details of proprietary work that is of significant economic value to them. This constraint on information availability has made it possible for the IWG so far only to discern the vague outlines of CIP R&D in industry, and industry's corresponding investments.

R&D Sector Survey

- *Banking and Finance*: No current research was identified in the banking and finance private sector. While this industry has made good use of technologies developed elsewhere, the IWG could not determine whether the private sector will develop on its own or contract the development of the new technologies that will be necessary to protect the infrastructure at the national level in the future.

- *Information & Communications*: Today's public telecommunications infrastructure includes the Public Switched Telecommunications Network (PSTN) and the Internet. These two separate networks, which already have many interdependencies, are expected to effectively converge in the future. The distinctions between separate PSTN and Internet R&D efforts are likewise expected to blur as the anticipated transition to a more integrated telecommunication infrastructure takes place over time.

  The private sector R&D community is currently pursuing several issues that affect network assurance related to the PSTN, the Internet, and the combination of the two networks, as shown below (along with the network assurance criteria each area affects):

  - *Private Network-to-Network Interface (PNNI)*: stability, interoperability, survivability, policy, and service issues.

- *Wavelength Division Multiplexing (WDM)*: performance, quality of service (QoS), security, and survivability issues.

- *Wireless*: performance, reliability, quality of service, and other service issues.

- *Next Generation Internet (NGI) Infrastructure*: performance, interoperability, quality of service, scalability, survivability, security, policy, and service issues.

- *Interdomain Routing, Policy Routing/Architecture*: stability, availability, reliability, and policy issues.

- *Label Switching Technology*: scalability, stability, quality of service, performance, interoperability, policy and service issues.

- *Active Networking*: performance, security, survivability, and service issues.

- *Quality of Service, Differentiated Services*: performance, quality of service/service issues;

- *Multicast*: scalability, stability, reliability, security, policy, and service issues.

- *Operations and Network Management, Distributed Control*: scalability, stability, quality of service, performance, interoperability, reliability, security, policy, and service issues.

- *Security*: security, survivability, performance, scalability, and service issues.

➢ *Energy*: In addition to individual companies, the primary organizations performing non-Federally funded R&D are the Gas Research Institute (GRI), the American Gas Association (AGA), and the Electric Power Research Institute (EPRI). All have experienced significant R&D budget reductions in recent years. The IWG did identify the following broad areas of interest as topics of private sector concern, though it was unable to ascertain what non-Federally funded R&D is ongoing:

- Instrumentation and Monitoring for Distributed Control;
- Analysis and Computation for Large-scale Systems;
- Advanced Control Methods; and
- Decision Support Tools

DOE identified a list of R&D topics in which the private sector is likely to have an interest and is likely to be involved:

- Critical Consequence Analysis of the Energy Sector;
- Real-time Control Mechanisms;
- Vulnerability Assessments;
- High Security SCADA Systems;
- Efficient Adaptable Encryption;
- Robust Authentication and Authorization;

- Sensor and Warning Technology;
- Transmission and Distribution;
- Emergency Response and Recovery;
- Evaluation of Policy Effects;
- Directed Energy Technology Countermeasures;
- Analysis of Scale, Complexity of the Energy System;
- Online Security Assessment;
- Dispersed Generation;
- Decision Support Systems;
- Evaluation of Institutional Barriers; and
- Threat Assessment for Risk Management.

- *Transportation*: A considerable amount of private sector effort can be seen in the development of detection methods for explosives, weapons, and other contraband. Much of this emphasis is associated with the increasing use of these security systems at airports and other transportation terminals, and with the growing volume of international freight moving in containers. There is considerable interest in developing fast, reliable, non-intrusive, and reasonably priced means to screen large numbers of passengers and large volumes of freight. One promising approach the private sector is pursuing involves integrating technologies (e.g., enhanced x-ray, computer-assisted topography [CAT] scan, and particle detection) into a single system capable of high throughput volumes.

  Finally, there is private sector work underway to refine the use of video systems to enhance security. This includes development of video pattern recognition capabilities to detect movement, on-board digital video storage directly to hard drives, and image and sound transmission from a transportation vehicle to a control/response center.

- *Vital Human Services*: The American Water Works Research Foundation is the chief organization doing research on water issues in the private sector. The focus of these projects is water quality and its resulting health and safety impact on the public. The projects range from theoretical modeling of distribution systems, to chemical and biological studies of various contaminants and physical assurance development. A sample of these projects follows:

  - Pathogen Intrusion in the Distribution System;
  - Water Quality Modeling of Distribution Systems and Storage Facilities;
  - Characterization and Modeling of Chlorine Decay in Distribution Systems;
  - Rapid Screening of Pathogens in Water;
  - Automatic Feedback Control of Chlorine Booster Systems for Distribution Residual Maintenance;
  - Detection and Occurrence of Caliciviruses in Drinking Water;

- Methods for Detection of Human Viruses;
- Removal of Cyanobacterial Toxins from Drinking Water Using Ozone and GAC; and
- Leak Detection.

One potential mechanism for intrusion into water system operations involves supervisory control and data acquisition (SCADA) systems. In organizations such as the Tennessee Valley Authority, the Corps of Engineers, and the Bureau of Reclamation, water SCADA systems are integrated with electric power SCADA systems, introducing sector interdependencies. Research on the security of SCADA systems is a major concern in electric systems as well.

Trends in Private Sector R&D Spending

R&D spending data for the major telecommunications providers has been available since 1988. Although year-to-year R&D spending largely fluctuates across different providers, the overall spending trend showed consistent, modest annual growth of 1.9%, from $342 million in 1988 to $376 million in 1993. However, from 1994 to 1996, provider R&D spending dropped alarmingly, from $272 million in 1994 to $219 million in 1996. This is an average annual decrease of 7%. This is a worrisome trend, especially given the rapid technological change in the industry.

Although not fully comprehensive, other industry spending figures for telecommunications-based R&D also exist. Published data is available for the 1985 and 1995 R&D expenditures of eight telecommunications companies: Lucent, AT&T/other, Bellcore, Motorola, Cisco, Alcatel, Ericsson, and Nortel. Most of these companies are either telecommunications carriers or vendor companies with major R&D laboratories. The contributions of this eight-company total are significantly larger than the overall Government and provider contributions. Although the last three listed are foreign companies, they are included to highlight their significant private sector contributions and to emphasize the international aspects of R&D spending in this field.

A look at the investment figures for these eight companies shows another disturbing trend. The total eight-company contributions increased by roughly 64% from 1985 to 1995, while the total five U.S. company contributions increased by only 50%. *Thus, the IWG calls special attention to the fact that foreign-based R&D investment on telecommunications is increasing significantly faster than U.S.-based R&D investment.*

The IWG also notes that *vendor* R&D investment is greater than for *provider* companies. The traditional dominant role that Bell Laboratories (now Bellcore) held in the past in R&D funding and innovative R&D is quickly diminishing and is being replaced by the telecommunications vendor companies. Vendor company R&D funding is directly related to healthy equipment sales, which are more volatile than the more predictable telephone cash flows.

The IWG has begun planning a series of workshops on CIP R&D. Topics under consideration include intrusion detection research to assure Federal operations; improving Government-private sector R&D sharing; international outreach; the adequacy of CIP R&D trained personnel, and human factors in critical infrastructure protection; among others. A conference is also under consideration. The IWG will also establish further contact with industrial associations (e.g., IEEE, computer security associations, etc.) and advisory committees such as NSTAC, the President's Information Technology Advisory Council (PITAC), and others.

Updating the Critical Infrastructure Protection R&D Menu

There are 13 tasks the Federal Government will need to perform annually to keep the R&D menu current and to ensure it remains abreast of current technology in infrastructure protection:

- Identify and update threats to and vulnerabilities in the Nation's critical infrastructures that are amenable to technological solutions.

- Identify and maintain a database of ongoing and proposed Federal Government CIP R&D programs and known private sector, academic, and international programs.

- Develop and update a comprehensive, conceptual menu of R&D programs required to address known and emerging infrastructure vulnerabilities.

- Identify update gaps and shortfalls in the existing programs based upon the comprehensive program and vulnerabilities. Develop an appropriate set of criteria for judging the priorities for Federal Government action.

- Work in close conjunction with relevant Department and Agency personnel and Sector Liaison officials and recommend R&D areas for increased focus. Identify budget requirements needed to fulfill the recommendations of the CIP R&D menu. Coordinate this activity with annual Federal budget cycles.

- Provide a forum and develop proposals to facilitate sharing of information about ongoing and planned CIP R&D programs within Government.

- Develop means to harmonize Federal CIP R&D with other existing Federal R&D programs with which there may be overlaps or similar interests (such as those related to weapons of mass destruction, high-performance computing, and force protection). Coordinate with other interagency forums and working groups (such as the Technical Support Working Group [TSWG], high-performance computing, etc.) as appropriate.

- Develop means to harmonize Federal CIP R&D with the private sector, state and local governments, academia, and international programs.

- Develop proposals to facilitate technology transfer among Government Agencies and between the Government and the private sector. (This may appear to be redundant with one of the objectives; however, it is important to emphasize this task).

- Establish and utilize a review group of outside industry and academic experts in critical infrastructure protection R&D disciplines to review existing and proposed programs.

- Propose mechanisms to encourage and provide the environment to foster a partnership among the Government, private sector, and academia for CIP R&D.

- Develop means to coordinate public outreach on R&D issues.

- Monitor foreign program and policy developments that may affect the direction or effectiveness of the Federal program, and address possible relevant international cooperation.

Management Challenges

The characteristics of the proposed R&D program, coupled with the sheer size and significance of the critical infrastructure assurance problem, virtually mandate innovative management concepts and structures to carry out the Federal Government's CIP R&D menu. The factors below demonstrate the need for innovative management concepts and structures to effectively develop and administer a successful R&D menu.

While the Government will fund a significant portion of the research, the private sector will probably perform the bulk of the developmental work. Market forces will drive this development and direct it toward products that have a market. Coordinating Federal R&D with ongoing private sector programs will be complicated by industry's desire to guard proprietary programs and trade secrets. Performing the right research at the right time, synchronizing Government programs appropriately with those in industry, and ensuring timely transfer of Government-developed technologies to industry will require close coordination and partnership with the private sector.

The Government CIP R&D menu by its very nature cuts across a large number of Federal Departments and Agencies. Ensuring proper coordination of individual R&D programs within Agencies, let alone across Agency boundaries, is an important task for the IWG to address. Likewise, the IWG must ensure that technologies are rapidly transferred among the Agencies, and out to the private sector. In its activities to date, the IWG has already observed cases in which Agencies had specific R&D needs yet were unaware that such programs were ongoing elsewhere within the Federal Government. In addition, a variety of Federal Government working groups manages similar or related programs, such as the Technical Support Working Group and the Weapons of Mass Destruction Protection IWG. It will be crucial to ensure proper coordination and communications among such groups. The crosscutting nature of critical infrastructure protection R&D budgets further complicates program management and demonstrates the need for innovative, new approaches.

Third, the technology, vulnerabilities, and threats are evolving at an accelerating pace, such that they will quickly outpace the ability of the traditional lengthy Federal budget process to keep up. This year's technological fix to a vulnerability could be obsolete within a few years, if not months. Entirely new systems could evolve in this time period, with their own vulnerabilities.

Given the three-year nature of the Government budget cycle (one year to develop the budget, one year to pass Agency funding bills in Congress, and one year to begin to execute the programs), the rapid pace of technological innovation in critical infrastructures will stress any system put in place to develop and coordinate a Government-wide R&D program. The Federal R&D menu must have the flexibility to deal with rapid changes in technologies and threats.

Fourth, the Federal R&D program should be coordinated with state and local governments. In particular, the needs of "first responders" to emergencies and other assistance providers will determine many of the research directions in the vital human services sector. Factoring these needs into the Federal R&D menu is a step that can only be done through innovative management and partnership with the state and local levels.

Fifth, the potential consequences of critical infrastructure assurance events impel us to consider steps beyond a business-as-usual approach to the problem. A major cascading failure in our information and telecommunications systems, whether hostile or non-hostile in origin, though perhaps unlikely, would threaten the economic foundations of the country. The sociological and political aftermath would further add to the damage done. This situation is the classic risk management problem of the small chance of a catastrophic consequence. The threat of nuclear weapons spawned new management approaches to national security from the late 1940s into the 1980s based on the potential threat consequences. In the same fashion, the potential consequences of a major cascading cross-infrastructure failure in the increasingly interconnected 21st century warns us to consider new approaches to managing R&D in this area.

Observations

- Current Federal CIP R&D is estimated at $500 million for FY2000.

- Determining the appropriate levels of CIP R&D funding will need to take into account new budget initiatives, including new PDD-62 initiatives in weapons of mass destruction and counter-terrorism, as well as the Information Technology Initiative.

- There is a potential problem in ensuring that our academic institutions will be able to conduct the basic research needed in this area and to train the numbers of scientists and engineers needed for critical infrastructure protection, due in part to the appealing opportunities in the private sector. Steps such as the Federal Information Technology Service and similar programs will be needed to address this problem.

- This portfolio of research will need continuing review and revision in the years ahead because of the dynamic nature of the technological environment it seeks to harness.

- The extent to which Agencies have experiences in CIP R&D management will affect the pace at which they can ramp up their efforts on the programs identified in this menu. The wide variation in CIP R&D management experience across different Agencies underscores the importance of coordinated R&D oversight and innovative management solutions for addressing the CIP R&D menu.

- Critical infrastructure protection presents one of the most demanding Federal management challenges of the post-Cold War era. The pace of technological change ensures that in the future the landscape of infrastructures and infrastructure protection will likely transform itself much faster than in the Cold War. The double-edged sword nature of this rapid pace of change will mean new avenues for hostile and non-hostile disruption will accompany the benefits from these changes.

- Any R&D process to manage our response to these new challenges must be sufficiently flexible to keep pace with this revolutionary environment.

Recommendations

- America needs a vigorous program of R&D in critical infrastructure protection to ensure that critical infrastructures remain safe in the years ahead as new technologies become embedded in these infrastructures.

- Existing and planned CIP R&D activities need coordination with other Presidential initiatives to preclude overlap and promote synergy among these initiatives.

- A program to strengthen university training and research in disciplines that support CIP R&D should be proposed in the FY2002 budget cycle.

- The National Science and Technology Council should explore options for R&D management models embodying the flexibility and nimbleness needed to ensure that the CIP R&D process can keep pace with the revolutionary technology environment for critical infrastructure protection in the years ahead. It should seek such models from both inside and outside the Federal Government.

ANNEX D

GLOSSARY AND ACRONYMS

Access	The right to enter or use a system and its resources; to read, write, modify, or delete data; or to use software processes or network bandwidth.
Alert	Notification of a specific attack directed at the information system of an organization.
Anomaly detection	Detecting intrusions by looking for activity that is different from the user's or system's normal behavior.
Assurance	Grounds for confidence that a system design meets its requirements, or that its implemented satisfies specifications, or that some specific property is satisfied.
Attack	A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it.
Attack signature recognition	The means to recognize specific identifiable characteristics—technical, procedural, or equipment-based—of known attack profiles.
Banking and Finance	A critical infrastructure characterized by entities, such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support activities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.
Capability	The ability of a suitably organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communications systems and/or to disrupt, deny, or destroy all or part of a critical infrastructure.
Chief Information Officer	Agency official that provide advice and other assistance to the head of the agency and other senior management personnel to ensure that information technology is acquired and information resources are managed in a manner that implements the policies and procedures of the Congress and the priorities established by the head of the agency. Section 5125(a) of the Information Technology Management Reform Act of 1996 (ITMRA) establishes the position of Chief Information Officer (CIO) by amending Section 33506 of the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.
Civil liberties	Those individual rights and freedoms protected by the Constitution, the Bill of Rights, and Federal law and regulations.

Competition	Activity of two or more entities taken in consideration of each other to achieve differing objectives. The commercial analogue of military combat.
Computer Emergency Response Team/ Coordination Center	An element of the Networked Systems Survivability Program of the Software Engineering Institute at Carnegie Mellon University. It keeps track of attacks on the Internet and issues advisories.
Computer Emergency Response Team	An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems. (DoDD 5160.54)
Consequence Management	Includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. The laws of the United States assign primary authority to the States to respond to the consequences of terrorism; the Federal Government provides assistance as required.
Crisis Management	Includes measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The laws of the United States assign primary authority to the Federal Government to prevent and respond to acts of terrorism; State and local governments provide assistance as required. Crisis management is predominantly a law enforcement response. Based on the situation, a Federal crisis management response may be supported by technical operations, and by Federal consequence management, which may operate concurrently.
Critical Infrastructures	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..
Cyberattack	Exploitation of the software vulnerabilities of information technology-based control components.
Cyberspace	Describes the world of connected computers and the society that surrounds them. Commonly known as the INTERNET.
Debilitated	A condition of defense or economic security characterized by ineffectualness.
Defense (also National Security)	The confidence that Americans' lives and personal safety, both at home and abroad, are protected and the United States' sovereignty, political freedom, and independence, with its values, institutions, and territory intact are maintained.
Denial of Service	A form of attack that reduces the availability of a resource.
Destruction	A condition when the ability of a critical infrastructure to provide its customers an expected upon level of products and services is negated. Typically a permanent condition. An infrastructure is considered destroyed when its level of performance is zero.

Economic Security (also Global Economic Competitiveness)	The confidence that the nation's goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens.
Electrical Power Systems	A critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.
Emergency Services	A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level (county or metropolitan area). In addition, state and Federal response plans define emergency support functions to assist in response and recovery.
Expert Review Team	Security experts to assist government entities with development of internal infrastructure protection plans; the ERT is charged with improving government-wide information systems security by sharing recommended practices, ensuring consistent infrastructure frameworks, and identifying needed technical resources.
Firewall	An electronic boundary that prevents unauthorized users from accessing certain files on a network; or, a computer used to maintain such a boundary.
Gas and Oil Production, Storage and Transportation	A critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms.
Government Services	Sufficient capabilities at the Federal, state and local levels of government are required to meet the needs for essential services to the public.
Incapacitation	An abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact.
Information and Communications	A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support: ➢ The processing, storage, and transmission of data and information; ➢ the processes and people that convert data into information and information into knowledge; and ➢ the data and information themselves.

Information Assurance	Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Security	Actions taken for the purpose of reducing system risk, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities using electronic, RF, or computer-based means.
Information Sharing and Analysis Center	Centers designed by the private sector that serve as a mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information. These centers could also gather, analyze, and disseminate information from the NIPC for further distribution to the private sector. ISACs also are expected to share important information about vulnerabilities, threats, intrusions, and anomalies, but do not interfere with direct information exchanges between companies and the Government.
Information System	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.
Information Technology	The hardware and software that processes information, regardless of the technology involved, whether computers, telecommunications, or others.
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.
Infrastructure Assurance	Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage. For instance, incident mitigation, incident response, and service restoration.
Infrastructure Protection	Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures. For instance, threat deterrence and vulnerability defense.
Intent	Demonstrating a deliberate series of actions with the objective of debilitating defense or economic security by destroying or incapacitating a critical infrastructure.
Interdependence	Dependence among elements or sites of different infrastructures, and therefore, effects by one infrastructure upon another.
Intrusion Detection System	Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network. Pertaining to techniques that attempt to detect intrusion into a computer or network by observation of security logs or audit data.

Joint Task Force-Computer Network Defense (JTF-CND)	The focal point for defense of DoD computer networks and systems, monitoring incidents and potential threats, and coordinating across DoD to formulate and direct actions to stop or contain damage and restore network functionality.
Metrics	An agreed upon quantitative measure of performance.
Mission Critical	Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information).
Mitigation	Pre-planned and coordinated operator reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigatory, and crisis management response; and facilitate reconstitution.
Network	Information system implemented with a collection of interconnected nodes.
Natural Disaster	A physical capability with the ability to destroy or incapacitate critical infrastructures. Natural disasters differ from threats due to the absence of intent.
Partnership	A relationship between two or more entities wherein each accepts responsibility to contribute a specified, but not necessarily equal, level of effort to the achievement of a common goal. The public and private sector contributing their relative strengths to protect and assure the continued operation of critical infrastructures.
Patch	A quick modification of a program, which is sometimes a temporary fix until the problem can be solved more thoroughly.
Physical Security	Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks, e.g., through use of conventional or unconventional weapons.
Public Confidence	Trust bestowed by citizens based on demonstrations and expectations of their government's ability to provide for their common defense and economic security and behave consistent with the interests of society; and their critical infrastructures' ability to provide products and services at expected levels and to behave consistent with their customers' best interests.
Public Key Infrastructure	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.
Recommended practices	Generally accepted principles, procedures, and methods to assure commonality, efficiency, and interoperability.
Reconstitution	Owner/operator directed restoration of critical assets and/or infrastructure.

Red Team	Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems.
Reliability	The capability of a computer, or information or telecommunications system, to perform consistently and precisely according to its specifications and design requirements, and to do so with high confidence.
Remediation	Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc., of critical assets and/or infrastructures, e.g., emergency planning for load shedding, graceful degradation, and priority restoration; increased awareness, training, and education; changes in business practices or operating procedures, asset hardening or design improvements, and system-level changes such as physical diversity, deception, redundancy, and backups.
Response	Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident.
Risk	The probability that a particular critical infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation.
Risk Assessment	Produced from the combination of Threat and Vulnerability Assessments. Characterized by analyzing the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities.
Risk Management	Deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level. Characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned value.
Scaling	Ability to easily change in size or configuration to suit changing conditions.
Sector	a) One of the two divisions of the economy (private or public); b) A group of industries or infrastructures that perform a similar function within a society. (e.g. vital human services)
Sector Coordinator	The majority of critical infrastructures are owned and operated by private sector entities. Members of each critical infrastructure sector will designate an individual to work with the Federal Lead Agency Sector Liaison to address problems related to critical infrastructure protection and recommend components for the National Plan for Information Systems Protection.
Sector Liaison	An individual of Assistant Secretary rank or higher designated by each Federal Lead Agency who cooperates with private sector representatives in addressing problems related to critical infrastructure protection and recommending components for the National Plan for Information Systems Protection.

Sniffers	A software or hardware tool that monitors data packets on a network to make sure messages are arriving as they should and everything else is working right.
Technology	Broadly defined, includes processes, systems, models and simulations, hardware, and software.
Threat	A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security. A threat may be an individual, an organization, or a nation.
Transportation	A critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being of this nation, including the national airspace system, airlines and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services.
Trap Door	A means of disabling a system's security, by a hardware or software mechanism which is intentionally hidden by designers of the system, often for the purpose of providing access to service technicians or maintenance programmers.
Trojan Horse	Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.
Vulnerability	A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat.
Vulnerability Assessment	Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.
Water Supply System	A critical infrastructure characterized by the sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and fire fighting.

ACRONYMS

A&I	Assurance and Integration
ABA	American Bankers Association
ACERT	Army Computer Emergency Response Team
ACTD	Advanced Concept Technology Demonstration
AFWIC	Air Force Warfare Information Center
AGA	American Gas Association
AIDE	Automated Intrusion Detection Environment
AISU	Analysis and Information Sharing Unit
ANSIR	Awareness of National Security Issues and Response System
ASD C^3I	Asst Secretary of Defense for Command, Control, Communications and Intelligence
ATM	Automated Teller Machine
B&F	Banking and Finance
BDR	Budget Data Request
BITS	Banking Industry Technology Secretariat
C^3	Command, Control and Communications
C^3I	Command, Control, Communications and Intelligence
CA	Certificate Authority
CAT	Computer-Assisted Topography
CDC	Centers for Disease Control and Prevention
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team/Coordination Center
CEST	Cyber-Emergency Support Team
CFO	Chief Financial Officer
CIA	Central Intelligence Agency
CIAC	Computer Incident Advisory Capability
CIAO	Critical Infrastructure Assurance Office
CICG	Critical Infrastructure Coordination Group
CINC	Commanders-in-Chief
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection

CIP IWG	Critical Infrastructure Protection Interagency Working Group
CIPIS	Critical Infrastructure Protection Integration Staff
CIPP	Defense Critical Infrastructure Protection Program
CIPRDI	Critical Infrastructure Protection Research and Development Initiative
CIRT	Computer Incident Response Team
CISSP	Certification for the Information Systems Security Profession
CITE	Center for Information Technology Excellence
CIWG	Critical Infrastructure Working Group
CJCS	Commander, Joint Chiefs of Staff
CNA	Computer Network Attack
CNE	Computer Network Exploitation
COMAFFOR	Commander, Air Force Forces
COMARFOR	Commander, Army Forces
COMMARFOR	Commander, Marine Forces
COMNAVFOR	Commander, Navy Forces
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CPDF	Central Personnel Data File
CRL	Certificate Revocation List
CSIRC	Computer Security Incidence Response Capability
DARPA/ITO	Defense Research Projects Agency/Information Technology Office
DASD	Deputy Assistant Secretary of Defense
DDR&E	Director, Defense Research and Evaluation
DERA	Defense Evaluation and Research Agency
DFAS	Defense Finance and Accounting Service
DHRA	Defense Human Resources Agency
DI	Defense Infrastructure
DIA	Defense Intelligence Agency
DIAP	Defense-wide Information Assurance Program
DII	Defense Information Infrastructure
DII/C^3	Defense Information Infrastructure/Command, Control, Communications
DIO	Defensive Information Operations

DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DOC	Department of Commerce
DoD	Department of Defense
DoD CIAO	Department of Defense Chief Infrastructure Assurance Officer
DoD CIAO Council	Department of Defense Chief Infrastructure Assurance Officer Council
DoD CIO	Department of Defense Chief Information Officer
DoD CIO Council	Chief Infrastructure Officer Council
DoDD	Department of Defense Directive
DoD(GC)	Department of Defense General Counsel
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
DSS	Defense Security Service
DVA	Department of Veterans Affairs
EMI	Electro-Magnetic Interference
EO	Executive Order
EOP	Executive Office of the President
EPA	Environmental Protection Agency
ECPA	Electronic Communications Privacy Act
EPRI	Electric Power Research Institute
ERT	Expert Review Team
EU	European Union
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCS	Federal Cyber Services
FedCIRC	Federal Computer Incident Response Capability
FEIT	Functional Evaluation and Integration Team

FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FIDNet	Federal Intrusion Detection Network
FIRST	Forum of Incident Response and Security Teams
FISSEA	Federal Information Systems Security Educators' Association
FOC	Full Operating Capability
FOIA	Freedom of Information Act
FRB	Federal Reserve Board
FTE	Full-Time Equivalent
FY	Fiscal Year
GAO	General Accounting Office
GII	Global Information Infrastructure
GIS	Geographic Information System
GNOSC	Global Network Operations and Security Center
GOTS	Government Off-the-Shelf
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GRI	Gas Research Institute
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
I^3P	Institute for Information Infrastructure Protection
I&C	Information and Communications
I&W	Indications and Warnings
IA	Information Assurance
IAP	Information Assurance Program
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
ICBA	Independent Community Bankers of America
ICC	Information Coordination Center
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers

IG	Inspectors General
IIWG	International Interagency Working Group
INFOSEC	Information Security
IOC	Initial Operating Capability
IP	Internet Protocol
IRM	Information Resource Management
ISAC	Information Sharing and Analysis Center
ISR	Intelligence, Surveillance and Reconnaissance
ISSO	Information Systems Security Officers
ISSS	Information Systems Security Strategy
IT	Information Technology
ITAA	Information Technology Association of America
ITMRA	Information Technology Management Reform Act
ITO	Information Technology Office
IWG	Interagency Working Group
IWGBPS	Interagency Working Group on Federal Cyber-Security Best Practices & Standards
JPO-STC	Joint Program Office-Special Technology Countermeasures
JTF-CND	Joint Task Force-Computer Network Defense
KAI	Key Asset Initiative
LAAS	Local Area Augmentation System
LEA	Law Enforcement Agencies
LES	Leading Edge Service
MISPC	Minimum Interoperability Specification for PKI Components
NASA	National Aeronautics and Space Administration
NCA	National Command Authority
NCS	National Communications Systems
NCTF-CND	Naval Communications Task Force-Computer Network Defense
NDPO	National Domestic Preparedness Office
NERC	North American Electric Reliability Council
NETS	National Education and Technology Standards
NGI	Next Generation Internet
NIAC	National Infrastructure Assurance Council

NIAP	National Information Assurance Partnership
NIETP	National INFOSEC Education and Training Program
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIPCI	National Infrastructure Protection and Computer Intrusion
NIPCIP	National Infrastructure Protection and Computer Intrusion Program
NIST	National Institute of Standards and Technology
NLETS	National Law Enforcement Telecommunications System
NMCC	National Military Command Center
NMCIAC	New Mexico Critical Infrastructure Assurance Council
NMERI	New Mexico Engineering Research Institute
NMJIN	National Military Joint Intelligence Command
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSD	National Security Directive
NS/EP	National Security/Emergency Preparedness
NSF	National Science Foundation
NSIRC	National Security Incident Response Center
NSTAC	National Security Telecommunications Advisory Council
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OASD	Office of the Assistant Secretary of Defense
OCONUS	Outside Continental United States
ODDR&E	Office of Director, Defense Research and Engineering
OMB	Office of Management and Budget
OMG	Object Management Group
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OSTP	Office of Science and Technology Policy
OUSD(P)	Office of the Under Secretary of Defense for Policy
PCAST	President’s Commission of Advisors on Science and Technology
PCCIP	President's Commission on Critical Infrastructure Protection

PDD	Presidential Decision Directive
PDIT	Program Development and Integration Team
PKI	Public Key Infrastructure
PNNI	Private Network-to-Network Interface
POC	Point-of-Contact
POTUS	President of the United States
PPBS	Planning, Programming, and Budgeting System
PSTN	Public Switched Telecommunications Network
PITAC	President's Information Technology Advisory Council
QoS	Quality of Service
R&D	Research and Development
RAL	Registered Asset List
SCADA	Secure Supervisory Control and Data Acquisition
SEC	Securities Exchange Commission
SECDEF	Secretary of Defense
SFS	Scholarship For Service
SMI	Security Management Infrastructure
SSE-CMM	System Security Engineering-Capability Maturity Model
TACON	Tactical Command
TBD	To Be Determined
TSWG	Technical Support Working Group
USACE	U.S. Army Corps of Engineers
USA DOMS	U.S. Army Director of Military Support
USDA	Department of Agriculture
USSPACECOM	U.S. Space Command
USTRANSCOM	U.S. Transportation Command
VA	Veteran's Affairs
VHS	Vital Human Services
WAAS	Wide-Area Augmentation System
WDM	Wavelength Division Multiplexing
WWU	Watch and Warning Unit
Y2K	Year 2000

INVITATION FOR PUBLIC COMMENT

This National Plan was developed to protect America's critical infrastructures. Representatives from Federal Defense and civilian Agencies, as well as private industry and state and local governments, worked together to build this Plan from the ground up.

This document is just a bundle of paper without input from our Nation's citizens who are affected by disruptions to our critical infrastructures. We invite your comments and suggestions on this National Plan.

Please feel free to contact us at:

CIAO
1800 G Street, NW
8th Floor
Washington, DC 20006
(202) 589-3200
(202) 589-3246 fax
or visit our Web site at http://www.ciao.ncr.gov