Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities

January 2001

Table of Contents

Preface

This congressionally requested report provides the status at the beginning of 2001 of Federal Government and industry programs on cyber security. Departments submitted their own input for this report.

In recent years, there has been a growing recognition that the new economy is dependent upon Information Technology (IT) networks and systems, which are vulnerable to malicious disruption. As a result, there have been Federal Government efforts to fix federal systems and work with industry to secure critical information systems.

The potential problems are even more significant than first thought. More of the American economy has become dependent upon IT systems. Those who have the skills and tools to disrupt our networks and systems have also increased, in numbers and capability. Malicious individuals, criminal groups, and nation states present significant threats to U.S. information systems.

Over the next three years, traditional telephony networks and data transmission systems are converging with the Internet into a single formatted, digital, packet-switched network. Fiber optic lines and new optical switches will create an expanding optical core for the new networks. Finally, wireless devices linked to the Internet and the new converged, fiber networks will replace a multiplicity of today's devices (cell phones, PDAs, pagers, notebook computers, and credit cards). While on-going efforts continue to increase security on the nation's current IT systems, government and industry must insure that security is designed into next generation networks.

In recognition of the growing threats and the new opportunities in the next generation National Information Infrastructure, the Federal Government has:

- Overcome the mistrust between the government and critical industry groups.
- Created effective public-private partnerships.
- Greatly increased the security of the Defense Department's networks and laid out a plan for continued improvement.
- Established information sharing and analysis centers in some key industries and some Federal Government agencies running major networks.
- Initiated a cyber security scholarship program and is working with higher education and industry to address the shortage of trained information technology personnel in the Federal Government.
- Begun establishing a baseline for standards and a system to enforce them within Federal agencies.
- Established initial requirements for a national system to identify, limit, and recover from significant information warfare attacks and malicious hacks.

- Initiated discussions with government and industry on interdependencies across sectors, the operation of the new networks, and the requirement for the converged telephony/IP system to be designed with enhanced security.

- Encouraged partnerships with industry to more sectors and continued stimulating market forces (audit, insurance, and legal) to reduce vulnerabilities in privately owned and operated critical infrastructures.

Additional accomplishments are enumerated in the report.

Achievements to date are notable, but there is still work to do. At present, there is no government-wide means for identifying critical systems and their vulnerabilities and then fixing them. Nor is there a government-wide means of tracking the progress of departments in achieving specified goals. The General Accounting Office of Congress has provided a useful review of cyber security of the departments, but has been able to examine only a few agencies annually.

The IT Revolution of the last eight years has transformed our nation for the better. Economic growth, better government service and efficiency, and a stronger defense are all possible in the years ahead if we continue to give high priority to securing cyber space.

I. OVERVIEW

I. OVERVIEW

Introduction

This report is submitted pursuant to the requirement in Presidential Decision Directive 63 (PDD-63) for the National Coordinator to provide an annual report on the implementation of PDD-63 to the President and heads of departments and agencies.

The first part of this introductory section briefly discusses the types of threats posed by the evolution of Information Technology (IT) and related trends. The second part provides an overview of PDD-63 and the government structures created to implement it. The last part sets forth a roadmap for the rest of the report.

The Problem and Challenges

Dependency, Vulnerability, and Threat

During the past decade, our increasing use of automated systems and devices has stimulated unprecedented prosperity. At the same time, the maturing of the Information Age has also led to new types of threats and vulnerabilities.

America's critical infrastructures are the foundation of our economy, national security, and quality of life. The functioning of critical parts of our economy, government, and national security now depend upon computer-managed information networks. Our infrastructures increasingly rely on interconnected information systems and networks. This development creates a new dimension of vulnerability which, when combined with an emerging array of threats, poses a new set of risks to the nation's security and economic power. Potential adversaries—be they nation-states, cyber-terrorist groups, criminal organizations, or disgruntled insiders—can easily develop effective cyber-attack capabilities to exploit this vulnerability.

Currently available hacker exploits permit an attacker to conceal points of origin by hopping through several intermediate way stations in cyber space—crossing and re-crossing national borders in the process. These capabilities make identification of an attacker a daunting challenge. Established terrorist groups are likely to view attacks against information systems and critical infrastructures as an attractive way to strike at government, commercial, and industrial targets with little risk of detection.

In short, unlike the familiar national-security threats of the past century, these cyber threats can come from anywhere. They can originate from any location, affect systems anywhere in the world, disguise their origins and travel routes, and do it all instantaneously. Without firing a shot or crossing a border, an enemy with the right tools and techniques can damage our economy and slow down our military.

The Need for Effective Public-Private Partnerships

Unlike other forms of national security threats, the Federal Government cannot address these threats to critical infrastructures in isolation. Most of our critical infrastructures are privately owned and operated. Many of the owners and operators are business competitors. The protection of our critical

infrastructures, therefore, necessarily requires a shared responsibility and partnership between owners and operators and the government.

Effective critical infrastructure protection (CIP), and in particular the provision of adequate cyber-security, really requires a comprehensive system approach that consists of business processes, cultures, and policies, as well as access to appropriate technical tools and trained personnel.

Failures of infrastructure and cyber-security can directly harm business operations by affecting their bottom lines, eroding consumer confidence, and disrupting operations. Serious problems can lead to major disruptions throughout the economy.

Furthermore, infrastructure protection by its nature cannot be static. In today's high-speed business world, core business processes and technology are constantly changing in order to create competitive advantages and efficiency. It is not always clear which drives which. The pace of change is measured in months rather than years. Consequently, assuring the safety of the information systems that underlie our critical infrastructures will mean integrating an on-going concern for security into the business decisions of managers as well as technologists. That process will have to start at the highest levels of management.

Presidential Decision Directive 63

On May 22, 1998, President Clinton issued PDD-63 to achieve and maintain the capability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

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

To achieve these ends, the PDD-63 articulates a strategy of:

- creating a public-private partnership to address the problem of information technology security;
- raising awareness of the importance of cyber security in the government and in the private sector;
- stimulating market forces to increase the demand for cyber security and to create standards or best practices;
- funding or facilitating research into new information technology systems with improved security inherent in their design;
- working with higher educational facilities to increase the number of students specializing in cyber security;
- helping to prevent, mitigate, or respond to major cyber attacks by building an information sharing system among government agencies, among corporations, and between Government and industry.

The government's basic approach to CIP, as reflected in PDD-63, has been built around a strong policy preference for consensus-building and voluntary cooperation rather, than regulatory actions. In an economy as complex as ours, and with technology changing as quickly as it is, cooperation offers the best and surest way to achieve our shared goals in this emerging area. However, the government's approach also recognizes the need for coordinated actions to improve its internal defenses and the nation's overall posture against these new threats.

For this reason, implementation of PDD-63 has proceeded along two simultaneous policy tracks:

- To establish an effective system of partnership arrangements with the private industry within each infrastructure sector, across all the infrastructure sectors, and with other key stakeholders, including the audit, insurance and investment communities, to raise awareness and to catalyze market driven activities and solutions.

- To improve the government's own systems and plans for critical infrastructure assurance, including the development of internal plans, improved recruitment, education and training for Federal personnel, and a comprehensive program of research and development in these areas.

PDD-63 addresses the unique structural challenges that CIP poses for the Federal Government.

> "No office, organization or individual within the Federal Government has overall responsibility for infrastructure protection or policy. This is not surprising as there was little need for a national focal point when infrastructures were largely independent discrete, insulated by geography and protected by military defenses. Today, however, the interdependent, interconnected nature of the infrastructures, and their exposure to cyber and other threats, creates a real need for a single point of focus. To support this, a federal framework needs to be created, working in conjunction with state and local governments and the private sector, to implement a national policy on infrastructure protection.[1]"

To meet these challenges, PDD-63 has created new organizational structures to compliment those already in place:

- The **National Coordinator for Security, Critical Infrastructure and Counter-Terrorism** at the White House National Security Council (NSC) staff. The National Coordinator serves as a spokesperson for the issue of cyber security and provides oversight for the implementation of PDD-63 and the National Plan.

- The **Critical Infrastructure Assurance Office (CIAO)**, an interagency office housed at the Commerce Department, assists in the coordination of the Federal Government's initiatives on critical infrastructure protection. It has three basic missions. First, it coordinates the drafting of the National Plan for Information Security Protection. Version 1.0 of the plan was issued by President Clinton in January 2000. Second, it assists Federal agencies in analyzing their critical infrastructure dependencies and interdependencies. CIAO has initiated Project Matrix whereby it is helping civilian agencies to identify those assets that are key to the fulfillment of their national security, economic stability, and critical public health and safety responsibilities. Finally, it coordinates national outreach, education and awareness efforts. The CIAO has been the catalyst in the creation by private-sector companies of the Partnership for Critical Infrastructure Security. In implementing its mandates, the CIAO is focusing on issues that cut across industry sectors (and are not the existing responsibility of agencies). In this way, it helps to ensure a coherent and cohesive U.S. approach to the protection of our critical infrastructures.

[1] "Critical Foundations –Protecting America's Infrastructures;" The Report of the President's Commission on Critical Infrastructure Protection, page 50.

- The **National Infrastructure Protection Center (NIPC)**, an interagency office housed at the Federal Bureau of Investigation (FBI), serves as a threat coordination center focusing on threat warnings, vulnerabilities, and law enforcement. The Center is staffed by a mix of FBI employees and detailees from other Federal agencies. In addition, the Center has had state law enforcement officials detailed on a rotating basis and hosts representatives from the United Kingdom and Canada. The center has a vital role in collecting and disseminating information from all relevant sources. The NIPC sanitizes law enforcement for inclusion into analyses and reports that it provides, in appropriate form, to relevant federal, state, and local agencies, owners and operators of critical infrastructures, private sector information sharing and analysis entities, and to the public. The NIPC also issues attack warnings or alerts to increases in threat condition to private sector owners and operators. In the first ten weeks of FY 2001 the NIPC has issued eight warnings. Each of the 56 FBI field offices has agents assigned to infrastructure protection matters, to include investigating computer intrusions, denials of service, and virus cases; performing outreach initiatives; creating computer crime task forces with state and local law enforcement; training for computer crime investigators; developing an intelligence base; and supporting significant FBI cases that require computer investigative expertise.

- 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
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 for the Cabinet-level Principals Committee.

- The **Critical Infrastructure Coordination Group** is the primary interagency coordination body for the implementation of PDD-63. CICG membership is comprised of senior policy level (Assistant Secretary or higher) officials and includes the Sector Liaisons, Functional Coordinators of the Lead Agencies, as well as representatives from other relevant Departments and Agencies, including the National Economic Council. The National Coordinator chairs the CICG. Where appropriate, the CICG is assisted by existing policy structures.

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

- The **Cyber Incident Steering Group (CISG) and Cyber Incident Working Group (CIWG)** are both sub-groups of the CICG that convene to coordinate policy and operational issues in the event that extensive cyber-related disruptions to critical systems occur. The CISG is chaired by the National Coordinator and provides policy guidance to the CIWG and recommendations to the NSC Principals. The CIWG, chaired by the Director of the NIPC, coordinates operational and law enforcement matters among the Federal Agencies during a cyber event. The work of these two bodies does not derogate existing agency authorities for law enforcement, intelligence, or national defense and ensures proper interagency coordination.

- The **Chief Information Officers Council (CIO Council),** comprised of Federal CIOs, works to protect the privacy and availability of the data on Federal information systems. Its **Subcommittee on Security, Privacy, and Critical Infrastructure** ensures implementation of security practices within the Federal Government in order to prevent interruption of government services, maintain privacy, and protect sensitive and national security classified information. Through these efforts, senior executives within the government are kept abreast of developing information security issues and exchange information on techniques for dealing with IT security risks.

- The **Joint Telecommunications Resources Board (JTRB)** assists the Director of the Office of Science and Technology Policy (OSTP) in the Executive Office of the President in the exercise of authorities over the National Communications System (NCS) in non-wartime emergency situations. The National Communications Center (NCC), a component of the NCS, is comprised of private sector companies and supported by OSTP and the JTRB. It is a key element of the Federal telecommunications infrastructure and represents a strong model of public-private partnerships.

- The **National Security Telecommunications and Information Systems Security Committee (NSTISSC)** was established in 1990 to provide a forum for the discussion of policy issues and to provide operational guidance for the protection of national security systems. Its members include a broad range of civilian and military agencies.

- The **National Information Assurance Partnership (NIAP)**[SM] is a U.S. Government initiative designed to meet the security-testing needs of both information technology producers and users. NIAP is a collaboration of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The partnership combines the extensive IT security experience of both agencies. The program is intended to foster the availability of objective measures and test methods for evaluating the quality of IT security products. In addition, it is designed to foster the development of commercial testing laboratories that can provide the types of testing and evaluation services, which will meet the demands of both producers and users.

- The **Federal Computer Incident Response Capability (FedCIRC)** is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense, law enforcement, the Intelligence Community, academia and computer security specialists from Federal civilian agencies and departments, forming a multi-talented virtual security team.

- The **Federal Cyber Services (FCS**) training and education initiative is an element of the National Plan and is designed to ensure an adequate supply of highly skilled Federal information system security specialists. The "Scholarship for Service" program, a component of FCS, was recently funded for FY 2001. The National Science Foundation and the Office of Personnel Management administer the program jointly. The program offers scholarships for up to two years in exchange for a commitment to an equal amount of service to the Federal Government.

A Roadmap to the Report

The remainder of the Report is organized as follows:

- *Section 2* reports on the government's efforts to foster effective public-private partnerships, beginning with a discussion of the sector-level programs sponsored by Federal lead agencies and concluding with a review of cross-sector partnership efforts, that include national education and awareness partnerships implemented by the CIAO and law enforcement information sharing/indications and warning partnerships implemented by the NIPC.

- *Section 3* reports on internal efforts within the Federal government to secure our internal systems and infrastructures. The section begins with a review of the programs at Cabinet-level departments (listed in alphabetical order). Later sub-sections review similar programs at Federal agencies and the government's overall efforts to promote CIP best practices and standards.

- *Section 4* reports on CIP education and training initiatives. These initiatives have several purposes: to increase the supply of trained IT security staff within Federal agencies, build academic programs in the fields of cyber-security and infrastructure protection, and increase awareness among educators and students of the need for good cyber-security practices.

- *Section 5* reviews CIP research and development programs. These programs are discussed on a sector-by-sector basis.

- *Section 6* contains progress reports independently prepared and voluntarily submitted for inclusion in this document by several private industry sectors and partnerships. We have offered private industry the opportunity to provide its own perspective on the state of CIP and related issues. These reports have been included as received from the respective industry sectors and partnerships and reflect their independent views.

II. STATUS OF PUBLIC-PRIVATE PARTNERSHIP BUILDING EFFORT

II. STATUS OF PUBLIC-PRIVATE PARTNERSHIP BUILDING EFFORT

A. Introduction

Section IV of PDD-63 dealt with creation of a public-private partnership to reduce vulnerabilities of the nation's major critical infrastructures subject to attack. It stated that for each of the major sectors of our economy, the Federal Government would appoint from a designated Lead Agency, a Sector Liaison official to work with the private sector to contribute to a sectoral National Infrastructure Assurance Plan. The National Coordinator would ensure overall coordination and integration of the sector plans, with a particular focus on interdependencies.

This section contains two parts. The first consists of reports from each of the designated Federal Lead Agencies on their activities to establish and support partnerships with their industry sectors. Several industry sectors and partnerships have also opted to provide interim status reports on sector achievements and activities, to complement the reports of their counterparts in the Federal Lead Agencies. The industry reports are included in Part VI of this report.

Secondly, this section will provide reports from the CIAO and the NIPC that describe implementation of cross-sector partnerships to perform responsibilities assigned to them by PDD-63.

Over the last year and a half, Federal Lead Agencies, the CIAO, and the NIPC have taken major steps towards mobilizing the infrastructure industries and the business community as a whole. These initiatives are garnering self-sustaining industry actions, as well as laying a foundation for future cooperative initiatives. Partnering efforts fall under two major categories: sector partnerships and cross-sector partnerships that support the individual sector efforts:

- Industry Sector/Federal Lead Agency Partnerships, supporting specific infrastructure industries:
  - Convening and helping industry sectors to organize themselves and plan;
  - Supporting sector unique initiatives related to information sharing, risk assessment and approaches, research and development, and legal and policy issue identification;
  - Supporting and expanding industry outreach and awareness.

- Cross-Sector Partnerships:
  - National Outreach and Awareness Partnerships, implemented by the CIAO, providing cross-industry forums, building business cases for action, encouraging mutual support and action, and facilitating emergence of market forces,
  - Law Enforcement Information Sharing/Indications and Warning Partnerships, implemented by the NIPC.

B. Sector Partnerships

The following describes the activities of each Federal Lead Agency to engage and support their industry sector on CIP initiatives. Reports of their progress on internal agency CIP activities are provided in Part III of this report.

1. Banking And Finance

Sector Lead Agency: Treasury Department

Partnership Role of Department of the Treasury

PDD-63 assigned Treasury "lead agency" responsibility for working with the banking and finance sector of the economy, a responsibility managed by Treasury's Office of Financial Institutions Policy. The Treasury Department's Assistant Secretary for Financial Institutions serves as Sector Liaison. After consultation with the industry, Treasury named the Chief Information Security Officer of Citigroup as the industry's Sector Coordinator.

The Department's contributions to developing and supporting a partnership with the banking and finance sector included:

- Convening and helping industry representatives to organize themselves and plan;
- Supporting sector unique initiatives with workshops and access to industry studies;
- Coordinating and helping to maintain focus for working group initiatives;
- Supporting and expanding industry outreach and awareness; and
- Providing Secretariat support for industry working groups, whose members work on a voluntary basis in addition to their normal workloads in private industry.

Together, Treasury and the industry are responsible for carrying out a number of tasks, including:

- Assessing the vulnerabilities of the sector to cyber and physical attacks;
- Recommending a plan to eliminate significant vulnerabilities;
- Developing an information sharing system for identifying and preventing major attacks;
- Proposing an agenda of research and development for information systems security;
- Developing an education and outreach program to increase awareness of industry infrastructure security risks; and
- Providing content for the industry's contribution to the *National Plan for Information Systems Protection (National Plan).*

Partnership Development and Support

Private Sector Outreach: As a first step toward the private sector outreach mandated by PDD-63, former Secretary Robert Rubin convened a Treasury information security conference on October 7, 1998. Attendees included a large number of industry information security officers and representatives of the financial regulatory agencies and others with a direct interest in CIP. Industry representatives at the conference readily agreed that the goals of PDD-63 were worth pursuing, and agreed to create and support what is now known as the Banking and Finance Sector Coordinating Committee on Critical Infrastructure Protection. The industry representatives also established working groups to address the issue areas they considered to be of highest priority.

Facilitate and Support Industry Meetings: With support from Treasury, the second meeting of the Coordinating Committee was held on March 11, 1999. It was a "nuts-and-bolts" type of meeting that established specific agendas for each of the working groups going forward. At that meeting, it was also decided that the creation of an industry information sharing and analysis center (ISAC) was especially important, largely because of impending Y2K concerns among government and industry leaders, and other signs of an increase in cyber threats. The third meeting, held on April 10, 2000, focused on assessing the vulnerability of the financial services sector to attack and on research and development priorities.

Support Working Group Activities: Each of the working groups is at a different stage in their activities. The R&D Working Group is consulting government, academic, and industry experts to develop priorities for government and private sector-funded research. The Vulnerability Assessment Working Group is reviewing a vulnerability analysis prepared for the President's Commission on Critical Infrastructure Protection (PCCIP) in 1997 and working on a plan for a follow-up vulnerability assessment of its own. The Outreach Working Group has worked with the national CIAO at the Commerce Department to help raise awareness of these issues, and is working on a plan for industry education and outreach. The recently established National Plan Steering Committee is drafting the sector's preliminary infrastructure assurance plan and coordinating with the PCIS.

The Financial Services Information Sharing and Analysis Center (FS/ISAC): The financial services industry was the first to respond to PDD-63's call for the establishment of an ISAC. After an arduous period of technical, legal, and organizational negotiations, approximately a dozen major financial services firms and industry utilities established the Financial Services Information Sharing and Analysis Center – the FS/ISAC.

Vulnerability Assessment and R&D: Sponsored by Treasury, with support from the national CIAO, a workshop was held April 10, 2000 for representatives from the sector to help provide a foundation for further action on sector vulnerability assessment and R&D. The agenda consisted of presentations by private industry, government, and academia on vulnerability assessment methodologies and approaches, and perspectives on an R&D agenda for the banking and finance sector. The subsequent discussions generated recommendations for each of the working groups to address as next steps.

Drafting The National Plan: For the immediate future, the banking and finance sector will focus almost exclusively on drafting its contribution to the *National Plan, Version 2.0*. Industry representatives have agreed that topics to be addressed in the sector plan will most probably include information sharing, vulnerability assessment/interdependencies, research and development requirements, education and awareness, sector defense against an attack (continuation of business), reconstitution (how to rebuild after an attack), and legal issues.

The sector's activities and achievements to date are described more fully in a combined industry/Treasury Department report provided in Part VI of this report.

2. Energy

Sector Lead Agency: Department Of Energy (DOE)

Partnership Role of DOE

The Department of Energy has a mandate to help ensure the reliability and security of the Nation's energy infrastructure. In light of this responsibility, as well as the related challenges posed by the new economy, DOE created the Office of Critical Infrastructure Protection (OCIP) in accordance with PDD-63 to focus solely on the infrastructure assurance needs of the energy industry. This office has the responsibility for building the partnerships with the electric power and oil and gas sectors to protect their infrastructures. This mission encompasses the physical and cyber components of the electric power, oil, and gas infrastructures, the interdependencies among those components, and the interdependencies with the other critical national infrastructures.

Outreach And Awareness Programs

As called for in PDD–63, the Office is working with industry in a genuine, mutual, and cooperative partnership to address CIP challenges. Vulnerability awareness and educational programs, for example, provide energy industry stakeholders with relevant information. As part of its outreach efforts, the Office also has undertaken a number of specific PDD–63 tasks in collaboration with the energy industry, including:

- Assessing how the energy sector is vulnerable to cyber or physical disruptions;
- Identifying ways to mitigate vulnerabilities;
- Developing ways to alert, contain, and divert attacks;
- Planning a system for responding to energy sector attacks; and
- Identifying ways to facilitate rapid restoration.

To accomplish these goals, OCIP plans and conducts outreach to energy industry stakeholders, including the development of information exchange modalities and mechanisms and vulnerability awareness and education programs.

Sector Coordinator Support

The Department, through the OCIP, is working closely with industry Sector Coordinators [i.e., the North American Electric Reliability Council (NERC) and the National Petroleum Council (NPC)] to develop a national energy CIP strategy. OCIP, along with the CIAO, has helped NERC develop a CIP "business case" for industry CEOs, presented a cyber security tutorial to the NERC Board of Trustees, and worked with NERC and the National Infrastructure Protection Center (NIPC) at the FBI to develop indications and warning criteria for electric power operators to use to report threats and incidents to NIPC. OCIP is also assisting NERC's new CIP Working Group, which will be addressing how to establish information sharing mechanisms. The NERC has provided a report of its activities and achievements to date, which is contained in Part VI of this report.

For the gas and oil industry, the OCIP Director is co-chair of a CIP subcommittee charged with drafting a CIP strategy for the industry. Through OCIP, the Department is providing technical assistance, briefings, and workshops to the NPC to help address issues such as threats and vulnerabilities, information sharing, incident response and recovery, and appropriate government research and development.

Regional Pilot Programs

OCIP, the City of Chicago, the regional Mayor's Caucus, and Commonwealth Edison have created the first-of-its-kind cooperative program to develop a regional energy emergency preparedness capability focused on local critical services and assets. The effort is an outgrowth of the Midwest power outages in the summer of 1999.

OCIP is also working with the 2002 Salt Lake City Winter Olympics Infrastructure Assurance Planning Subcommittee to develop a regional CIP plan. To this end, OCIP facilitated the "Black Ice" regional critical infrastructure interdependencies exercise in Salt Lake City, Utah, in the autumn of 2000. Two hundred twenty-five representatives from 65 regional infrastructure entities, Federal Government, regional governmental offices and agencies, public works, and law enforcement agencies participated in the exercise, which was a joint effort of the Utah Olympics Safety Committee (Infrastructure Protection Subcommittee) and DOE. OCIP is providing assistance to the infrastructure protection subcommittee members to use the results of the exercise to enhance regional emergency response and recovery efforts.

Research and Development

OCIP is also engaged in a multi-year research and development program to develop cost-effective technologies and capabilities (e.g., databases, methodologies, tools) that can be used to achieve several goals and contribute to industry's capability to protect itself:

- Increase our understanding of physical and cyber disruptions (natural, accidental, deliberate) to the energy infrastructure that could result in cascading or widespread regional outages;
- Develop energy infrastructure assurance "best practices" through vulnerability and risk assessments; and
- Protect against, mitigate the impacts of, and improve the ability to recover from disruptive incidents within the energy infrastructure.

The R&D initiatives focus on analysis and risk management and protection and mitigation technologies.

Identification and Mitigation of Vulnerabilities

Critical energy infrastructures are complex and highly integrated. They rely on a broad range of enterprises that work in harmony to deliver energy services necessary for the functioning of our economy and society. The challenge of protecting the systems and assets that provide energy is vested in these enterprises. Engaging these enterprises is therefore essential to reducing vulnerabilities, reducing potential impacts of service interruptions, and rapid restoration of vital energy services. DOE's OCIP, through its Infrastructure Assurance Outreach Program (IAOP), works with private sector entities to assess infrastructure vulnerabilities. The goal of the program is to enable industry to achieve a more secure operating condition by providing the means for self-help.

Through the vulnerability assessment efforts of the IAOP, the Department of Energy is:

- Engaging the energy industry in developing and implementing collaborative strategies for enhancing infrastructure assurance;
- Enabling comprehensive and confidential assessment of vulnerabilities;

- Providing assistance to industry in reducing vulnerabilities;
- Facilitating cooperative analysis of the nation's energy infrastructure vulnerability;
- Developing trust between the public and private sectors;
- Developing a "best practices" vulnerability assessment methodology; and
- Meeting the mandates of PDD–63.

While private sector firms should conduct comprehensive vulnerability assessments, many lack the awareness, resources, or experience to do so. The IAOP works with utilities to identify and evaluate the threats to and vulnerabilities of their electric, natural gas, and oil infrastructures. These efforts encompass both physical and cyber infrastructure components. The IAOP is leveraging the assessments and follow-on analyses to develop generic lessons learned and recommended practices for the energy industry.

The data, products, and analyses that are produced during an assessment are the property of the company and remain confidential. The IAOP intends to share lessons learned and is developing and refining an assessment methodology in cooperation with these companies. The IAOP is a collaborative effort: the knowledge and experience gained from the program will enable the private sector to conduct effective self-assessments in the future.

Helping Energy Stakeholders Understand Infrastructure Interdependencies

The nation's energy infrastructures are becoming increasingly complex, physically interconnected, and interdependent. These dependencies are both internal (e.g., among the electric power, natural gas, and oil infrastructures) and with other critical infrastructures (e.g., with the telecommunications, transportation, and water infrastructures). For example, natural gas may fuel critical gas-fired generators in the electric power system, while at the same time electricity may be used to operate critical systems needed for gas delivery. Similarly, an electric substation in an electrical distribution system may provide electric power to a key telecommunications switching center. Under certain system conditions, failure or loss of power in the substation would directly affect the telecommunications center's ability to operate. The telecommunications center in turn may support the Supervisory Control and Data Acquisition (SCADA) systems for gas and oil pipelines, electric power, water and transportation systems, which support the electric power infrastructure.

The Energy Infrastructure Interdependencies Program (EIIP) is aimed at identifying and understanding such interdependencies, both among the energy infrastructures and with other critical national infrastructures. This capability will help DOE and others within the energy sector assess the technical, economic, and national security implications of energy infrastructure development and policy decisions designed to ensure reliability and security of the nation's energy systems. There is not yet a clear understanding of the nation's vulnerabilities to infrastructure interdependencies and disruptions but, through the EIIP, DOE is trying to gain such insights into the energy sector.

Workshops and Exercises

DOE has sponsored industry-government workshops to address broad CIP needs and specific concerns such as intrusion detection technologies. A workshop on infrastructure interdependencies R&D was held in June 2000. Another workshop focusing on water systems vulnerabilities was jointly sponsored with the Environmental Protection Agency in August 2000.

Other Collaborative Activities

OCIP also performs the following CIP-related functions:

- Identifies and develops mechanisms to transfer technologies and capabilities to industry;
- Leads and coordinates efforts within the Department to expand cooperation on energy infrastructure protection with friendly nations, international organizations, and multinational corporations;
- Evaluates and recommends ways to address legal and related issues associated with CIP for the energy sector; and
- Assesses, in collaboration with industry, the potential benefits of standards and "best practices" for the energy infrastructure.

3. Information and Communications (I&C)

Sector Lead Agency: Department of Commerce/NTIA

Partnership Role of NTIA

The National Telecommunications and Information Administration (NTIA), principal advisor to the President on telecommunications and information policy, was designated to serve as the lead agency to protect the U.S. information and communications (I&C) infrastructure from cyber and physical attack. NTIA's role as lead agency for the I&C sector is to work closely with industry, which owns and operates these key infrastructures, cooperating as partners and building upon existing relationships with the business community to increase security.

NTIA works closely with the Sector Coordinators for the I&C Sectors: the Information Technology Association of America (ITAA), the Telecommunications Industries Association (TIA), and the United States Telecom Association (USTA). In addition, NTIA works directly with key telecommunications and information technology companies and with other organizations, such as the President's National Security Telecommunications Advisory Committee (NSTAC). NTIA's CIP responsibilities include:

- Developing an awareness and education outreach program for the sector to raise awareness of the threat and sectoral vulnerabilities;
- Assisting the I&C sector in identifying, mitigating, and eliminating vulnerabilities;
- Facilitating establishment and operation of I&C ISACs;
- Advancing compatible solutions for the global I&C infrastructure by working with foreign governments, international organizations, and multinational corporations; and
- Providing industry with information on results from U.S. Government R&D on CIP.

Public-Private Partnership Development and Support

The Communications & Information Sector Working Group (CISWG) includes Internet companies and companies dealing with wireless technologies as well as telecommunications and IT industries. The CISWG has five very active industry-government subcommittees, which meet regularly:

- National Plan Drafting**:** The committee is playing a supportive role in regard to the drafting of industry's National Plan for the I&C sector. The first draft of the I&C sector National Plan will

be reviewed by NTIA's Sector Coordinators. The committee submitted a progress report to the PCIS and the national CIAO in November 2000, and the final I&C Sector CIP National Plan will be submitted in February 2001.

- NSTAC input: NSTAC will provide input to the *National Plan* directly to the National Security Council (NSC). In developing its input, the NSTAC's Industry Executive Subcommittee (IES) will invite I&C sector members to participate in its deliberative process. After the IES completes its product, it will be shared with the I&C sector.

- CIP Practices: The committee's mission is to further the development and exchange of information regarding useful CIP practices in the I&C sector and make those practices available to other sectors. The committee prepared a formal recommendation on CIP practices for inclusion in the *National Plan*, calling for the establishment of a web portal, which would provide users with access to existing resources for CIP practices. The site would also include a "street smart" guide for users on how to address CIP practices, a suggested methodology for analyzing CIP practices, and a comment capability where users can share their experiences with the resource links provided by the portal. The committee proposed that funding and maintenance of the site be done by one of the three I&C sector coordinators.

- Self-Assessment: This committee's mission is to provide a means by which the I & C sector can assess the usefulness of CIP assessment methodologies and tools. The committee's objectives include: to define an attribute set of vulnerability assessment methodologies and tools for effective CIP assessment within the I&C sector; to validate that set with industry, government, and trade associations; to provide the attribute set to the I&C sector; and to provide input to the *National Plan* process. The group successfully completed its work and presented an attribute set of vulnerability assessment methodologies and tools for inclusion in the *National Plan*.

- R&D: The committee was established to further the development and exchange of information between the Federal Government and private sector regarding I&C CIP R&D programs, thereby facilitating coordination of Federal R&D efforts and potential collaborative efforts. The committee's objectives include:
  - Providing a forum to identify and address issues relative to the ongoing and planned Federal I&C CIP R&D agenda, policy, and program;
  - Monitoring and coordinating both ongoing and planned Federal CIP R&D efforts relative to the I&C infrastructure and vulnerabilities;
  - Facilitating collaborative I&C CIP R&D programs between the Federal Government and the private sector; and
  - Annually reviewing and commenting upon the various committee working documents.

- International Outreach: This committee addressed a number of international outreach issues, which had an impact on subsequent international CIP policy developments. Subcommittee members identified key CIP industry issues for discussion at a U.S.-Canada Bilateral Meeting in Ottawa on September 20, 2000; at a U.S.-U.K. Bilateral Meeting on October 2, 2000 in London; and at a U.S.-Australia Bilateral on October 11, 2000 in Washington. They developed a recommendation that private companies participate in future CIP bilateral discussions, which was endorsed at the Canadian, U.K., and Australian bilaterals, with the hope of including industry in the next round of talks that take place. The committee also recommended that the U.S. Government begin to discuss CIP issues in multilateral fora, such as the Organization for

Economic Cooperation and Development, Asia Pacific Economic Council, and the European Union, with close private sector collaboration. Subsequently, CIP issues have been discussed in all three fora. The co-chair for the International Outreach Subcommittee also serves as the chairman of the NSTAC's Industry Executive Sub-Committee, which is responsible for developing NSTAC input for the *National Plan*. I&C sector member participation will facilitate consideration of international goals and objectives identified by the International Outreach Subcommittee in the NSTAC's input to the *National Plan*.

City/State CIP Preparedness Case Study

NTIA and the Department of Defense are partnering on a CIP project to jointly conduct a vulnerability assessment of critical infrastructures involving military bases and cities/towns (e.g., Denver, Boulder and/or Colorado Springs) in the Rocky Mountain Corridor. The vulnerability assessment project, which began in September 2000, focuses on protection of the I&C, energy, transportation, and water infrastructures. The project, scheduled to be completed in April 2001, will culminate in a written case study of a region that has identified CIP vulnerabilities and addressed remediation needs. This case study will be made available to other cities, counties and interested parties.

Supporting National Awareness and Outreach by I&C Community

Working with the CISWG, NTIA is participating in national cross-sectoral outreach with the I&C sector, supporting and participating in meetings on CIP issues across the country to increase awareness of CIP issues, and promoting availability of helpful information and resources. The agency's major outreach effort for FY 2000 was the Telecommunications and Information Security Workshop, held in Tulsa, Oklahoma, at the end of September 2000. NTIA co-sponsored this workshop with the University of Tulsa, the National Institute for Standards and Technology (NIST), and the National Security Agency (NSA). The purpose of the workshop was to identify the security issues and solutions emerging as information networks are integrated into the existing telecommunications networks to support both telephony and data services. In addition to the technical issues related to convergence, the workshop focused on current CIP policy issues affecting the I&C sector. NTIA organized five panels of senior level government and industry speakers from across the United States and Europe to address key emerging policy and security issues.

International CIP Partnership Support Activities

NTIA has worked closely with the Department of State and other Federal Agencies in bilateral CIP discussions with close U.S. allies to achieve compatible international security policies. As a first step, NTIA provided text for the State Department's blueprint for international CIP activities, which reflected the I&C sector's perspective on appropriate international CIP issues. NTIA has used the International Outreach CISWG Sub-Committee to identify principal CIP-related issues of concern to the I&C sector as input for development of a U.S. agenda for international discussion, and continues to be involved as part of the U.S. delegation engaged in bilateral and multilateral discussions.

Industry/U.S. Government R&D Information Sharing

NTIA has produced a number of reports on U.S. Government R&D related to CIP that are shared with industry. U.S. Government studies include a list of CIP R&D activities identified by agency for FY 2001, with a summary of agency initiatives, and a table identifying U.S. Government CIP vulnerabilities

and the ongoing/planned R&D programs addressing them. NTIA will develop a plan to publish and disseminate information on U.S. Government R&D involving CIP in a variety of fora. With the provision of information regarding U.S. Government R&D efforts underway, the private sector will be better able to identify and focus their efforts and resources on additional CIP projects that are non-duplicative.

Also of note, NTIA and the NIST have established a coordination mechanism to ensure that their R&D efforts are not redundant and, as far as possible, are complementary. NIST is charged with protecting the nation's critical infrastructures by developing standards, measurements, and testing methodologies needed to protect information technology. The coordination effort will be cognizant of CIP activities in other parts of the Department of Commerce and throughout the Federal Government.

Leveraging Existing Department of Commerce/Federal Programs and Resources for the Partnership

Working with the CISWG and the Department of Commerce ((DOC) Electronic Commerce Sub-Committee, NTIA has been integrating CIP issues in the Commerce Department, Department of Agriculture (USDA), and Small Business Administration (SBA) e-commerce outreach programs. NTIA has also begun to integrate CIP issues into NIST/MEP training program materials, seminars, and workshops. In addition, NTIA is integrating CIP issues into IT/e-commerce outreach and Market Development Program, and has prepared a presentation on CIP issues, which will be disseminated through DOC, USDA, and SBA domestic field offices, and through NTIA's international Commercial Service offices.

Some Current CIP Activities of Partners

While working with the three I&C sector coordinators and numerous key companies in the sector, NTIA also coordinates with other Federal Agencies (e.g., the Departments of Defense and Energy), and with other organizations such as the NSTAC. Some CIP activities undertaken by these partner organizations include:

- Information Technology ISAC: In January 2001, Secretary Norman Mineta joined by executives of 19 companies from the Information Technology (IT) industry announced the creation of the Information Technology (IT) Information Sharing and Analysis Center (ISAC). The announcement fulfilled an industry pledge made at the February 14, 2000, White House meeting with President Clinton hosted by ITAA with a group of leading IT companies and organizations and top Administration officials. The meeting took place to discuss Internet and information security issues in light of the denial of service attacks that occurred early in 2000. The ISAC will share information regarding threats, incidents, vulnerabilities, countermeasures and other solutions, and best security practices.

- Workshops and Conferences: The I&C sector coordinators have sponsored a number of workshops and conferences to raise CIP awareness. For example, the Global INFOSEC Summit, which took place in October 2000, was sponsored by the World Information Technology and Services Alliance (WITSA) and the ITAA, which gathered industry and government leaders from around the globe to discuss the critical issues of information security and infrastructure assurance. The organizers believe this event helped launch a global partnership for addressing INFOSEC issues on an on-going basis.

- National Coordinating Center for Telecommunications (NCC): This industry/Government coordination center, which began as a recommendation of the NSTAC, provides day-to-day operational support for national security and emergency preparedness of the nation's telecommunications systems. A year ago, the NCC established ISAC function under its national security and emergency preparedness telecommunications mission.

4. Transportation (DOT)

Sector Lead Agency: Department of Transportation

Partnership Role Of Department Of Transportation

PDD-63 established the Department of Transportation (DOT) as the lead Federal Agency for protecting the transportation sector from information-based and unconventional threats. PDD-63 requires DOT to identify a private sector coordinator. As DOT worked to identify a coordinator, the Department has tentatively identified the following components of the transportation infrastructure as critical:

- Civil Aviation, particularly the National Airspace Systems;
- The nation's rail system, focused on command, control and communication systems;
- The nation's pipeline transmission systems;
- The nation's ports and waterways, including the St. Lawrence Seaway;
- Defense mobilization critical transportation links, including rail, highway, and ports; and
- Global Positioning System (GPS).

DOT's role in CIP is to facilitate and coordinate activities of the private sector owners and operators of the nation's transportation infrastructure, as well as protect critical infrastructure owned and operated by the Department.

Transportation Sector Outreach

DOT's strategy is to focus initially on the rail industry, establishing close links with the rail sector, building as it needs to with other segments of the transportation sector.

The Association of American Railroads (AAR) recently agreed to accept the Sector Coordinator role for the rail segment of the transportation infrastructure starting with the railroads and potentially taking on the additional role of Sector Coordinator for surface transportation.

The AAR is planning a workshop in February 2001, which will bring together the major railroads to discuss industry participation and develop a CIP plan. Their first priorities will be to address approaches to risk assessment and information sharing.

5. Water Supply

Sector Lead Agency: Environmental Protection Agency (EPA)

Partnership Role of EPA

Various Federal Agencies have responsibilities for the public's welfare, regardless of the cause of the potential threat, be it natural disasters, accidents or intentional acts. Under the authority of the Safe

Drinking Water Act (SDWA), the EPA issues national regulations for the maximum safe level of inorganic, organic, microbial, disinfection by-product and radio nuclide contaminants in drinking water.

Under the SDWA, public water systems are required to monitor their drinking water to ensure that it is safe for their customers. Monitoring schedules differ according to the type of contaminant and the population served by the system. EPA approves the analytical methods to be used and certifies the laboratories that conduct analyses. Public water systems are required to notify the public whenever there is a violation of a drinking water standard.

In the event of an incident that threatens or actually contaminates a public drinking water system, such as in the aftermath of Hurricane Floyd, the EPA offers direct assistance to the affected communities by way of water testing and engineering assessments. Other Federal Agencies, such as the Corps of Engineers and FEMA, upon a Presidential declaration under the Stafford Act, may immediately supply bottled or tanked water and help reconstruct damaged systems.

Partnership Activity

EPA plans to work closely with the water utility industry through their professional associations. In accordance with its draft plan *National Infrastructure Assurance Plan: Water Supply Sector*, the EPA is working in partnership with the Association of Metropolitan Water Agencies and the American Water Works Association. EPA will work with water utilities undertaking measures to safeguard water supplies from terrorist and seditious acts. EPA will also implement an assessment of the vulnerability and methods to reduce vulnerability of the drinking water supply to terrorist acts.

In association with the Department of Energy, EPA sponsored a two-day workshop at the Argonne National Laboratory during summer 2000. The purpose of this workshop was to assemble various U.S. Government and water utility experts on water supply infrastructure protection. The workshop resulted in various recommendations as to how the Federal Government can best assist the water utilities in improving protection of this critical infrastructure. The EPA and the American Water Works Association - Research Foundation have contracted with the DOE's Sandia National Laboratory to develop a vulnerability assessment methodology. This methodology will be initially developed by having security experts look at the vulnerabilities of a particular utility. The methodology will then be tested on other utilities with different characteristics to make it more generally applicable to the industry.

The other major effort centers on threat information. EPA is working with the FBI to encourage the Association of Metropolitan Water Agencies to sponsor an industry-based Information Sharing and Analysis Center. This association, whose Executive Director is the Sector Coordinator, is also organizing an industry steering committee. The purpose of this committee will be to coordinate the activities among the various governmental and industry groups.

There is also relevant research underway in DOD, FEMA and HHS that would help support the partnership. The Department of Army is conducting research in the area of detection and treatment to remove various chemical agents. FEMA is developing a statewide and citywide model capable of tracking and predicting the movement of biological and chemical agents in surface waters (state-wide) and in a water treatment and distribution system (city-wide). HHS/CDC is developing guidance on potential biological agents and the effects of standard water treatment practices on their persistence.

6. Emergency Fire Services and Continuity Of Government

Sector Lead Agency: Federal Emergency Management Agency (FEMA)

Partnership Role of FEMA

The Federal Emergency Management Agency (FEMA) is the Federal Government's Lead Agency in the areas of Fire and Emergency Services and Protection to the Continuity of Government Programs.

Fire And Emergency Services Sector Partnership Activities

The United States Fire Academy (USFA) has the lead to coordinate awareness activities among fire and emergency services fire responders (33,000 fire departments, ten major national organizations, 50 State fire marshals) including related services such as 911 centers (4,300 centers; one national organization) and emergency equipment manufacturers (eight national associations). Information from the National Emergency Numbering Association (NENA) suggests that there are, depending upon definition, 3500 to 6100 emergency service centers. These systems generally meet performance specifications developed by the community. Technical specifications are developed in cooperation/coordination with local communications providers, and hardware/software is provided from a variety of vendors.

FEMA's experience during the Y2K rollover demonstrated that challenges in sharing information with such a diverse community were themselves major issues affecting preparedness. The need for some level of 'best practices' as a part of the awareness campaign became readily apparent. The USFA has several wide information distribution systems, which include e-mail notification, newsletter mailings, web page announcements, cooperation with professional publications and newsletters. The USFA also works with 20 to 25 of the major fire service associations.

The thrust of FEMA's activities supporting the Fire and Emergency Services community is to disseminate physical and cyber infrastructure protection information to the fire and emergency services community so that they can protect critical physical and cyber infrastructures. Specific support to the Emergency Fire Services community includes:

- Weekly review of news, computer emergency response team reports**,** fire and emergency service publications, and Web sites to identify critical physical and CIP issues/rumors/stories.
- Research of issues/rumors/stories about critical physical and cyber infrastructure vulnerabilities, and their impact on fire and emergency services. Based on the results of the research, either confirm or debunk the information
- Distribution of a monthly newsletter for major fire service organizations sharing critical physical and cyber infrastructure protection information.
- Issue two formal critical physical and cyber infrastructure protection information brochures for distribution to all fire and emergency departments and organizations.
- Receive / respond to incoming correspondence, e-mail, telephone calls regarding critical physical and cyber infrastructure protection.

Continuity Of Government Sector Activities

FEMA's critical missions are accomplished through the support of its physical operating facilities dispersed across the country. FEMA is the lead agency for facilitating a coordinated Continuity of Government (COG) program. In accordance with PDD-63, this effort shall ensure that vulnerability assessments and fixes to systems supporting COG are implemented.

7. Emergency Law Enforcement

Lead Agency: National Infrastructure Protection Center (NIPC)

Partnership Role of the NIPC

The Emergency Services Sector is comprised of three components: Fire, Medical, and Law Enforcement, each with a lead Federal Agency responsible for infrastructure protection plans and activities. The Department of Justice, through the FBI, is assigned responsibility for Emergency Law Enforcement Services (ELES).

Within the FBI, the NIPC coordinates ELES infrastructure activities, with the NIPC Director designated as the Sector Liaison Official.

Partnership Activities

As sector liaison for law enforcement, the NIPC is developing a plan to reduce vulnerabilities of state and local law enforcement to attack, and developing methods and procedures to share information within the sector.

- Unlike other sectors, ELES has no private partners. Virtually all emergency law enforcement services in the United States are performed by public agencies. The ELES Forum was established to act as the sector's private counterpart and its members represent major U.S. law enforcement organizations

The ELES Forum meets four times a year. A current objective is development of a sector plan and an initial operating capability. The Forum also discusses other items of interest such as training, awareness and education, and development of a warning notification system. The Forum approved the NIPC Watch and Warning Unit to act as the sector ISAC.

The most recent ELES Forum meeting was held December 5-7, 2000, in Brunswick, GA. At the meeting, a final draft of the plan was reviewed and an action plan for implementation was developed. The NIPC, with the participation of the Forum, also completed a vulnerability survey to assess the state of infrastructure protection preparedness in law enforcement agencies. Survey responses are being compiled and analyzed and will be distributed to participating agencies and made available to interested parties. The NIPC and the FBI Field Offices are also working with the state and local law enforcement agencies to raise awareness with regard to vulnerabilities in this sector.

8. Public Health Services Sector

Lead Agency: Department Of Health And Human Services

The Department of Health and Human Services (HHS) is the Lead Agency for the Public Health Services Sector. The goal of the CIP program is to develop a comprehensive program, including the identification of critical assets and protection of the critical infrastructures that pertain to the health care and human service sectors. This concept includes protection of laboratory and personal health services from physical attack and disruption, loss of confidentiality and integrity of information, and loss of availability of services.

The HHS intends to implement this responsibility by sponsoring a virtual ISAC and by having private sector representatives coordinate the outreach effort to disseminate private sector information.

C. Cross-Sector Partnerships

1. National Outreach and Awareness Partnerships

Partnership Role of the CIAO

A part of CIAO's mission is to coordinate a national education and awareness program to promote critical infrastructure assurance. CIAO promotes activities that inform business and technology leaders across industry and public institutions of the need to manage the risks that come with the benefits associated with reliance on information systems. CIAO focuses on initiatives that cut across industry sectors and are not the existing responsibility of agencies. In these initiatives, CIAO focuses on the policy, strategy and investment decision-making leadership across industry. CIAO's major activities to date in this initiative are reflected in the following five major areas:

- Partnership for Critical Infrastructure Security (PCIS);
- Business Risk Management Community;
- Mainstream Business Channels;
- Common Support for Industry Sector/Federal Lead Agency Partnerships; and
- Academic/Industry Colloquium.

Partnership for Critical Infrastructure Security (PCIS)

As industries began to organize themselves into partnerships with Federal Lead Agencies, they identified a need for cross-industry dialogue and sharing of experience to improve effectiveness and efficiency of individual sector assurance efforts. The PCIS was convened in response to that expressed need.

The partnership provides an awareness and participatory forum for government and owners and operators of critical infrastructures to address cross-industry issues of mutual interest and concern. It encourages opportunities for mutual support and action across the sectors. It also engages other stakeholders in CIP, including the risk management (audit and insurance), investment and mainstream business communities. It builds upon public private efforts underway between lead Federal Agencies and Sector Coordinators designated for each of the critical infrastructure sectors. The partnership is organized by industry for industry, with the U.S. Government acting as a catalyst and a participant.

Major PCIS activities include:

- Interdependency Vulnerability Assessment and Risk Management;
- Cross Information Sharing, General Industry Awareness and Outreach;
- Common Legislative and Public Policy Issues;
- Research and Development and Workforce Development;
- Input into subsequent versions of the National Infrastructure Assurance Plan; and
- Outreach to state and local governments.

An exploratory meeting with industry was convened on December 8, 1999, hosted by the Secretary of Commerce in New York.. The first industry organizing meeting was held on February 22, 2000 in Washington, D. C. at the U.S. Chamber of Commerce facilities, attended by over 135 company representatives. The partnership held its mid-year meeting in San Francisco on July 27, 2000, with representatives from industry, state and local and Federal Governments attending. An agreement was reached by industry to work individually and together on providing input into the *National Plan* by end of March 2001. A governance structure was put in place in the form of a coordinating committee that included all the sector coordinators from each of the industry sectors listed in PDD-63 with the government sector liaisons as *ad hoc* members. The U.S. Chamber of Commerce and the national CIAO serve as Joint Secretariat for the Partnership by request, the Coordinating Committee of the partnership has provided an interim status report of its accomplishments and activities to date, which is contained in Part VI of this report.

Business Risk Management Community

The business risk management community, consisting of auditors, financial security analysts, the insurance community, the legal community and financial reporting boards serve as unique channels of communication to senior leadership of industry. Their role and responsibility to senior leadership are to assess business risks, communicate noteworthy changes to those risks, and support the management of them. Starting in Spring 1999, an awareness and education partnership was implemented by CIAO with a consortium consisting of The Institute of Internal Auditors (IIA), National Association of Corporate Directors (NACD), the American Institute of Certified Public Accountants (AICPA), and the Information Security Audit and Control Association (ISACA)**.** This consortium brought the involvement of a number of noted insurance firms, risk management professionals, legal counsel with particular expertise in information systems, respected corporate board members, audit experts and financial security analysts from Wall Street.

The consortium held a series of five regional conferences, called "Audit Summits," kicked off with a high profile event in Washington, D.C. on April 18, 2000. These meetings were hosted or sponsored by prominent corporations that included JC Penney's, Home Depot, New York Life Insurance, Oracle Corporation, Arthur Anderson, Deloitte & Touche Tohmatsu, PriceWaterHouseCoopers, and KPMG. The target audiences were directors of corporate boards, chief auditors, and other corporate senior executives. The meetings rolled out a report, *A Call to Action for Corporate Governance: Information Security Management and Assurance*. This report provided guidance for corporate boards on managing information security risks. In addition, a report by a noted Wall Street analyst from Salomon Smith Barney, *Information Security Impact on Securities Valuation,* was distributed on the possible effect of disruptions of information systems on shareholder value.

Various discussions on corporate insurance, risk management and liability, along with these two reports, formed a "business case for action" relevant to boards of directors and corporate executives. Over 10,000 copies of the guide were distributed in the year 2000 to corporate directors across the U.S. IIA, who led and coordinated the "Audit Summits" for the consortium, rolled out a final report in October summarizing the conferences to over 300 of its chapters across the United States (including a videotape) as an education tool for auditors and also as support for tailored development and delivery of a "case for action" to their own corporate boards. Press coverage for the Audit Summits ranged from the Wall Street Journal to Reuters, United Press International, and Computer World, as well as television such as CNN, local channels from CBS, NBC, and ABC.

As part of this initiative, CIAO staff also briefed financial security analysts in New York on the business issues related to information security. These briefings reinforced analysts' understanding of the importance of managing information technology properly, including the security of those information systems. The briefings also appeared to reinforce an emerging analysts' view that the information security segment of the information technology industry merits independent tracking and assessment. Salomon Smith Barney published an Equity Research Report in September on "*Internet Security Software*," laying out the landscape of the market for information security software (and services), describing the market drivers and scope, thereby "defining" information security as a noteworthy market segment in the financial security markets for probably the first time. This report was distributed to institutional investors across the United States.

Mainstream Business Channels

Mainstream Industry Leadership: As part of its "partnership" with CIAO, the U.S. Chamber of Commerce has agreed to help distribute the *Call to Action for Corporate Governance: Information Security Management and Assurance* to affiliates (about 3000 of them) across the U.S., once CIAO completes tailoring the material for their use.

Corporate Boards of Directors: As a follow-on to its participation as a member of the consortium sponsoring the audit summits, the National Association for Corporate Directors (NACD) held a panel on Information Security and Corporate Governance in its program for its annual membership meeting in October 2000. The panel included a Chief Financial Officer, a corporate President and Chief Operating Officer, and a senior partner of a services firm. NACD has initiated of its own volition a survey and development of a "best practices" white paper for board oversight of information security. As a result of its participation in the Audit Summits, NACD's leadership has identified information security as an emerging issue on which it will continue to educate and provide support for its membership (many of whom sit on boards of corporations from the Fortune 5000). CIAO continues its partnership with NACD resulting from the audit summits.

CEOs and CIOs: As a result of a representative attending an Audit Summit, CXO Media, Inc., publishers of CIO Magazine (CIO audience) and Darwin (CEO audience), is cooperating with the CIAO in a "partnership" to raise awareness and understanding of the issue of information security and management, targeting specifically CIOs and CEOs of Fortune 5000 companies. As part of this cooperation, CXO Media, Inc. and CIAO co-sponsor two Internet Security Policy fora, specifically on information security related policies and strategies, and CXO Media will include a session in each of its major annual conferences on CIP and information security.

The first Internet Security Policy Forum was held and web cast on September 27, 2000, in Washington, D.C. Feedback from the audience indicated it was effective and successful. The entire event was archived and is available for reference on CIO Magazine's Web site. Over 5,000 visits to the archive have been made since September 2000. Sessions on CIP and information security were included into CIO Magazine's annual conferences in September and October. An average of 400 CIOs and other corporate executives attend these prestigious, invitation only events. CIAO co-hosts the information security and CIP sessions. The next conference, scheduled for January 30, 2001 will include a prime time session on "Protecting Infrastructures Across Borders," that will include public speakers from the U.S., Canada, Europe, and the Pacific Rim. As a result of the education provided by these sessions, and their own previous interest in this issue, both Darwin and CIO Magazines have begun to publish editorials and articles regularly on the subject.

Support For Industry Sector/Federal Lead Agency Partnerships

Due to its experience with its own outreach program, CIAO also provides support for the Federal Lead Agencies and their counterparts in industry for outreach and awareness building, specifically through the sponsorship of workshops on common issues shared by many of the sectors, including risk management approaches, information sharing, legal obstacles, etc. It has also provided support for the building of industry specific "business cases for action," since the business cases for senior leadership in industry tend to center around common concerns such as business operational survivability, customer relationships and confidence, and investor and public confidence.

National Colloquium for Information Systems Security Education

Our nation needs an information-literate work force that is aware of its vulnerability, as well as a cadre of information professionals who are knowledgeable of the recognized "best practices" available in information security and information assurance. The National Colloquium for Information Systems Security Education (the Colloquium) was established to serve as a forum to bring government, industry, and academia together to meet those challenges.

The Colloquium provides a forum to discuss and form needed direction in Information Security undergraduate and graduate curricula, common requirements, specific knowledge, skills and abilities, certification requirements, and establishment of professionalization boards. International participation began in 1999, and is predicted to continue in 2001.

Primary issues that were dealt with during the annual conference in 2000 included the outlook for information security from an industry perspective and the educational requirements for the year 2000 and beyond; the need for and the identification of Centers of Excellence in Information Assurance Education and the educational requirements that academia, government and industry perceive as an educational necessity. Working partnerships also continued to be strengthened among the participants with a commitment to expand more effective communications and to share information security resources; an agreement to continue the living body of the Colloquium and the annual conference; and, to further enhance its role as a forum for dialogue and collaboration among the three distinct constituencies represented.

2. Law Enforcement Information Sharing: Indications and Warning Partnerships

Partnership Role of the NIPC

The NIPC is at the core of law enforcement's warning, investigation, and response system for threats to, or attacks on, the nation's critical infrastructures. The NIPC sanitizes law enforcement and intelligence information for inclusion into analyses and reports that it provides, in appropriate form, to relevant federal, state, and local agencies; the relevant owners and operators of critical infrastructures; private sector information sharing and analysis entities, and the public itself. The NIPC also issues attack warnings or alerts to increases in threat condition to the private sector owners and operators.

The NIPC's major activities to date in this area fall under the following:

- InfraGard;
- Industry-specific Indications and Warning Systems;
- Key Asset Initiative; and
- Program Support Outreach.

InfraGard

The NIPC, in conjunction with private industry in general, has developed an initiative called "InfraGard" to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. The initiative facilitates the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each FBI Field Office. Chapter membership includes representatives from the FBI, private industry, other government agencies, state and local law enforcement, and the academic community. All FBI Field Offices have established InfraGard chapters.

Sector Indications and Warning Systems

NIPC, in partnership with the North American Electrical Reliability Council (NERC), has developed an "Indications and Warning" System for physical and cyber attacks. Under the pilot program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC to the power companies make this program especially worthwhile.

Key Asset Initiative

A second effort involving cooperation with the private sector is the Key Asset Initiative (KAI). A key asset can be defined as an organization, system, group of organizations or systems, or physical plant, the loss of which would have widespread and dire economic or social impact on a national, regional, or local basis. The KAI initially involves determining which assets are "key" within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in case of an emergency. FBI Field Offices are responsible for developing a list of the assets within their respective jurisdictions, while the center maintains a national database.

Program Support Outreach

The NIPC has also been working on a set of outreach conferences under the auspices of the Department of Justice and the Information Technology Association of America. The Attorney General, representatives from the NIPC, Special Agents from FBI Field Offices, and other law enforcement officials met with industry representatives at Stanford University in April 2000 at EDS in Herndon, Virginia in June 2000. At both conferences the Attorney General stressed ways that industry and law enforcement need to work together against computer hackers and intrusions.

NIPC representatives spend a significant portion of time speaking across the country and around the world to private sector and government groups, as part its effort to raise awareness about the cyber threat and to foster cooperation between industry and law enforcement. Recent meetings include the NSTAC, the System Administration, Networking, and Security (SANS) Institute; the Information Security Forum; the National Governors Association; the American Society for Industrial Security (ASIS); and the American Bar Association.

III. STATUS OF AGENCY CIP PROGRAMS

III. STATUS OF AGENCY CIP PROGRAMS

A. Federal Agency Roles and Responsibilities

PDD-63 and the National Plan rely upon the Federal departments and agencies to perform specified Lead Agency functions, which relate cyber security to their primary mission areas. There are, however, certain cross-government functions, for example:

- The Office of Personnel Management and the National Science Foundation are administering a new scholarship program, Cybercorps, to train college students who will then work in a Federal agency;

- The General Services Administration operates a telecommunications network used by many departments. GSA also operates the Federal Computer Emergency Response Team and will operate an intrusion detection and information sharing system for participating agencies;

- The Treasury Department has been assigned the mission of developing the Public Key Infrastructure system for itself and for the non-national security departments and agencies.

Separate small programs in each agency cannot perform these government-wide roles efficiently and need a single department to develop them on behalf of the Executive Branch. This has, however, sometimes led to confusion or lack of support for the budgets of these needed cross-Government programs.

Under PDD-63, Federal Agencies have a number of distinct responsibilities:

- All agencies are required to protect their own internal critical infrastructures, especially their cyber systems.
- Some agencies with special expertise or functional responsibilities are tasked with providing services to the government as a whole.
- A number of agencies are also charged with developing partnerships with private industry in their sectors of the economy.

The agencies' sector partnership efforts were described in the preceding section of this Report. This section focuses on agency internal and government-wide efforts.

In addition, there are other entities of the U.S. Government that have responsibility for formulating security and best practices standards that apply to information, security, and critical infrastructure assets. These agencies have also reported on their progress. This section also contains reports on these efforts.

Project Matrix

In response to Presidential Decision Directive 63, the national Critical Infrastructure Assurance Office established Project Matrix last year to "coordinate analyses of the U.S. Government's own dependencies on critical infrastructures." Participating in Project Matrix helps each Federal Department and Agency identify the assets, nodes and networks, and associated infrastructure dependencies and interdependencies that are required for them to fulfill their national security, economic stability, and critical public health and safety responsibilities to the American people. A number of Departments and Agencies refer to Project Matrix in their reports.

Project Matrix also helps each participating Federal Department and Agency:

- Identify the nodes and networks that should receive robust cyber and physical vulnerability assessments;
- Conduct near-term risk management assessments;
- Justify funding requests for high-priority security enhancement measures in the areas of physical security, information system security, industrial security, emergency preparedness, counter-intelligence, counter-terrorism; and
- Review actual business processes to better understand and improve the efficiencies of their organization's functions and information technology architectures.

Project Matrix involves a three-step process. In Step 1, the Project Matrix team identifies and prioritizes each Federal Department's and Agency's PDD 63 relevant assets. In Step 2, the team provides a business process topology on and identifies significant points of failure associated with each Department's or Agency's most critical assets. In Step 3, the team identifies the infrastructure dependencies associated with select assets identified in Step 1 and analyzed in-depth in Step 2.

Aside from the Departments of Justice and Defense and the U.S. Intelligence Community, Project Matrix has solicited the voluntary participation of 14 Federal Departments and Agencies. The Departments of Commerce, Energy, Health and Human Services (HHS), Treasury, and the Social Security Administration (SSA) compose the first group of Federal organizations that have volunteered to participate in Project Matrix. The Department of Commerce was the prototype for Steps One and Two and participated in the development of Project Matrix. Step One has been completed and formal reports have been prepared for SSA, HHS, and Treasury. The Department of Energy is initiating Step One at this time, and the Department of Commerce is repeating Step One to be consistent with the other Federal agencies and to ensure all of its data is in included in the Project Matrix database.

The Project Matrix team's findings are sensitive. For illustrative purposes, however, we can say that in the case of SSA, HHS, and Treasury all three organizations rely collectively on approximately 4,000 physical and cyber assets to conduct their day-to-day business. As a result of Step One, the Project Matrix team has determined that about 50 of these 4,000 assets require near-term priority attention.

SSA, HHS, and Treasury have indicated a desire to participate in Steps Two and Three. In each of these steps, the Project Matrix team will help complete a functional analysis on the 50 assets and identify their interdependencies and possible points of failure within the public and private sectors.

The Project Matrix team has been asked to complete an initial discovery phase in the Securities and Exchange Commission and the Environmental Protection Agency. Depending on the results of the reports, both organizations may participate fully in Project Matrix. The Department of Housing and Urban Development has asked to participate in Project Matrix even though their support was not requested. The team will seek the participation of the Departments of Interior and Transportation within the next few weeks.

The Project Matrix team also is assessing the applicability of its methodology to state and local governments, private industry, and foreign U.S. allies. In terms of state governments, discussions with Texas and Virginia are scheduled for this winter. In the case of the private sector, the team has decided to accept the National Communications System's offer of support and the facilitation of a possible partnership with major components of the nation's telecommunication industry. On the international front, exploratory discussions with Canada were initiated in December.

In FY 2001, the Project Matrix team will complete the documentation of its entire analytical process for use throughout the public and private sectors, improve its Step One automated data collection tool, develop compatible automated Step Two and Three tools, and establish a master crisis management database system for use by the national security community in assessing in near real time the impact to critical United States Government operations of real world events affecting adversely the nation's critical infrastructures.

Federal Departments and Agencies do not operate independent of one another. Due to significant advances in information technology, the public and private sectors have become inextricably intertwined. As a result, there is limited utility in each Federal Department and Agency viewing physical and cyber security only in the context of their own organization. Project Matrix provides each Federal Department and Agency an expanded, more comprehensive, realistic, and useful view of the world within which they actually function. Both the Administration, Congress, and private sector providers of the nation's critical infrastructures will require such information to implement cost efficient and effective physical and cyber security enhancement measures in the future.

B. Cabinet Departments

The following are reports provided by the Cabinet Departments, in alphabetical order. Each Department report begins with a section on internal CIP programs, followed by a discussion of external efforts.

1. Department of Commerce

Internal CIP Activities

The Department completed its draft CIP Plan and submitted it to the national CIAO in November 1998. A revised draft was submitted to the CIAO Expert Review Team in April 1999.

The Department formed a Critical Infrastructure Protection Management Group (CIPMG) to provide a monthly forum for coordination of the Department's CIP efforts, including internal responsibilities and Lead Agency role, and as an information and resource sharing opportunity to ensure that the Department's diverse CIP responsibilities are responsibly and effectively managed.

During FY 1999, the heads of all DOC operating units reviewed their critical business functions and identified those systems that they believed qualified as minimum essential infrastructure (MEI). Each of the operating units with critical infrastructure elements completed a draft CIP plan, responded to a National Security Council data call for intrusion detection monitors, and drafted a list of their critical interdependencies.

The Office of the CIO completed a contract for an independent validation and verification of the operating units' MEI choices. This allowed them to measure the gap in security resources for a FY 2001 budget submission, to evaluate the Department's CIP Plan and related plans such as IT security, contingency, and continuity of operations, and to develop a threat framework to be used in subsequent vulnerability assessments. The effort resulted in a finer granularity of asset identification, was more accurate in terms of national security, included physical assets and interdependencies of other government agencies, and was rank ordered for priority treatment. The Department revised its critical asset list accordingly in June 1999 and now has a prioritized list of assets that are critical in terms of national security. DOC subsequently constructed and populated a database of IT systems that includes the critical infrastructure ranking.

The success of this endeavor contributed to the CIAO's decision to use this methodology as a model for the civilian sector of the Federal Government and for its approval by the NSC and OMB. This was the pilot phase of the CIAO's Project Matrix Step One.

In June 2000, the Department's Office of the Inspector General (OIG) completed a review and issued a report on CIP efforts at Commerce. The Department CIP plan will be revised in keeping with this report, and following on the June 1999 contract effort, as time and resources permit.

The Office of the CIO contracted with the National Security Agency for information security assessment training for 36 Department of Commerce IT Security officers and to conduct an assessment for CIP critical assets. The assessment training was completed in September 2000 and NSA is drafting the assessment report.

2. Department of Defense

Department of Defense CIP Vision

CIP, within the Department of Defense, is an integrated, warfighter-focused effort to identify and mitigate vulnerabilities of critical assets essential to commander in chief (CINC) mission accomplishment and operational readiness. CIP establishes and maintains a comprehensive, fully integrated, and sustainable cyber and physical program for ensuring the availability of infrastructures critical to national security.

Within the Department of Defense, CIP ensures that the infrastructures needed to execute mission essential and national defense functions are available when needed. CIP looks at what we must have to meet our defense mission (e.g., facilities, equipment, information systems, communication systems and networks, people, power, contracts, etc.), then determines what are the most critical assets, identifies their associated vulnerabilities, recognizes infrastructure interdependencies, and then takes measures to reduce these vulnerabilities.

Government-wide Efforts: National Defense

As the functional coordinator for national defense, DOD has begun implementation and coordination of the activities of the Federal Government necessary to the national defense. It has formed a National Defense Infrastructure Coordination Group, made up of all involved Federal agencies, which acts as the coordinating body for the activities necessary for national defense. It also provides coordination and support to the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism and the CICG.

Incorporated into the Department's CIP implementation plan are unique sets of functions. These include military plans and operations, international cooperation, intelligence support, research and development, and education and awareness. For each of these functions, lead components within the Department have been designated to integrate the national defense activities across the various sectors and the other functions at the national level. The DOD plan called for, and the Department has established, a staff responsible for integrating and coordinating all CIP activities for the Department.

DOD will continue to invest in measures to protect our critical infrastructures and provide the information assurance needed for successful mission accomplishment. As a result, CIP budget requirements have been incorporated into the DOD programming and budget process for the FY 2002-2007 Defense Program.

Internal CIP Activities

The Department of Defense has made significant progress in CIP over the past year by focusing on the following objectives:

- Identifying what assets are critical to mission success, using a warfighting mission emphasis driven by the CINCs of our Unified Commands and supported by defense sector and service business operations;
- Determining if these critical assets are also vulnerable by leveraging existing anti-terrorism, physical security, information assurance, industrial sustainment and commercial dependency assessments and developing a single integrated assessment of mission vulnerabilities; and
- Prioritizing vulnerability remediation efforts by focusing on those infrastructures most essential to warfighter mission accomplishment and Department readiness.

In order to meet the above objectives, the Department has focused its CIP efforts over the past year in three major areas:

- Information Assurance – the identification and elimination of cyber vulnerabilities;
- Y2K – the development and application of Y2K-proven processes to CIP demonstrating that highly complex infrastructures can be understood, and that single points of failure, when identified, can be corrected in an expeditious and affordable manner; and
- Broader CIP Development – specific CIP efforts focused on developing and demonstrating the viability of those remaining component elements essential to making CIP a reality with the Department of Defense.

Information Assurance: To protect our information environment, the Department is using a defense-in-depth approach consisting of layered security systems and procedures, employing active and passive defensive measures to prevent unauthorized access to information and information systems. Defense-in-depth protects critical assets and processes by creating a deterrent posture, enhancing network security programs and operations, effectively training and certifying personnel, and leveraging new technologies.

This approach forces any adversaries to defeat multiple layers of protection before they are capable of impacting any activities. It is this layered security concept that allows DOD to make maximum use of commercial technology and minimize the investment it must make in unique government developed solutions. This construct is focused on the integration of the capabilities of people, operations and technology to defend the local computing environments (or enclaves), the enclave boundaries, the networks that link these enclaves, and the supporting infrastructures. While the vulnerabilities of systems can never be eliminated, they can at least be mitigated. In order to protect the information environment, Defense Department initiatives include:

- Deploying a strong, interoperable PKI across the Department to provide end-to-end encryption and authentication services for "sensitive but unclassified" information and to provide improved access control to information/computer systems. It will also provide security for classified information that must be sent over unprotected networks. Department-wide policy on deployment of a Department PKI was signed by the Deputy Secretary of Defense in May 1999 and updated in August 2000.

- Modernizing DOD's strongest encryption technology to keep pace with the rapid changes in information technology.

- Reengineering the "Information Enterprise," which is necessary to protect the Department's information systems.

- Advancing computer forensic capabilities. On September 24, 1999, the Department opened the Defense Computer Forensics Laboratory. This is a state-of-the-art facility to process computer evidence in criminal, fraud and counterintelligence investigations.

- Improving the Department's ability to actively defend computer systems. DOD has established a Joint Task Force for Computer Network Defense (JTF-CND) and the Commander-in-Chief, U.S. Space Command assumed overall responsibility for computer network defense on October 1, 1999.

- Establishing an information assurance vulnerability alert system for distributing vulnerability information to all Department elements. To support this capability, a database was developed to immediately distribute vulnerability information to each system administrator and to track and report the responses to these alerts.

- Establishing a comprehensive education, training and awareness program for military, civilians and contract employees. All users are required to receive initial awareness training prior to issuance of an account and systems/network administrators on both classified and unclassified systems are required to be trained and certified along with other personnel performing "critical" IA functions.

- The Chairman of the Joint Chiefs of Staff (CJCS) issued guidance to CINCs, Services, and Agencies to improve Information Assurance Vulnerability Alerts (IAVAs) compliance and requested commander involvement in the defense of their networks.

- The Joint Staff (J-6) has developed and is working toward implementation of an instruction identifying the minimum IA capabilities required for CINCs, Services, and Agencies (C/S/As).

- The Joint Staff (J-6) consolidated several existing IA working groups under one panel that reports to the Military Communications-Electronics Board (MCEB). The panel's work led to a significant reduction in the Department's information system's mobile code vulnerability

- The Joint Staff deployed a pilot IA capability to complement the network management capability provided to the CINCs. The pilot program enables JTF commanders to monitor the IA status of their AOR.

- As a member of the National Security Telecommunications Advisory Council (NSTAC), J-6 is involved in the NSTAC directed Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force. NSTAC provides industry-based analyses and recommendations to the President regarding policy affecting national security and emergency preparedness (NS/EP) telecommunications. One of its highlighted initiatives includes coordinating with the national CIAO to support significant advances toward the goals of PDD-63.

Y2K: As a global infrastructure reliability challenge, Department of Defense actions taken in preparation for the Y2K Date Conversion dramatically increased the visibility and criticality of both cyber and physical CIP throughout the Department.

Significant CIP results were accomplished during the Y2K effort as the Department shifted its focus towards an integrated cyber and physical infrastructure readiness approach, thereby dramatically improving the integration between the Department's CIO, CIAO's, CINC's, the Services, Defense

Agencies, and the Department's senior leadership. Department personnel worked together in integrated teams to make information systems and physical infrastructures Y2K compliant and reliable.

This dramatically improved the understanding of the Department's dependencies on critical domestic, host-nation, and international cyber and physical infrastructures. Y2K demonstrated that the Department could create an effective CIP program to protect both critical cyber and physical infrastructures and respond to the infrastructure challenges.

Broader CIP Development: Building on the information assurance and Y2K success, the Department of Defense is taking a broader view of the CIP problem – focusing also on the underlying critical infrastructures upon which our critical warfighting capabilities and cyber systems rest. Over the past year, the Department has developed and proven the CIP capabilities that provide the final pieces to complete the Department's CIP strategy.

At the Department installation levels, new and current commanders are being trained and advised on the criticality of private sector support in implementing and maintaining many of their daily activities. We have found that those commanders who have been on the job for several months have realized the need for unique working relationships with their local communities. These include establishment of fora where commanders and local/private sector leaders discuss the vulnerabilities and resolutions to many critical infrastructure problems. Such fora of information sharing have been very beneficial for both civil and military communities.

The Department's CIP efforts are focusing on the interdependencies of our infrastructures. For example, if the Army wants to move forces out of Fort Hood, there will be a need for reliable transportation, logistics, communications, power and industrial base assets and infrastructures. In addition, we must be able to determine how these infrastructures depend on each other and understand how the loss of one impacts the ability of the others to continue to function. The first step required the Department to mature its physical vulnerability analysis and assessment capabilities by enhancing its understanding of and ability to identify commercial infrastructure dependencies. With these efforts well underway, CIP focus shifted to three major areas:

- Developing a methodology linking infrastructure impacts to CINC (i.e., warfighter) mission accomplishment. It combines inputs from the CINCs with Sector and Service efforts and thus links the warfighter mission needs to the supporting infrastructures and assets. This capability was developed and proven through a series of prototypes.

- Developing an integrated assessment process that leverages the existing vulnerability assessments (e.g., physical security, IA, anti-terrorism, commercial assessments, etc.) into a comprehensive integrated vulnerability assessment that is necessary if both the warfighter and core business infrastructure vulnerabilities are to be identified and corrected. This construct was field tested at several locations to refine and enhance the process.

- Developing a set of standardized vulnerability assessment protocols so that every Departmental assessment produces comparable results. Realizing this construct enables risk management to be practiced from a Department-wide perspective for the first time.

By developing these three capabilities, the Department is now in a position to effectively manage consequences because we know what the impact of an infrastructure or asset failure is. In addition, over the last year, CIP efforts have:

- Developed and promulgated the *Department of Defense Critical Infrastructure Protection Execution Plan – Calendar Year 2000*.

- Developed *Defense Infrastructure Sector Assurance Plans (DISAPs)* to address the identification and vulnerability remediation steps necessary from a sector perspective and to define end-to-end sector functionality and those supporting assets essential to mission success.

- Developed prototype CIP analysis and assessment capability for identifying and assessing critical assets in support of Department missions.

- Developed and implemented capability to analyze and assess critical information transport dependencies on commercial telecommunications infrastructures to identify vulnerabilities and actions to mitigate potential single points of failure.

- Successfully included CIP planning and programming guidance in defense planning guidance.

- Initiated development of a risk-management framework to guide the prioritization of infrastructure protection efforts and investments.

A more detailed description of the Department's CIP activities is in Appendix A.

3. Department of Education

Internal CIP Activities

The Department's goal is to ensure the protection of its information and other critical infrastructure assets protection of against destruction, corruption, or loss of confidentiality.

The Department of Education has made significant progress over the past year by elevating the priority of its efforts to identify and mitigate vulnerabilities that are essential to promoting the Department's mission. These accomplishments include:

Additional Staff: The Department has significantly increased its staff resources addressing critical infrastructure protection requirements. Specific personnel resource accomplishments include:

- In April 2000, designating an individual as the Department's CIAO.
- In November 2000, hiring two individuals with expert knowledge of computer security.
- In July 2000, hiring an experienced Network Security Officer who is responsible for all security and infrastructure protection of the Department's wide area network (WAN) EDNet.
- In July 2000, hiring an individual to assist in all infrastructure protection activities.
- In October 2000, establishing the Deputy CIO for Information Assurance (DCIO-IA) as a permanent career SES position.

Creation of the Information and Critical Infrastructure Assurance Steering Committee: In May 2000, the Department established the Information and Critical Infrastructure Assurance Steering Committee on critical assurance matters and to coordinate and implement the Department's CIP program.

The Committee established work groups in a wide range of areas including:

- Assisting in the implementation of PDD-63.

- Developing security awareness and training program.
- Ensuring background investigations are conducted for both Departmental staff and contractors.
- Assisting in developing continuity of operations plans.
- Assuring privacy protection plans exist.
- Assisting towards utilizing Authentication/Public Key Infrastructure (PKI) digital encryption technology to ensure confidentiality, data integrity and non-repudiation.

Critical Infrastructure Protection Plan (CIPP): On December 7, 2000, the Department submitted a revised CIPP to the national CIAO, with copies to the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, and the Acting Federal Sector Lead, General Services Administration (GSA). This revised CIPP adheres to the Federal Sector Critical Infrastructure Plan Outline prepared by the GSA and addresses deficiencies previously identified by the CIAO and the Department's OIG. The CIAO's Expert Review Team reviewed and provided recommendations for improving our CIPP in February and June 1999. In September 2000, the Department's OIG completed an audit of our PDD-63 planning and assessment activities, which included recommendations for improving the CIPP.

Policies: In August, an updated and improved Information Technology Security Policy was submitted to the Office of Management's Administrative Communications System for clearance as a Department directive. This policy references requirements for protecting the Department's critical infrastructure. The CIO concurrently announced this as an interim policy. Comments are being received and a final policy directive will be issued in April 2001.

Awareness and Training: The Department is in the process of establishing a security and critical infrastructure protection awareness and training program to ensure employees and contractors develop and exercise fundamental security and infrastructure protection practices and habits. This goal will be achieved by implementing a comprehensive, effective security and critical infrastructure protection awareness and training program.

The Department already has begun to take steps to educate its personnel on some critical infrastructure protection issues. The Department has established an internal security training policy and has implemented a Web-based "Security Awareness Training" module, including a lesson on critical infrastructure protection. As of November 2000, 97 percent of the Department's personnel have completed this security awareness training.

A broader security and CIP training program will be offered to the Department's personnel nationwide, to ensure all understand the issues surrounding security and critical infrastructure protection. Topics will include:

- Asset and threat identification;
- Vulnerability assessments;
- Remediation and mitigation planning;
- Response and reconstitution actions;
- Warning and alert systems; and
- Use of the incident handling reporting system and procedures.

Specific training programs that are being developed focus on personnel who require specialized security and critical infrastructure protection training. The intensity and content of the courses will vary with job category. The Department has established five training categories, which are based on the National Institute of Standards and Technology's (NIST) Information Technology Security Training Requirements.

Over 900 individuals in the Department have been identified whose job responsibilities place them in one of these five categories:

- Group I – Includes individuals responsible for the computer security and/or critical infrastructure program of the Department, its review and implementation.
- Group II – Includes individuals required to fully understand the nature of the Department's computer security and critical infrastructure protection program.
- Group III – Individuals who are responsible for ensuring that the Department's security and critical infrastructure protection program is fully implemented and effected in all contracts issued by or used by the Department.
- Group IV – Includes technical personnel whose duties directly affect the security and infrastructure protection of the Department's critical assets.
- Group V –Individuals who need to be aware of computer security and infrastructure protection requirements that affect their functions. The Security Awareness and Training Work Group will explore training and education opportunities available elsewhere in the Federal Government and utilize existing commercial-off-the-shelf training products, including web-based training, interactive CDs, and videos.

Security and Critical Infrastructure Protection Expertise: On August 14, 2000, the Department and the GSA signed an Interagency Agreement allowing the Department to contract with GSA's Safeguard Program partners to provide technical support in addressing critical infrastructure assurance program requirements. On September 29, 2000, GSA awarded a contract to Electronic Data Systems Corporation (EDS) to provide expert technical support for the development and implementation of the Department's information and critical infrastructure assurance program. Several tasks were subsequently added, including the identification of mission essential infrastructure assets and a threat analysis and vulnerability assessment for each of these assets.

4. Department of Energy

Internal CIP Activities

The Department of Energy is systematically ensuring that its critical physical and cyber infrastructure assets are protected. The Department's first CIP plan, developed in November 1998, identified various task areas, including asset identification, vulnerability assessments, corrective action plans, emergency management initiatives, policy issues, resource and organization requirements, and interagency coordination. This is a living document and is being revised to reflect more recent initiatives and the results of an OIG audit.

Historical Perspective: The Department already has mechanisms in place for protecting its internal critical assets. The Department's physical security directives have always required stringent protective measures for important assets. With regard to improving protection of critical internal cyber systems, the Department has focused its efforts over the last two years on fixing clearly identified vulnerabilities in the Department's classified and unclassified cyber systems. These vulnerabilities have been highlighted by a number of successful attacks against unclassified systems across the complex, as well as reviews conducted by GAO, the Department's Independent Oversight Organization, and the Department's OIG. The CIO prioritized limited cyber security resources to improve computer security training across the Department, to field improved protection measures at our Departmental cyber incident response center, and to update Departmental cyber security policies and site-specific cyber security plans.

Recent Initiatives, Integrated Safeguards and Security Management: In addition to continuing efforts to strengthen its physical and cyber security posture through the analysis of vulnerabilities and the implementation of comprehensive mitigation measures, the Department has embarked on a comprehensive program to upgrade its physical and cyber security through the implementation of Integrated Safeguards and Security Management (ISSM). ISSM results in cultural change, integrating security into all aspects of operations and work. It is incorporated into critical processes, from planning through implementation, and ensures feedback to foster continuous security improvement. A similar program implemented in the safety regime has led to significant upgrades in the Department's safety posture with both acknowledgement and endorsement by Congressional oversight organizations. This approach is currently being replicated in the security area utilizing the previous lessons learned to ensure rapid deployment and implementation.

Project Matrix: In late 1999, the Department structured a process and questionnaire to systematically identify its critical internal assets. Project Matrix, a government-wide effort sponsored by the national CIAO, replaced these approaches in early CY 2000. The Department's CIAO and CIO signed an Interagency Agreement with CIAO on May 12, 2000, for the performance of Project Matrix and have subsequently funded identification and prioritization of critical assets relevant to PDD–63. The Department is one of the first five Federal organizations to implement this groundbreaking process. On July 19, 2000, the NSC endorsed Project Matrix as the desired approach for identifying and accurately characterizing the most important cyber and physical assets across the 14 high-profile Federal agencies (including DOE).

The Department with the approval and support of the Deputy Secretary has adopted this systematic process. A formal memorandum was issued on September 8, 2000 that commits the DOE to the following:

- Developing a prioritized list of physical and cyber assets relevant to PDD–63;
- Updating the internal CIP section of the CIP plan;
- Developing a gap analysis between the physical and cyber assets relevant to PDD–63 and their current security/mitigative status;
- Pilot implementation of Steps 2 and 3 of Project Matrix (interdependency analysis and private sector support analysis); and
- Implementing interdependency and private sector support analyses.

5. Department of Health and Human Services

Internal CIP Activities

The Department of Health and Human Services (HHS) CIP program will develop and implement a comprehensive and coordinated approach to protecting the critical infrastructures of the Department and its business partners. The goal of the program is to protect the critical infrastructures of the Department's health care and human service sectors from physical attack and disruption, loss of confidentiality and integrity of information, and loss of availability of services. The Department has adopted a three-year schedule, which began in October 2000, to implement the CIP project.

To address risk factors for critical infrastructure assets, HHS has developed a risk management program that ensures appropriate safeguards are taken to protect the data, information systems, and facilities under its control. This program addresses the three major security areas - physical, cyber, and personnel.

The risks to the physical infrastructure have been identified and mitigated using the minimum-security standards recommended by the Justice Department's Federal Marshall's Study. Additionally, each HHS Operating Division (OPDIV) is required to conduct annual vulnerability assessments of the security programs for buildings under its control to ensure that new risks are identified and mitigated.

The management of cyber risk is addressed by implementing Enterprise Infrastructure Management (EIM). The EIM program will provide an umbrella for the internal HHS systems and increased security for inter- and intra-agency networks. EIM is an operational IT management framework that protects the IT operating infrastructure by restructuring management practices, procedures, and functional boundaries and by providing automated tools to reduce user and systems administrator workload. In support of EIM, security policies addressing a wide range of cyber security issues are being developed to sustain our OPDIVs enhanced security programs.

Security risks associated with personnel, whether employees or contractors, have been defined and regulated for a long time. The management of these risks includes background checks commensurate with the sensitivity level of the position and limitations on the access allowed to sensitive data or systems. OPDIV Personnel Security Representatives (PSR), backed by the Department's Personnel Security Office, are responsible for assuring that position sensitivity levels are correct and consistent, and the individuals filling those positions meet investigative requirements. As of January 2001, each OPDIV and Staff Division Information Systems Security Officer (ISSO) must obtain certification from the PSR that an employee or contractor meets investigative requirements prior to the ISSO authorizing access to protected IT systems.

In addition, continuity of operations plans (COOPS) are in place to ensure the continuation of essential functions during situations that may disrupt normal operations. These plans provide the guidance needed to prepare for, respond to, recover from, and mitigate intentional and unintentional threats to those critical assets required for the Department's worldwide public health responsibilities. EIM will provide the cyber communication vehicle for the COOP and a special secure data and video teleconferencing capability.

The newly established Office of Information Technology Security and Privacy (OITSP), within the HHS Office of Information Resources Management, is responsible for overseeing the implementation of the CIP and for maintaining the HHS Computer Security Incident Response Capability (CSIRC). The CSIRC attempts to prevent, detect, and respond effectively to security incidents. To fulfill its PDD-63 responsibilities, HHS has adopted the Project Matrix (PM) methodology of the national CIAO. The project will provide a catalog of all of the facilities, systems, and processes along with their vulnerabilities and a plan of action to mitigate identified risks.

6. Department of Housing and Urban Development

Internal CIP Activities

HUD depends heavily on its information technology to carry out its mission and provide services to the public. HUD does not process classified information or operate classified systems; however, HUD recognizes the importance of protecting the privacy of citizens' personal information that is handled in the course of carrying out its mission. HUD is taking a proactive stance in responding to the growing concerns to ensure the continuity of government in a national crisis and defend against cyber attacks by strengthening the protection of its automated information resources. HUD's goal is to achieve and maintain the ability to protect its critical infrastructures from intentional acts that would significantly diminish its ability to perform essential functions and to ensure ongoing business operations.

HUD has taken the following actions to support its commitment to CIP:

- Hired a CIAO in May 2000;
- Provided resources to the HUD CIAO to help oversee the implementation of PDD 63, OMB A-130, Appendix III, and other laws and mandates pertaining to critical infrastructure protection and information assurance;
- Updated its CIP plan to include OIG recommendations in June 2000;
- Installed an intrusion detection system on the HUD network;
- Developed a HUD-wide education, and awareness program;
- Developed a information systems security Web site for its users;
- Established a letter of agreement with the federal computer incident response capability;
- Established a statement of work for services provided by GSA's Safeguard Program for computer security planning, security reviews, risk management, critical infrastructure continuity and contingency planning, physical infrastructure protection, emergency preparedness, and information assurance. HUD will establish partnerships with relevant private sector industries to address critical infrastructure protection through GSA's Safeguard Program;
- Initiated a Project Matrix Assessment by the national CIAO;
- Developed an information systems security program policy outlining the Secretary's policy for critical infrastructure protection and information assurance, assigned responsibilities to program areas, and defined the CIAO structure within the office of the CIO;
- Developed an information systems security handbook to provide CIP and IA procedural guidance to HUD employees and contractors; and
- Developed a draft incident response policy.

7. Department of Interior

Internal CIP Activities

The Department of the Interior has completed initial physical security assessments of its assets. The Department is in the process of upgrading the physical security safeguards recommended in the security assessments and is also conducting security assessments on its CIP information technology systems.

The CIO has issued a revised Department security plan that incorporates requirements for the protection of information assets designated as critical infrastructure. The plan specifies the use of NIST published security principles and practices.

Interior is presently using the GSA's SafeGuard Program to obtain the technical and administrative support for IT security program development. The Department is in the process of issuing an updated CIP plan that includes recommendations made as a result of the recent OIG audit.

8. Department Of Justice (DOJ)

Internal CIP Activities

The Justice Management Division (JMD) is responsible for developing the Department's Internal Information Assurance Plan required under PDD-63. JMD prepared an initial DOJ CIP plan in November 1998 and submitted the plan for evaluation to the national CIAO expert review team. The CIAO provided recommendations for changes and these changes were incorporated by JMD into a second DOJ plan in April 1999. In May 2000, JMD prepared a draft CIP interim operating capability document that was supposed to include an inventory of critical infrastructure assets, a vulnerability assessment for

those assets, and a remedial action plan if unacceptable vulnerabilities were identified. The due date for the final Document was May 2000. This Document was never sent to the CIAO. The DOJ OIG reviewed the document in May 2000, during an internal audit of DOJ compliance with PDD-63. The OIG found that the draft CIP interim operating capability document was incomplete and did not meet the requirements of PDD-63. Based on the findings of the audit report from the OIG, JMD has developed a new plan for meeting the PDD-63 requirements, leveraging work that is being performed by DOJ components to certify and accredit all computer systems and networks.

Currently, DOJ is completing the identification of the minimum essential infrastructure (MEI) - the inventory of DOJ information systems and supporting facilities and staff the Department must have to carry out its missions related to national security and law enforcement. JMD staff has developed a draft MEI inventory using guidance from *Practices for Securing Critical Infrastructure Assets*, published by the national CIAO. JMD is working with the components that operate and maintain the systems proposed for inclusion in the MEI to thoroughly document the decision to include each system in the MEI. The inventory of systems will include information on system location(s), facilities housing or supporting the system, the personnel supporting the system, and any other interdependencies (e.g., other data systems or networks used to feed or access the system identified in the inventory). The revised MEI and accompanying documentation will be submitted to the DOJ Information Technology Investment Board (ITIB) for concurrence. We expect this process to be completed in January 2001.

JMD will conduct vulnerability assessments of the assets included in the approved MEI based on system certification and accreditation documentation provided by Department components operating the systems. Documentation JMD will review will include system security plans, risk assessments, and contingency plans. In addition, each system included in the MEI will be subjected to an independent verification and validation review to assess the completeness and quality of their security planning efforts. Using this process, we expect to complete the vulnerability assessment of the MEI by June 30, 2001.

The extent and scope of the remedial action plan will be dependent upon the vulnerability assessment. The JMD will work with each component to identify actions that can be taken to mitigate the vulnerabilities discovered through the assessment. JMD expects to complete the remedial action plan and any corresponding funding plan by September 1, 2001.

Government-Wide Efforts: Law Enforcement

The United States Government has worked to enhance protection of critical infrastructures by ameliorating problems arising from the international nature of computer crime. It has been active in two primary multilateral fora dealing with computer crime: as an observer working with the Council of Europe Convention on Cyber Crime and the G8 Subgroup on High-Tech Crime. It has also done extensive work to promote awareness of issues relating to computer crime in other international fora, including the United Nations and the Organization for American States.

The Council of Europe Convention breaks new ground by being the first binding multilateral instrument drafted specifically to address the problems posed by the international nature of computer crime. The negotiation of this Convention is in its final stages, and U.S. representatives are still working to incorporate the comments of industry groups and privacy advocates, working toward a Convention that provides important benefits for public safety without unduly burdening industry or infringing the legitimate privacy interests of individuals.

Additionally, representatives of the Department of Justice serve as chair, as well as head of the U.S. delegation, to the G-8 Subgroup on High-Tech Crime. The work of the Subgroup has focused on

practical enhancements to the abilities of international law enforcement to prevent, investigate, and prosecute high-tech crime. Among the accomplishments of the G-8 is the establishment of a global network of 24-hour points of contact for rapid assistance in urgent high-tech investigations. (The Computer Crime and Intellectual Property Section of the Criminal Division serves as the U.S. point of contact.) More recently, the Subgroup has engaged in a dialogue, through conferences and workshops, with worldwide industry leaders to jointly address cybercrime issues and promote safety and security in cyberspace. The Subgroup also was instrumental in producing a set of ten principles and a ten-point action plan to combat international computer crime, which was adopted by G-8 Justice and Interior Ministers in December 1997, and subsequently endorsed by G-8 Heads of State.

PDD-63 created the CICG as an interagency committee charged with analyzing CIP issues and developing policy recommendations. A subgroup on legal issues was created and is chaired by the Department of Justice. The subgroup studied possible legal disincentives to information sharing. The success of an information sharing mechanism depends on the creation of a trusted environment where both the 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. Potential contributors from the private sector may be reluctant to share specific threat and vulnerability information because of impediments they perceive to arise from antitrust and unfair business practice laws. For example, failure by a company to share such information, or to act on such information shared by others, might carry liability consequences for public and private participants. Furthermore, 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 subgroup on legal issues continues to focus on legal or process reforms that may effectively overcome these and other similar obstacles.

Government-Wide Efforts: NIPC/FBI

The NIPC, an interagency office located at the FBI, serves as the focal point for the Government's efforts to warn of and respond to cyber intrusions. In accordance with PDD-63, the NIPC has elements responsible for warning, analysis, computer investigation, emergency response coordination, training, outreach, and development and application of technical tools.

The NIPC/FBI's role in response consists of investigating intrusions to identify the responsible party and issuing warnings to affected entities so that they can take appropriate protective steps. In the cyber world, determining what is happening during a suspected intrusion is difficult, particularly in the early stages. An incident could be a system probe to find vulnerabilities or entry points, an intrusion to steal or alter data or plant sniffers or malicious code, or an attack to disrupt or deny service. The cyber crime scene is totally different from a crime scene in the physical world in that it is dynamic -- it grows, contracts, and can change shape. Determining whether an intrusion is even occurring can often be difficult in the cyber world, and usually a determination cannot be made until after an investigation is initiated. In the physical world, by contrast, one can see instantly if a building has been bombed or an airliner brought down.

Further, the tools used to perpetrate a cyber terrorist attack can be the same ones used for other cyber intrusions (e.g., simple hacking, foreign intelligence gathering, organized crime activity to steal data, etc.), making identification and attribution more difficult. The perpetrators could be teenagers, criminal

hackers, electronic protestors, terrorists, foreign intelligence services, or foreign military. In order to attribute an attack, FBI Field Offices gather information from within the United States using either criminal investigative or foreign counter-intelligence authorities, depending on the circumstances. This information is necessary not only to identify the perpetrator, but also to determine the size and nature of the intrusion: how many systems are affected, what techniques are being used, and what the purpose of the intrusions is--disruption, espionage, theft of money, etc.

On the warning side, if it is determined an intrusion is imminent or underway, the watch and warning unit is responsible for formulating warnings, alerts, or advisories and quickly disseminating them to all appropriate parties. If 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 the government and the private sector so they can take immediate protective steps.

Finally, pursuant to PDD-63, the NIPC has electronic links to the rest of the government in order to facilitate the sharing of information and the issuance of warnings. The PDD directs all executive departments and agencies 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 bolster its technical capabilities, the Center selectively employs private sector contractors. By bringing other agencies directly into the Center and building direct communication linkages to government agencies and the private sector, the Center provides a means of coordinating the government's cyber expertise and ensuring full sharing of information, consistent with applicable laws and regulations.

9. Department of Labor

Internal CIP Activities

The Department takes a comprehensive approach to protecting its critical infrastructure. The Department also recognizes that employee awareness and strong integration of security practices into the lines of business are essential elements to protect vital information systems. Therefore, the Department, under the governance of the CIO, uses a collaborative approach to its information technology planning and management functions. Agency information technology professionals, administrative officers, and business professionals from program areas work together to turn strategic plans into reality.

Selected accomplishments for FY 2000 include:

- Development of an IT Architecture. The IT architecture provides a common basis for interoperability, portability and unifying standards development. Security standards are addressed in the technical reference model (March 2000).

- Development of a cyber-security program plan that contains the overall plans, milestones, and critical path to enhance the protection of critical information systems (October 1999).

- Establishment of a systems development and life cycle management methodology, to provide systematic design, development, change management and documentation standards for information technology systems, including the application of security measures throughout a systems' life cycle (July 2000).

- Development of a *Computer Security Handbook*, that provides departmental guidance for developing agency-specific cyber security programs, for conducting vulnerability assessments, incident response and reporting, and security awareness and training. It also establishes the Department's emergency incident response team (April 2000).

- Conducted vulnerability assessments and updated system security plans for critical assets and general support systems and major applications as defined by OMB Circular A-130.

- Conducted computer security awareness training for Department employees, and provided specialized information technology security training for information technology professionals.

- Installed an intrusion detection system on the Department's core network backbone.

- Replaced the firewall system on the core network.

- Implemented an automated tool to perform log analysis functions.

- Budgetary support for achieving infrastructure improvements and systems protection was obtained through the Department's information technology capital planning and management process. Through this process, departmental information technology security, privacy and related requirements were identified, quantified in terms of cost and benefits, and managed through the systems development life cycle program. The Department established a multi-year budget crosscut initiative entitled "Security and Privacy" beginning in FY2001 to ensure adequate financial resources were obtained to strengthen the Department's cyber security program.

10. Department of State

Internal CIP Activities

In response to the mandates of PDD 63, the Department of State identified and documented all its IT assets, developed a draft CIP plan and conducted a preliminary vulnerability assessment. The CIP plan was instrumental in highlighting the Department's fundamental reliance on the existent cyber-based technology and it's supporting IT infrastructure. Nearly every business process that directly or indirectly supports the Department's primary missions is reliant on the IT infrastructure. The CIP plan also helped in the identification of mission essential processes and the infrastructure that supports them. The CIP plan was subsequently revised and submitted to the National CIAO. The CIAO's review of the Department CIP plan was favorable.

The vulnerability assessment underscored the Department's dependency on the IT infrastructure as it concentrated on the identification of serious vulnerabilities; highlighted the complexity of the Department's IT infrastructure; and further illustrated the Department's unquestionable reliance on it to accomplish its primary missions. The vulnerability assessment was followed by a series of tabletop exercises intended to further identify the likelihood of specific threats. The results from the tabletop exercises were subjected to a comprehensive analysis intended to help integrate IT security and PDD-63 requirements into already existing IT lifecycle management processes.

The Department must ensure that its IT resources are adequately managed, maintained and protected at all times in order meet the requirements of PDD-63 by 2003. To this end, the Department created the PDD-63 governance board comprised of senior-level officials responsible for overseeing the implementation of this directive. The governance board and the Department's CIO bear primary responsibility for

information assurance requirements for the agency and its missions throughout the world. The Bureau of Diplomatic Security, along with the CIO, bears responsibility for formulation of IT security policy and its promulgation. These groups will work together to comprehensively address PDD-63.

For the Department of State, maintaining an acceptable IT security posture and protecting its critical infrastructure are closely related goals, which require unyielding commitment in terms of vision, planning and investment. Their attainment is contingent upon the Department's ability to implement an efficacious IT lifecycle management structure that embraces security as a critical variable rather than an adjunct function or an accidental and possibly costly after-thought.

Initial Operating Capability: The Department has expended significant efforts in response to PDD-63. To date, it has actively sought to engage the Federal community and the Federal CIO Council in the development and implementation of appropriate information assurance strategies that incorporate industry best practices and effectively utilize Federal resources and assets. The following is a brief synopsis of these efforts:

- Identified Department business processes as required by OMB Circular A-11;
- Inventoried and base lined Department corporate IT assets;
- Reused, to the extent possible, data collected as a result of the Department Y2K effort;
- Developed a layered defense strategy for IA;
- Developed a comprehensive computer incident response team to respond to computer incidents involving the Department networks;
- Established the Foreign Affairs Community Threat Analysis Cell (FACTAC) to coordinate and facilitate the collection and dissemination of IT threat information;
- Created the computer incident response capability program to address incidents of a non-criminal nature, and coordinate notification and operational incident response;
- Established the virus incident response team with primary responsibility for the protection of the Department's IT infrastructure against threats posed by malicious code;
- Conducted comprehensive tests of mainframe contingency and disaster recovery plans for critical business processes reliant on these systems;
- Established the Network Intrusion Detection Program, designed to provide warning and alerts for possible unauthorized access to the Department's networks, centrally monitored on a 24x7 basis.
- Conducted computer security evaluations of overseas and domestic sites; and
- Conduct penetration tests of Department networks to identify vulnerabilities.

Security Education, Awareness and Training: The Department has expended significant resources and efforts to enhance IT security awareness, training and education efforts. The CIO has worked closely with the Bureau of Diplomatic Security to incorporate IT security fundamentals into the Department's training curriculum offered by the National Foreign Affairs Training Center. Additionally, the Department requires that all the Department's employees, contractors, and consultants attend a mandatory annual refresher IT security education and awareness course.

The Department has also coordinated closely with the Federal CIO Council, other Federal agencies and private industry to promote IT security awareness by sponsoring the following events within the last year:

- Cyber Threat Summit hosted by the Department of State;
- CIP Day hosted by the Department of State; and
- Lecture on threats posed by computer hackers.

Management Controls and Policy: The Department established the Office of the Corporate Information Systems Security Officer (CISSO) in 1998 to oversee the implementation of PDD-63 for all IRM-owned IT resources and coordinate a Department-wide implementation of critical infrastructure assurance requirements. The CISSO is primarily responsible for ensuring that all Department corporate assets, to include IT systems, physical components and supporting applications, are adequately protected. The Department created the security infrastructure working group comprised of senior agency officials from the Bureau of Information Resource Management, the Bureau of Diplomatic Security, the Bureau of Management, and other Department organizations to oversee the development and implementation of information assurance policies and programs at the Department. This group has been instrumental in the development of PDD-63 remediation strategies and in coordinating joint efforts between bureaus.

The Department is currently working to reengineer its IT security policy development and promulgation process to adequately respond to rapidly changing technologies and requirements. The Department has updated its body of policy to reflect recent legislative initiatives and related requirements.

In support of information security and privacy requirements, the Information Resource Management Bureau has established the PKI program office chartered to coordinate and develop a Department-wide PKI approach. The PKI Program Office has worked closely with the Federal CIO Council and the Department of the Treasury to coordinate responses and research PKI solutions. The PKI Program Office is currently conducting a key recovery pilot project.

Lastly, the Department is spearheading an intergovernmental effort through the Federal CIO Council to develop a standardized PDD-63 terminology for the Federal government. In support of this effort, the Department will sponsor a CIP workshop with the objectives of reaching government-wide consensus on the appropriate terminology in reference to PDD-63, and a uniform approach to integrate PDD-63 requirements into the Federal budgetary process.

Government-wide Efforts: Foreign Affairs

A sound long-term strategy to protect U.S. critical infrastructures depends not only on implementation of our national plan, but on appropriately communicating our plan and cooperating with other nations and international organizations. The United States Government already conducts a wide range of bilateral and multilateral CIP-related initiatives (e.g., international standards discussions, law enforcement, national security, and research and development. Such *ad hoc* efforts, however, can be less effective and slow to develop without high-level, government-to-government contacts to encourage CIP cooperation as a national priority. Uncoordinated agency efforts also can lead to foreign governments receiving mixed or incorrect messages about U.S. national CIP policy.

The United States is implementing an international strategy to coordinate CIP outreach to other governments and international intergovernmental organizations by promoting CIP awareness, emphasizing vigilance in security standards and practices, and enhancing law enforcement cooperation as basic elements of the strategy for addressing CIP threats. An interagency working group under State Department leadership has already established agendas with certain governments for government-to-government work on CIP. Working with the NSC, the working group will continue to establish agendas with other governments and coordinate U.S. involvement in international intergovernmental organizations. Priorities will reflect the extent to which U.S. infrastructure is interdependent with that of any particular country or group of countries.

The bilateral meetings held so far underscore the continuing need to raise awareness that CIP is a matter of national economic and political security. CIP must be accomplished in partnership with the private

sector. Part of that partnership includes building trust between the private sector and law enforcement communities who will frequently be the first line of warning and response to CIP attacks. Accordingly, secure and rapid ways to exchange threat and response information must be developed internationally and to ensure that countries have adequate laws and agreements that will facilitate cooperation in the investigation and prosecution of entities that perpetrate attacks on critical infrastructures.

11. Department of Transportation

Internal CIP Activities

The Department of Transportation's CIO is leading a Department-wide effort to improve the security of DOT's information systems. Leading initiatives include:

- Updating and revising all Departmental IT security policy and guidance;
- Working with the operation administrations within DOT to improve the security of all DOT internet accessible IT assets; and
- Researching and demonstrating new IT security technologies.

Within our Operating Administrations, the Federal Aviation Administration (FAA) and Coast Guard (CG) remain at the center of our infrastructure protection efforts. The National Airspace System (NAS) and several Coast Guard systems have been identified as critical under this definition.

FAA and the NAS: The FAA Administrator established an Information Systems Security Program (ISSP), which established policy and assigned organizational and management responsibility to ensure implementation of the ISSP. A Director of Information Security was also assigned within the Agency's CIO office.

The *Information Systems Security Enhancement Handbook Version 1.0* was released to the FAA organizations, which provides a framework to develop ISS programs. The handbook provides direction regarding the types of information to be collected and Documented, the assessment of the information, and a process for ISS certification and authorization.

The *Information Systems Security Architecture (ISSA) Version 1.1* was released in 2000. The ISSA is a top-level design document for integrating security into the NAS. The ISSA uses requirements defined by previous policy, threat, vulnerability, and risk assessments to derive security services for NAS Air Traffic Control operations.

The FAA has established a C&A process for FAA information systems. The C&A process addresses life-cycle security risk issues for information systems. FAA's C&A work began using the list of mostly National Airspace Systems provided in response to PDD-63, however, the C&A process will extend beyond the NAS. FAA has completed the C&A process for 18 systems and the FAA Administrator has a contract with DOT for 20 additional systems in FY 2001.

The FAA has begun to develop a prototype for concept called Integrated Facility Certification (IFC) at the Washington Air Route Traffic Control Center in Leesburg, Virginia. The IFC concept addresses a holistic view of physical, personnel, and information systems security at a facility level to compliment the certification and authorization process of information systems.

The FAA has partnered with the FBI National Infrastructure Protection Center (NIPC) and detailed a senior level ISS professional to NIPC. This assignment fosters the sharing of threat and incident information, along with outreach to infrastructure service providers and the transportation industry.

FAA has established an outreach program to open a dialogue with labor, industry, and the international community on the issues and solutions for the information systems security program. The outreach program plan will be distributed in second quarter FY-2001.

FAA has established an Initial Operating Capability (IOC) of a Computer Security Incident Response Capability (CSIRC) to detect and prevent malicious activity. The CSIRC will provide threat information to FAA entities and respond to reported and detected incidents as staff and tools are added in FY-2001.

The FAA has provided Information Systems Security awareness training to over 40,000 FAA employees. In addition, more than 70 FAA employees have been trained for the Certified Information Systems Security Professional examination. This advanced training increases security awareness for professionals in the information systems field, builds an in-house ISS expertise, and provides an incentive to retain expertise in the agency.

Coast Guard: The Coast Guard has completed risk assessments and security plans for the following designated critical systems: the Operations System Center, whose systems serve as the information heart of the Coast Guard's search and rescue, law enforcement, marine safety, logistics, and personnel support functions; the automated mutual-assistance vessel rescue system used to provide U.S. and foreign search and rescue authorities with pertinent information about merchant vessels on the high seas that might be in a position to provide assistance to a distressed vessel or aircraft; the marine safety information system used in the analysis of safety degradation patterns and equipment failures, to focus and redirect marine safety activities and resources; the marine information for safety and law enforcement information system, which provides information sharing to improve communications, resource utilization, and the effectiveness of Coast Guard missions; the communication system network that carries receive/transmit voice, data, and control information between the communications area master stations and four communication stations; and the national distress response system provides distress, safety, and command and control VHF-FM communications that covers all areas of boating activity (including inland waters) in which the Coast Guard has search and rescue responsibilities.

Office of Intelligence and Security: DOT's Office of Intelligence and Security plans the following initiatives:

- Continue development of the infrastructure assurance training and awareness program in cooperation with the transportation industry and the operating administrations.
- Continue the assessment of critical transportation information systems and develop systems to rapidly disseminate and share vulnerability and threat information.
- Develop a comprehensive approach to assessing threats to and vulnerabilities of transportation's physical and information infrastructure, and implement integrated technologies and procedures tailored to these threats.
- Continue to work with the operating administrations to improve the flow of threat and warning information to field elements.

Global Positioning System (GPS): PDD-63 requires DOT (in consultation with the DOD) to thoroughly evaluate the vulnerability of our national transportation infrastructure, which relies on GPS. The Volpe National Transportation Systems Center was tasked to study this issue and is expected to deliver a final report on this topic in the near future. Volpe's preliminary report identified GPS vulnerabilities and their

potential impacts to aviation, maritime transportation, railroads, and intelligent transportation systems. The final report will also recommend potential mitigation alternatives. The Office of the Secretary of Transportation plans to coordinate a review of the findings by in the second quarter of FY 2001. Specific mitigation approaches will be developed.

Threat Warning Dissemination: DOT has chartered a Department-wide communications requirements study. This study will develop a process to receive and disseminate threat warning information, and establish a communications architecture to coordinate and share cyber threat information quickly both internally and externally.

Education and Awareness: DOT will be working with the Federal Law Enforcement Training Center (FLETC) to develop a new CIP training course, leading a FBI transportation critical infrastructure training conference in June, and developing a DOT-wide CIP education and awareness plan with the Volpe Center.

12. Department of the Treasury

Internal CIP Activities

The Department's strategy for developing a critical infrastructure assurance strategy, plan and capability to protect its own infrastructure, in accordance with PDD-63, is summarized in the Treasury CIP plan (TCIPP), dated November 18, 1998. The Department established a Treasury Infrastructure Protection Panel (TIPP), comprised of the CIAOs and CIOs from each of the Treasury Bureaus. The panel is chaired by the Treasury's CIO, who also serves as the Treasury CIAO. The TIPP is responsible for developing, formulating, recommending, and establishing the policies, guidelines, plans, and organizational relations for a comprehensive CIP program as outlined in the TCIPP.

Treasury has steadfastly adhered to a fundamental operational principle that all of its security disciplines must play a major role in contributing to the protection and assurance of Treasury Critical Infrastructure (TCI) in times of peace, crisis, disaster or emergency. Therefore, we have been working closely over the last two years to integrate our security disciplines (i.e., information systems, personnel, industrial, and physical security) and our classified and sensitive information management and emergency management programs to achieve critical infrastructure goals and objectives.

Significant TCIPP implementation activities undertaken under the auspices of the TIPP include:

- The identification and prioritization of its critical infrastructures with the help and support of the national CIAO's Project Matrix team.

- The establishment of a cyber CIP working group to assist the TIPP in developing and implementing a Treasury-wide CIP program to deal with cyber threats. Group members have developed policy, an implementation plan, and guidance, including a systemic approach for assessing vulnerability of cyber systems. An IT security capability "roadmap" is being formulated to develop CIP multi-year management plans for protecting cyber (IT) systems. A subgroup has identified automated tools for use in assessing the vulnerability of critical cyber systems.

- Security practices to mitigate the risk to agency cyber systems include:
  - Annual OIG audits of IT internal controls;

- Incorporation of new system applications into Agency-wide IT architecture, with risk management as a part of the system life cycle to comply with requirements in the Information Technology Management Reform Act (also known as" Clinger-Cohen");
- Active vulnerability and virus-scanning programs in the bureaus;
- Formal Computer Security Incident Response Capability (CSIRC) in four bureaus and informal incident response teams on call in the others; and
- Penetration testing.

- The establishment of a CSIRC working group to develop a Departmental-wide CISRC to coordinate incident response and reporting and processes for identifying and resolving computer security irregularities that affect Treasury operations across the Department. The group has established a memorandum of understanding with FedCIRC and is finalizing concepts and procedures for issuing timely warning/alert notifications to Treasury's OIG and bureau CSIRCs.

- The establishment of a physical security task force to coordinate vulnerability assessment planning for Treasury facilities identified as TCI.

- The expansion of the charters and agendas of Treasury's terrorism threat advisory, insider threat, and emergency management working groups to include CIP issues and concerns to promote integrated CIP planning and expand CIP education and awareness across the Department.

- New, Treasury CIAO-sponsored threat briefings for TIPP members to increase their awareness of threats to Treasury critical infrastructure and to increase risk management planning.

- Utilization of the FTS Safeguard Program, as well as other federal and private sector entities to acquire professional services to support information assurance, vulnerability assessments, contingency planning and other TCIPP implementation activities.

- The establishment of a Critical Infrastructure Protection Training Program (CIPTP) at Treasury's Federal Law Enforcement Training Center. The first CIPTP course developed with the help of representatives of the Departments of Energy, State, Justice, and Commerce (national CIAO); the Social Security Administration; Tennessee Valley Authority is scheduled for February 2001. The course is open to Federal, State and local law enforcement and security professionals engaged in CIP and will be held quarterly.

- The Treasury CIO will host an upcoming IT Conference in February 2001.

In the year ahead, Treasury will continue implementing many of the activities cited above and will increase the number of TCI vulnerability assessments to reduce and or eliminate identified vulnerabilities and risks. The Department will also explore the possibility of working with the National CIAO in undertaking Steps 2 and 3 of Project Matrix to determine key TCI interdependencies. And, most importantly, Treasury will continue to foster greater linkage and cooperation between its CIP and continuity of operations planning programs to strengthen the Department's overall security and emergency preparedness posture.

13. Department of Veterans Affairs (VA)

Internal CIP Activities

The VA Department provides for CIP as part of its Department-wide information security program and strategy. VA has been made acutely aware, through numerous audits, studies, and penetration tests, that an underlying cause of its poor information security was that it did not have a continuous management approach to proactively control risk. Instead, there was a tendency to react to individual audit findings, with little or no ongoing executive attention to systemic causes of control weaknesses. Since VA's CIO significantly strengthened central security management and planning in early 1999, improvements have been pursued within a risk management process.

VA's corporate security initiatives are funded from annual contributions from the Department's Administrations and the general operating expenditures account and managed by the Department-wide security function within the Office of Information and Technology. The program is embraced by a multi-year capital investment plan approved by VA's capital investment board in August 1999.

VA's information security initiatives respond to vulnerabilities reported by enterprise-wide cyber, personnel, and physical vulnerability assessments, as well as recent GAO and OIG audits. VA's initiatives were designed to address the six major security control categories used by GAO to measure agency programs. Efforts to date have been pursued from an enterprise-wide perspective, concentrating on areas where consistency and balance across the Department are essential.

VA's program uses a balanced-horizon approach. Through accelerated actions, VA's program seeks to gain the dramatic security improvements that can be immediate, require only modest labor by Department staff, and need little or no out-of-pocket expenditures. These initiatives include the major improvements that can be gained by adjusting simple computer configuration settings to comply with existing Department policies. Through long-range actions, VA's program seeks to gain the improvements that will come only after the execution of concentrated and sustained investments.

The following are some of VA's information security initiatives:

- Implement improved account management. The policy strengthened the minimum acceptable content of passwords, required improved account housekeeping, and better protected accounts with system administrator privileges. This policy was approved on January 21, 2000.

- Remove unsecured dial-in connections. This action is to implement the prohibition on all unsecured dial-in connections by employees, contractors, or other individuals with physical access. The prohibition was also established by the January 21, 2000 policy.

- Implement configuration standards for external electronic connections. All VA external electronic connections, such as Internet gateways, must incorporate the controls listed in VA Directive 6212, *Security of External Electronic Connections*, which was approved on September 21, 2000. The controls listed in the Directive are considered "the floor" for due diligence for such connections.

- Require incident reporting to the VA Critical Incident Response Capability (VA-CIRC) as a standard practice. All VA computer security incidents must be reported to VA-CIRC through the facility ISO.

- Correct personnel controls on system administrator staff. VA has completed a comprehensive review of staff positions that were coordinated with the Office of Personnel Management (OPM). As a result

of this review, we examined the security clearance status of incumbent staffs that have system administrator privileges. These staffs must receive a background investigation in accordance with VA regulation and commensurate to the position sensitivity designation.

- Achieve total workforce review of VA-standard awareness curriculum. An Intranet Web-based product is already available to all employees that fulfills the requirement for orientation and annual refreshment in security practices applicable to the average employee.

- Appoint Information Security Officers (ISOs). Every VA facility and office must staff a skilled and qualified ISO who works on information security activities full-time or at least as a primary duty.

- Implement enterprise-wide intrusion detection. This action will coordinate an effective and integrated enterprise-wide intrusion detection capability. The intrusion detection program will be integrated with VA's other standard security infrastructures as well as with VA's organization, policy, and business culture.

- Deploy enterprise-wide anti-virus regime. An enterprise-wide anti-virus regime will provide stronger protections against virus outbreaks. The regime will include services for product updates, reduce manual intervention to distribute and install product updates, automate policy setting, and provide for assurance reporting.

- Implement VA certification and accreditation program. This action will provide VA a formal program for certifying and accrediting general support systems and major applications.

- Implement VA's Public Key Infrastructure (VAPKI) capability. VAPKI must be completely operational to provide to employees and commercial trading partners certain security services (strong authentication, data integrity, and non-repudiation) for general support systems and major applications.

- Upgraded physical security procedures. This has included added metal detectors and X-ray devices at VA data centers and facilities. This also includes an initiative to coordinate physical and logical access safeguards using smart ID cards.

C. Federal Agencies

The following are reports provided by the Federal Agencies, in alphabetical order. Each Agency report begins with a section on internal CIP programs, followed by a discussion of external efforts.

1. Environmental Protection Agency

Internal CIP Activities

As required by PDD-63, the EPA made a determination that critical infrastructure assets existed at 16 locations. A vulnerability assessment was conducted at each location during 1999, which focused on physical security, IT security, telephone security and emergency response. Each location was then required to write a mitigation plan to correct those vulnerabilities found. The individual responses have been collated into an updated CIP plan, which is currently under internal review.

These vulnerability assessments consisted of a site visit by security experts and the use of commercial software to assess the information network system. Concurrent with this activity, the GAO conducted an

audit of EPA's information security program, which included operations at the National Computer Center, one of the Agency's critical infrastructure sites. Using readily available hacker tools, the GAO performed penetration tests on EPA's systems. The results are available in the report, *Information Security, Fundamental Weaknesses Place EPA Data and Operations at Risk*, GAO/AIMD-00-215, July 2000.

EPA's response to the GAO findings can be found starting on page 26 of that report. In summary, EPA has accelerated improvements to its IT infrastructure security. The EPA also developed a security action plan to implement IT security corrective actions over a period of time according to a priority based on the severity of the risk and the resources needed to mitigate the risk. Nearly all near-term corrective actions have been implemented as of November 30, 2000. Mid-term actions and the few remaining near-term actions are scheduled for the next six months. Long-term actions are scheduled beyond the mid-term planning horizon.

2. Federal Emergency Management Agency (FEMA)

Internal CIP Activities

Extending FEMA's information management services to its partners in emergency response provides a unique security challenge. The National Emergency Management Information system (NEMIS) is the cornerstone of FEMA's information management structure. NEMIS supports the mission by providing automation support to core emergency management functions and processes that must be performed by the government. These functions include providing emergency coordination of Federal, state and local response operations, disaster assistance for individual victims, support of public and mitigation programs for state and local government recovery efforts and field levels of operations. NEMIS builds on existing FEMA information technology network capabilities and replaces outdated disaster processing capabilities. NEMIS has capitalized on the inherent security features of the FEMA switched voice and data network, which include an enterprise approach to Intranet periphery using firewalls and dial-in controlled access. Next, the NEMIS access control system (NACS) provides role-based access controls (RBAC) to the various modules, as well as internal management controls by controlling access to various data, screens, tabs, and buttons. The senior management of the FEMA programs served by NEMIS have been heavily involved in the specification, review, and approval of this RBAC system.

For external access, NEMIS uses a double firewall approach, which secures the Intranet, but permits access to data within the area between the firewalls. NEMIS also is using a double firewall approach to support its interface with the Internet. A database server in the "demilitarized zone" (DMZ) between the firewalls is used to store a copy of data for access from the Internet or to receive input from an Internet user. Access to sensitive applications such as the Rapid Response Information System, the Weapons of Mass Destruction Database, and the Public Assistance Application will require the use of Secure Socket Layer (SSL) technology, including digital certificates for access. NEMIS is using the GSA administered Automated Certificates Enhancement System to acquire government-standard certificates. FEMA is the second Federal agency to sign up to use the GSA ACES program.

The FEMA Enterprise Security Management Team (ESMT) has provided review, guidance, and approval of all aspects of NEMIS external security -- from concept development through implementation. The EST has provided guidance to the NEMIS implementation team on best practices as identified by the CIAO, FedCIRC, and industry partners involved in the Critical Infrastructure Protection process. FEMA continues to capitalize on the cyber security focus of congressional committees and in the private sector. Using funds available through CIP initiatives, FEMA has been able to implement a program of system vulnerability testing and scanning. FEMA has contracted with NSA to conduct a three-phase testing and

evaluation program of all FEMA's critical systems. Phase one was completed in June of 2000. Lessons learned about systems vulnerabilities, policy, and procedure shortfalls are being addressed. Phases two and three are currently being scheduled based on NSA availability. During phases two and three, all FEMA critical systems will be evaluated for security both internally and externally. Additionally, FEMA has contracted with a private consulting firm to assist in the vulnerability analysis and security plan development of FEMA's 13 critical systems. Evaluations and plans for nine of those systems will be completed by January of 2001, with the additional four systems to be evaluated in a follow-on effort in FY 2001.

Historically, FEMA's critical infrastructure has been largely comprised of physically separated systems. As FEMA moves toward an open, collaborative computing environment with its partners and other agencies, these systems are increasingly dependent upon each other. Thus, the failure of one component in the infrastructure may cause a cascade of failure into one or more other components. For example, a breach in physical security may lead to theft of a critical server, or a breach through a cyber-based system could lead to a complete shutdown of environmental controls for an entire office. Therefore**,** FEMA will continue to evaluate the potential threats and risks and work to acquire the resources to protect our critical infrastructure.

3. General Services Administration

Internal CIP Activities

GSA has made important accomplishments in developing an internal information assurance plan. These include:

- GSA appointed a CIAO to be responsible for the protection of all aspects of GSA's critical infrastructure.

- Through GSA's CIAO, a CIP plan was developed to assure that GSA's critical infrastructure assets (both physical and cyber) were protected according to PDD-63 definitions.

- GSA developed and adopted a methodology to be used for the identification of GSA's most critical systems and facilities.

- The GSA CIAO is currently assuring that GSA's "most critical systems" are being identified and assigned a vulnerability assessment review to comply with PDD-63.

- The GSA CIAO has requested the preparation of corrective action/mitigation plans from each GSA service that has system vulnerabilities above an acceptable level of risk.

- The requested corrective action/mitigations plans are being prepared with the methodologies to reduce the vulnerabilities to an acceptable level of risk. The plans will also outline an approach to eliminate the systems' vulnerabilities permanently.
  - Corrective action/mitigation plans are required to identify necessary research and development requirements, and to provide a total cost analysis to support the mitigation process.
  - Corrective action/mitigation plans have been requested for submission to the GSA CIO no later than June 2001. These plans will be consolidated to produce an overall GSA remedial action plan to be submitted to the GSA's Administrator no later than September 30, 2001.

- The GSA CIAO cultivated GSA's awareness of Government-wide threats and vulnerabilities as they relate to the Federal Government's national requirements, and their relationships with the private sector.

- The GSA CIAO established vigorous, information-sharing networks through the development of the GSA CIAO and FedCIRC Web sites.

- The GSA CIAO established an electronic commerce network to assure quick and easy methods to obtain and share critical infrastructure media and memoranda.

- Established the FTS Safeguard Program to provide GSA and other departments and agencies a wide range of solution sets through Federal and industry partners, focusing on information assurance, vulnerability assessment methodologies, contingency planning techniques and/or research and development planning activities.

- Introduced the FTS enigma program to provide GSA and other Federal departments and agencies a "trusted neutral" to perform information security/vulnerability assessment services. Enigma provides the necessary services to examine the vulnerabilities of a customer's mission, organizational security program policies, and information systems. Enigma's goal is to determine the vulnerabilities of the Federal government's automated information systems, and recommend effective, low-cost countermeasures.

- The GSA CIAO hosted or participated in numerous infrastructure protection conferences, panels, informational seminars, roundtables, and sub-groups to promote Federal and private sector infrastructure protection.

Government-Wide Efforts: The Federal Computer Incident Response Capability (FedCIRC)

FedCIRC, operated by the General Services Administration (GSA), is the focal point for dealing with computer security related incidents that affect IT resources of the Federal Government. It is the hub of a virtual collaborative partnership comprised of computer incident response and security and law enforcement professionals working together to analyze and respond to events threatening the Federal computer network. FedCIRC provides both proactive and reactive security services for the civilian Agencies and Departments of the Federal Government, and is a source of information and guidance for the protection of the sensitive information and systems that form the electronic backbone of our nation's governing body.

The mission of the FedCIRC is to:

- Provide civil agencies with technical information, tools, methods, assistance, and guidance;
- Provide cross-agency liaison activities and analytical support;
- Influence industry to develop quality products and services through collaboration;
- Encourage responsible network management across government, and promote the highest security profile for government IT resources; and
- Promote incident response and handling procedural awareness within the Federal Government.

Sharing Information

The FedCIRC partnership consists of Federal incident response teams, law enforcement, the private sector, academia, and U.S. Government agencies responsible for securing the national information

infrastructure. Usually, FedCIRC establishes partnerships by memoranda of understanding that clearly define the relationships, roles, responsibilities, and reporting requirements of the participating parties. The FedCIRC and associated partners participate in a cooperative sharing of incident related information, statistics and trends.

Information reported to FedCIRC shall be used constructively to stage effective defenses of the information technologies and information within the Federal domain. The sharing of information is accomplished in a manner that does not open the reporting organization up to additional threat or exposure. Information shared with law enforcement entities, other than the reporting organization's Office of the Inspector General, will observe legal mandates and follow due process to ensure the preservation of Constitutional rights and freedoms.

Warning, Response and Recovery

FedCIRC alerts and advisories are categorized upon transmission according to the known or suspected severity of impact. Response action summaries from agencies and departments may be required contingent upon the prevailing threat. Responses follow the specified formats included with the alert notification.

Each incident is reported following a standard reporting process publicized by the FedCIRC. Providing the information cited in the reporting guideline enables FedCIRC to formulate an appropriate response and to aid in decision making for additional follow-up action.

The primary focus of incident response will always be the containment and recovery from an event affecting systems or network resources, but FedCIRC will cooperate with law enforcement officials involved in a legal investigation.

Strengthening the Operational Infrastructure

FedCIRC processes already in place for the incident response community fit well with the Federal and private sector information sharing partnerships for the protection of the nation's critical infrastructure.

To improve on current communications capabilities for the distribution of threat and vulnerability information, FedCIRC plans call for the implementation of two contingency options to augment the distribution of alert and protection information and to insure continued service during impairment of routine Internet dependent communications.

Installation of a high volume fax and voice message delivery system is planned for FY 2001. The system enables FedCIRC to deliver up to 800 voice or fax messages per hour to government Agencies and Departments should an event pose a threat to the information infrastructure. It would additionally eliminate the agency's dependence upon E-mail and Web service as the only delivery mechanism for alerts and protection information.

In the event of a catastrophic telecommunications failure where both network and telephone services were impaired or unavailable, FedCIRC plans also call for a low power radio broadcast facility that would service the metropolitan Washington area. This method would transmit alert and advisory information and would be used to increase awareness of threats to the infrastructure.

4. National Aeronautics & Space Administration (NASA)

Internal CIP Activities

NASA enters the next decade with a number of strategic initiatives that are highly dependent on having a robust and effective IT infrastructure.

To meet these requirements, NASA will spend nearly $2 billion on IT services and equipment in FY 2001, of which about five percent, or $101 million, will be devoted to IT security programs that are designed to improve system integrity and prevent vital data from being compromised. The $73 million increase in IT security spending in just two years reflects NASA's commitment to making IT security an integral part of all systems operated by the Agency for the next decade.

The concerted effort to improve IT security has been framed by several audits: a 1998 internal review by Agency staff, several OIG audits, and a 1999 report by the GAO. The evaluations concluded that significant improvements were needed to counteract the threat to critical systems. NASA responded vigorously to the recommendations during 1999 and the first half of 2000 with an aggressive program to remedy deficiencies as quickly as possible. The IT security objectives that were established include:

- Improving adherence to Agency IT security policy;
- Reducing system and application vulnerabilities;
- Improving intrusion monitoring, reporting, and response;
- Achieving a trained workforce of users, managers, system administrators, and network administrators; and
- Improving mechanisms for user authentication and data protection.

The following activities were initiated:

- The position of Deputy CIO for IT security was established and filled;
- A comprehensive set of policy directives and technological improvements was put in place;
- A NASA-wide IT Security Council was established to involve senior managers in major issues;
- An Agency-wide system of incident reporting was implemented to track and reduce vulnerabilities;
- An ambitious training program was established and made available to all NASA employees on a secure Internet site;
- Network monitoring tools and encryption products were procured as part of the new vulnerability reduction program; and
- IT security planning was made a key component of computer systems development activities.

The metrics that were devised to measure progress on these initiatives show that the approach is succeeding and that IT security has improved significantly. Examples of success include:

- The percentage of hostile probes that result in successful system compromise has dropped steeply from eleven percent at the beginning of 1999 to two percent at present;
- The goal of providing basic IT security training to eighty percent of civil service personnel will be reached in calendar year 2000;
- IT security plans are now in place for 90 percent of NASA's special management attention systems, and a commitment has been made to senior management to complete the remaining plans by the end of calendar year 2000;
- Occurrence of specific vulnerabilities on NASA systems was reduced to less than 0.25 vulnerabilities per system; and

- A uniform PKI capability will be fully deployed to all NASA Centers in FY 2001.

A panel of experts identified the vulnerabilities, and selected scanning tools are being used to detect the vulnerabilities. Approximately 85,000 systems were scanned.

While major progress in addressing the concerns raised in the audits has been made, NASA plans to move promptly and forcefully to accomplish further improvements. Examples of such improvements include:

- The vulnerability ratio goal of 0.25 (ratio of system vulnerabilities detected to systems scanned) for FY 2000 will be further reduced in FY 2001 and FY 2002;
- Training requirements will be expanded to include managers and system administrators;
- IT security plans will be implemented for all NASA computer systems containing sensitive information;
- Key PKI applications for secure messaging and file encryption will be deployed; and
- IT security technology will be updated to strengthen local user access procedures and deal with potential incidents.

NASA's broad mission ensures that its IT security requirements will remain complex. The Agency must maintain a constant and extensive interface with industries and academic institutions that are conducting research and providing access to U.S. and foreign nationals who are seeking public information on NASA projects and accommodate contractors who must have access to critical systems. NASA also must sustain links to sites such as its Control Center in Moscow, offices in Paris and Madrid, and other sensitive facilities worldwide. These circumstances produce a complex environment in which NASA must balance public demand against Internet-based threats without eroding its ability to support vital operations. To achieve an acceptable level of security under such conditions will not be easy, and NASA recognizes that the significant improvements it has made in the past two years must be followed by a focused, ongoing effort. The IT security program has positioned the Agency to meet this challenge.

5. National Science Foundation

Internal CIP Activities

The National Science Foundation, created in 1950, makes merit-based grants and cooperative agreements and provides other forms of support to educators.

The National Science Foundation has made significant progress in CIP over the past year. The NSF has a variety of security practices in place to mitigate risk to agency systems including those accessible via the Internet. To ensure that a verification of risk assessment for NSF's mission critical systems processing sensitive but unclassified information, the NSF's OIG conducts a comprehensive internal audit of IT controls annually as part of the financial accounting audit.

In compliance with the Clinger-Cohen Act, any new system applications are developed to fit the agency-wide IT architecture that implements risk management into the system life cycle. These security structure and controls include the implementation of strong authentication for network applications.

All NSF employees have access to the Internet from the LAN-attached desktop PC. Most use of the Internet by NSF employees is for e-mail or for web access, which is protected by an in-depth Firewall Team. This group, which includes a newly appointed Director, ADP Security, and individuals responsible for NSF's firewall, Internet connection, LAN support, e-mail support and systems administration. Key members of the Firewall team receive FedCIRC and CERT alerts and are on other

security-related mailing lists. The Firewall team handles reports of problems using the firewall, as well as requests for special connection through the firewall.

In order for NSF to improve its ability to defend its computer systems, the NSF has an active vulnerability-scanning program in place and is in the process of deploying an extensive intrusion detection-monitoring program for all NSF networks.

NSF continues to have an active virus-scanning program in place. During the Melissa Virus incident in March 2000, the incident response team, in cooperation with FedCIRC, was able to quickly assess the threat, develop a defensive strategy, and direct appropriate defensive actions. Again, in May 2000, the LOVELETTER virus provided another example of the NSF's incident response team's rapid action. The team quickly identified the potential damage and provided rapid notification to staff and business partners.

The NSF has established a computer security awareness program for all NSF employees. In 2001 the Department of Defense training team will conduct a comprehensive education, training and awareness program for all systems administrators. In addition, all NSF staff and contract employees are required to attend security awareness briefings in accordance with the Computer Security Act of 1987 (Public Law 100-235).

In cooperation with NSF's OIG, an NSF computer incident response team was established in 2000. All procedures to follow if an intrusion is detected on a NSF system are in place. These include actions to isolate the affected machine, save information for evidence of the intrusion, and notify IT management as well as the OIG. In addition, these procedures address how to correct the problem and restore to normal operations.

The Agency's Director for ADP Security focuses on the overall network security architecture and how it's implemented into the agency infrastructure. With this newly appointed position, NSF has geared up security policies focusing on remote access, firewall implementation, intrusion detection, penetration testing, vulnerability assessments and overall security awareness.

6. National Security Agency

Internal CIP Activities

NSA has conducted numerous vulnerability and risk assessments of its infrastructures and has invested in a modernization of its information infrastructure that will assure critical assets and functions are properly protected. Specific accomplishments over the past 18 months include:

- Appointing a CIAO;
- Developing a CIP Plan which includes investment decisions based on the security evaluation of facilities, telephone systems, and information systems;
- Defining three levels of criticality for its systems;
- Using Y2K and continuity of operations plans to determine which systems fell into each level of criticality;
- Investigating several risk assessment techniques and selecting an appropriate one for use within NSA;
- Performing risk assessments of the most critical assets;
- Conducting briefings for field representatives to facilitate assessments at field sites; and
- Implementing the NSA Information Systems Incident Response Team.

Government-wide Efforts

The NSA has the responsibility, via its technical capabilities and expertise, to assist Federal Agencies in their CIP efforts. The Information System Security Organization (ISSO) has several initiatives, which can be used as excellent examples for other agencies and the private sector to model or build upon for development of their CIP programs.

The NSA/ISSO regularly supports DOD and Federal Government customers through a "crawl, walk, run" process focusing on INFOSEC and OPSEC assessments, network evaluations, and RED Teaming. NSA/ISSO has provided over 30 combined assessments and Red Team operations to DOD organizations and about 20 to other Federal Agencies when requested by the agencies. In addition, over 30 OPSEC training classes have been provided to Federal Agencies through the interagency OPSEC Support Staff.

An interagency working group, called the Federal Security Practices Subcommittee, was established as a sub-committee of the CIO Council's Committee on Security, Privacy and Critical Infrastructure. NSA provides support to the sub-committee and has senior representation on the CIO Council's Committee on Security, Privacy, and Critical Infrastructure.

NSA continues to advise and assist GSA, DOD, and OMB in the development of procurement regulations, particularly as they apply to Information Assurance-related CIA procurements. With regard to the acquisition of IA products, NSA has worked with the National Security Telecommunications and Information Systems Security Committee (NSTISSC) to promulgate NSTISSP 11, National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products." NSTISSP 11 establishes policy regarding the acquisition of evaluated COTS and GOTS products (IA and IA-Enabled) that are to be used in national security telecommunications and information systems, as defined in National Security Directive 42, July 1990.

NSA's National Security Incident Response Center (NSIRC) continues to provide expert assistance to the DOD JTF-CND, DISA, FedCIRC and NIPC in isolating, containing, and resolving attacks and intrusions threatening national security systems. NSA also supports the NIPC with analysis of data from specific incidents. In June 2000, NSA developed of Cyber "Critic" Messaging guidelines. These guidelines define the conditions under which information of cyber attacks can be distributed through the Critic network to National Security consumers. In May 2000, a Defense Red Switch Network telephone was installed in the National Security Operations Center, which enhances connectivity to DOD components for cyber events.

The NSA National Centers of Academic Excellence in Information Assurance Education is a program, which encourages universities to examine their information assurance curricula as well as campus IA posture, against a set of national standards. Applications are received from those universities having the most mature IA/ INFOSEC education programs. Part of the criteria used in judging applicants are a set of national training standards developed originally for use within the classified community. There are currently fourteen designated centers. The call for the next set of applications began September 30, 2000, and culminates in May 2001.

The National INFOSEC Education and Training Program (NIETP) provides national leadership in the IA community. The NIETP, cited in the *National Plan* as a model for the nation, offers a variety of products and services in IA education and training.

The NSTISSC serves as the senior policy making body for IA in the classified community. This group has spearheaded the development and ratification of training standards for key personnel in the IA arena.

The standards serve as focal points for training and education development within the Federal government as well as the broader academic community. Related to these standards is the Information Assurance Courseware Evaluation Program, which seeks to validate that courses of instruction offered by schools and commercial vendors meet the criteria of the NSTISSC training and education standards. Having these certified programs of instruction available will bring much needed standardization and quality in IA training to the greater Federal as well as commercial communities.

To further its goals to improve education and training, NSA, working with leaders in academic and business arenas, convened the first national Colloquium for Information Security Education in the spring 1997. This forum brought together industry, academia and government to discuss national education requirements and solutions for meeting our nation's need for increased numbers of professionals educated in information assurance. In May 2000, the CIAO hosted the fourth meeting. This gathering of representatives and stakeholders is producing sharing of courseware, and defining requirements in the IA arena.

NSA's Information Assurance Research Office (IARO) conducts a comprehensive research program in the technologies and techniques needed for the development of future high-assurance solutions and defensive information operations tools. Specific research areas include active network defense, cryptography, secure network management, switched network security, secure distributed computing, and identification and authentication.

A detailed description of NSA CIP activities is in Appendix A.

7. Nuclear Regulatory Commission

Internal CIP Activities

The Nuclear Regulatory Commission (NRC) is proceeding with the work necessary to support PDD-63. The CIP Plan will be updated in 2001.

In support of PDD-63, the NRC computer security staff initiated an independent survey of the NRC wide area network to test and evaluate network in-place security controls. A report was prepared that included findings, conclusions, and recommendations. It was concluded that the NRC network is well protected from the outside by its firewalls.

A separate vulnerability study was initiated for those systems identified as critical infrastructure in the NRC operations center. The operations center is the focal point for the NRC's response to emergencies and contains a majority of the NRC's critical infrastructure. This study will be completed early in calendar year 2001. All recommendations will be evaluated and implemented, where appropriate, by the PDD-63 imposed deadline of March 2003.

Although the focus of PDD 63 is on cyber systems, the physical security of facilities must also be considered. NRC has a comprehensive, "in-depth" physical security program to protect its personnel, information, and assets. NRC is in general compliance with physical security measures outlined in the DOJ Federal Marshall's Study to counter terrorism and other national level physical security initiatives. To reduce the "insider threat," a background investigation, appropriate to the information sensitivity or system access required, is conducted on all NRC and contractor employees afforded unescorted building access. Additionally, physical access to network switches, hubs and infrastructure computers is further limited to authorized individuals through the use of card readers and combination lock mechanisms. NRC

continually assesses and adjusts its physical security program and measures (i.e., guard patrols and access control procedures) based on the general Federal Government posture and agency specific situations.

8. Social Security Administration

Internal CIP Activities

The Social Security Administration (SSA) is the main repository for personal employment information used to determine eligibility for Social Security retirement, survivor, and disability benefits. It also handles the Supplemental Security Income program and much tax information for the Internal Revenue Service, Medicare/Medicaid information for the Health Care Finance Administration, Black Lung information for the Department of Labor, and other data which affects eligibility for many state/Federal programs ranging from Food Stamps for the Department of Agriculture to housing subsidies for HUD. All of this information is personal and confidential, and almost all is dependent on SSA information technology systems.

Confidentiality has always been paramount at SSA. Our very first regulation required that the data we collect be kept confidential. It is natural that security of our cyber and physical assets be equally important since they protect our data. In October 1999 the SSA CIO determined that SSA should begin to establish a CIP plan. The CIP work group was established in October 1999.

The national CIAO provided training and advice on using the new Project Matrix approach to define and document SSA's physical and cyber assets. The SSA CIP work group used the CIAO questionnaire to define our assets and specify the most critical. Using the list of critical assets in priority order, the work group examined the products of previous physical and cyber reviews, including audits, to determine which previous efforts, if any, met the rigorous criteria of PDD-63 vulnerability analyses. The PDD-63 vulnerability analysis program was begun in FY 2000 with the award of contracts for one new analysis and the modification of three planned reviews, which were significantly expanded to meet the PDD-63 standard.

The contracts are structured so that any significant problems identified during the analyses will be addressed immediately. At the conclusion of each contract, all areas of potential security improvement will be identified, along with a proposed range of enhancements. The CIP work group will present these findings to SSA executive management for review and selection of a course of action. All findings will be tracked until the chosen remediation is in effect.

As part of the first step in the CIAO Project Matrix, SSA is planning for a minimum of two vulnerability analyses per year until all critical assets have been addressed. SSA is also undertaking the Step Two analysis of a minimum of two critical assets this fiscal year. These future analyses will concentrate on information and support dependencies, where organizations are dependent on SSA, and where SSA is dependent upon other organizations for support, including data received, computer systems support, and utility services.

Attached is an Appendix that contains details about SSA's planning to establish a Critical Infrastructure Protection Plan, including the timeline in which the planning occurred. Also included in the Appendix is the current status of SSA's plan, broken down into the ten program areas identified in the *National Plan*.

D. Best Practices and Standards

1. Office of Management and Budget (OMB): Integrating Security into the Capital Planning and Budget Processes

In February 2000, OMB issued important new guidance to the agencies on incorporating and funding security in information technology investments. In brief, this policy states that funding will not be provided for agency requests that fail to demonstrate how security is built into and funded as part of each system.

This policy carries through on the requirements of the Clinger-Cohen Act of 1996 and emphasizes that security must be incorporated into and practiced throughout the life cycle of each agency system and program. To accomplish this, beginning with the FY 2002 budget, each agency budget request to OMB for information technology funding must, among other things:

- Demonstrate life cycle security costs for each system;
- Include a security plan that complies with applicable policy;
- Show specific methods used to ensure that risks are understood, continually assessed, and effectively controlled; and
- Demonstrate that security is an integral part of the agency's enterprise architecture including interdependencies and interrelationships.

New Legislation

On October 30, 2000 the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform (Security Act)." The security provision amends the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35) and primarily addresses the program management and program evaluation aspects of security.

Like OMB policy, the Security Act requires agencies to incorporate and practice risk-based and cost-effective security throughout the life cycle of each agency system and thus firmly ties security to the agencies' capital planning and budget processes.

The Security Act also requires annual:

- Agency program reviews;
- Inspector General evaluations of agency security programs;
- Agency reports to OMB; and
- OMB report to Congress.

The annual review and reporting requirements will promote consistent, ongoing assessments of government security performance. Below, the discussion of the accomplishments of the Chief Information Officer's Council describes a recently developed uniform method for agency program reviews.

The CIO and CFO Councils: Standards And Best Practices

Standardizing the security controls for government systems has a conceptual appeal because it can reduce the complexity and expense of developing, implementing, and monitoring security on a system-by-system basis. This is increasingly important given the government's shortage of expert information security

personnel. Government computer security would almost certainly improve if specific standards were prescribed and implemented for each government information system.

However, specific standards for all systems -- a one-size-fits-all security approach -- may not accommodate the vastly different operational requirements of each information system and could unnecessarily impede business operations. Executive branch agencies operate more than 26,000 major information systems, many of which directly interact with the public, industry, or State and local governments. Just as each system has its own unique operational requirements, so too are its security requirements.

CIO and Chief Financial Officer's (CFO) Council

The CIO Council and the CFO Council recognize both the benefits and potential problems with standardized security approaches.

In addition to sponsoring or co-sponsoring five security conferences this past year, the CIO and CFO Council are working together to promote strong agency system security practices while maintaining operational flexibility. They have undertaken the following important initiatives:

Security Benchmark for Agency Financial Systems

The CFO Council is reviewing the viability of establishing a security benchmark or standard security expectation for agency financial systems.

Securing Electronic Government Transactions to the Public – Resource Guide

The CIO Council, the CFO Council, and the Information Technology Association of America are working together to develop a benchmark for risk-based, cost-effective security for three types of electronic government services:

- Web-based information services;
- Government procurement; and
- Financial transactions with the public.

A resource guide for securing electronic transactions with the public will be released in early 2001 to assist agency CIOs in promoting electronic government initiatives within their agency. Together with the CFO Council initiative for agency financial systems, this effort may prove to be an effective pilot for establishing similar benchmarks for other discrete classes of programs and information systems.

Best Security Practices

The CIO Council, led by the U.S. Agency for International Development and NIST, has developed a web-based repository (http://bsp.cio.gov) of sound Federal agency security practices that have worked in the real world. The CIO Council's Best Security Practices initiative collects, documents, and disseminates these practices to help agencies reduce the cost of developing and testing new security controls, improve the speed of implementation, and increase the quality of their security programs.

The goal is to populate the repository with more than 100 practices by mid 2001 and continually expand offerings from then on. In their guidance to the agencies on implementing the Government Information

Security Reform Act, OMB has instructed agencies to use the CIO Council best practices initiative to fulfill the new act's requirement to share best practices.

Sample Policies

Complimenting the benchmarking and best practices initiatives, the CIO Council is also identifying model policies for agency use. Two policies have recently been distributed:

- NIST developed *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*. This document provides suggestions to agencies when acquiring security-related information technology products.
- Internal Revenue Service developed *Model Information Technology Privacy Impact Assessment.* The Council found this to be a best practice for evaluating privacy needs of and risks to personal and financial data in government information systems.

Measuring Performance -- Federal Information Technology Security Assessment Framework

A well-known computer security expert, Robert Courtney, once said, "Good security is the ultimate non-event." In that phrase he summarized the difficulty in measuring effective security.

Over the past year, the CIO Council, working with NIST, OMB, and the GAO developed the Federal Information Technology Security Assessment Framework. The framework, issued in December 2000, provides agencies with a self-assessment methodology to determine the current status of their security programs and, where necessary, establish a target for improvement. The framework is based upon requirements found in OMB's security policies, GAO's Federal Information Systems Controls Audit Manual, and NIST's security guidance. In developing the framework, the CIO Council recognizes that the security needs for the tens of thousands of Federal information systems differ and must be addressed in different ways.

The framework comprises five levels to guide agency self assessments and to assist them in prioritizing efforts for improvement:

- Level 1 reflects a documented security policy;
- Level 2 shows documented procedures and controls to implement the policy;
- Level 3 indicates that the procedures and controls have in fact been implemented;
- Level 4 shows that the procedures and controls are continually tested and reviewed; and
- Level 5 demonstrates that procedures and controls are fully integrated into a comprehensive program.

Each level represents a more complete and effective security program and agencies should bring all systems and programs to level 4 and ultimately level 5. OMB and the CIO Council have alerted agencies that when individual systems do not meet the framework's level 4, the system may not meet OMB's security funding criteria.

As mentioned earlier, the new Government Information Security Reform Act emphasizes the importance of assessing security effectiveness and requires annual agency reporting to OMB of the results of the agency security reviews. OMB has instructed agencies to use the framework to fulfill their assessment and reporting obligations under the Security Act.

Outreach and Awareness

Successful security programs require sustained senior management support. Maintaining this senior-level support is a goal of a CIO Council sponsored bi-monthly newsletter being published by NIST. The newsletter highlights for CIOs and other agency executives security issues of special significance.

During FY 2001, the CIO Council plans the following initiatives in the areas of security, privacy and critical infrastructure protection:

- Develop with NIST a model risk management program;
- Develop funding strategies for PDD-63 activities;
- Develop guidelines for agencies to meet the PDD-63 requirements;
- Promote the privacy impact assessments for Federal information systems;
- Develop sample policies for privacy and security;
- Sponsor and promote workshops and conferences; and
- Assist the FedCIRC in providing early warning of security incidents and otherwise support FedCIRC's operations.

2. National Institute of Standards & Technology

Critical Information Infrastructure Protection (CIIP) Grants Program

For FY 2001, Congress provided funds for a CIIP Grants Program as a new $5 million initiative for NIST.

The specific focus of the CIIP program is to address critical information infrastructure protection security concerns that are not being adequately addressed elsewhere. Failure to adopt effective infrastructure protection technologies means that vulnerabilities in the nation's information infrastructure will persist. The objectives of this program are:

- An improvement in the scientific and technological basis for infrastructure protection;
- An improvement in the robustness, resilience, and security of the communication and information infrastructure;
- New hardware and software tools and components for the design, construction, and evaluation of security enforcing systems; and
- The start of a technology base of advanced testing and evaluation techniques focused on key security infrastructure components and systems.

The objectives of the program may be achieved through enhancement of system architectures to improve system survivability, allow graceful degradations under stress, and ease reconstitution following failures – whether due to attacks, natural disasters, or human error.

Federal Computer Security Program Managers' Forum

The Federal Computer Security Program Managers' Forum is an informal government interagency group, organized and chaired by NIST, that meets every two months to exchange information on computer security matters, and to identify and resolve security issues related to the development and application of new and emerging information technologies.

Security Practices

Information sharing on matters relating to security can prevent duplication of effort and lead to faster and cheaper solutions. In March 2000, the Security Subcommittee of the CIO Council established a Web site (http://bsp.cio.gov) hosted by the GSA, to promulgate best security practices. The objective is to provide an easily accessible and useful source of information to Federal employees on effective existing security tools and practices. GSA and NIST review all submissions before they are placed on the Web site.

Expert Review Team

The nation is at risk from disruptions of critical government IT services due to natural disasters, human error, equipment failures, and purposeful attack- including both cyber-terrorism and physical attacks. PDD-63 and guidance issued by the OMB require that Federal agencies identify and fix existing vulnerabilities in their information systems. An initiative to establish an Expert Review Team to assist Federal agencies in protecting their critical IT systems has been submitted to the Congress. Five million dollars have been requested in order to establish an eight- member team at NIST. The initiative includes a one-time operational fund of three million dollars to help agencies fix their most pressing security vulnerabilities.

NIST Standards and Guidance

NIST issues Federal information processing standards when there are compelling Federal government requirements and no acceptable industry standards or solutions. For example, NIST has been working with industry and the cryptographic community to develop an Advanced Encryption Standard (AES) that specifies an encryption algorithm(s) capable of protecting sensitive government information well into the twenty-first century. NIST announced its selection of the proposed AES algorithm (developed in Belgium and called Rijndael) in October 2000 and will soon be publishing the proposed draft for public comment. Expectations are that the standard will be adopted in spring 2001.

NIST issues special publications which provide comprehensive guidance on security matters (e.g., how to develop an effective organizational security policy) and issues *Information Technology Laboratory (ITL)* bulletins which provide the security community in-depth guidance on topics such as intrusion detection systems, operating system security, computer vulnerabilities, and trends in hacking.

NIST is developing a cryptographic toolkit that defines approved algorithms for encryption, digital signature, and hashing and key management.

A list of current FIPS, NIST special publications, ITL bulletins and the cryptographic toolkit can be found at http://csrc.ncsl.nist.gov.

The Computer Security Resource Center

The NIST Computer Security Division operates and maintains a Web site that contains information about computer security issues, products and research of interest to the computer security and IT community. The Computer Security Resource Center can be accessed at http://csrc.ncsl.nist.gov.

Cryptographic Module Validation Program

NIST established the cryptographic module validation program (CMVP) on July 17, 1995 to validate cryptographic modules to security requirements for cryptographic modules, and other cryptography based

standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 are accepted by the Federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are five National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-1 compliance testing, four in the U.S. and one in Canada. As of December 2000 over 125 validation certificates have been issued through the program. The certificates actually represent nearly 150 separate cryptographic modules from more than forty different vendors. The number of validated modules has nearly doubled each year of the program's existence.

3. The National Information Assurance Partnership (NIAP)

NIST and NSA have jointly established the National Information Assurance Partnership (NIAP), a security testing and evaluation program that promotes the development and use of security-enhanced IT products and systems.

The NIAP is collaboration between NIST and NSA designed to meet the security testing needs of IT producers and consumers. The long-term goal of NIAP is to increase the level of trust consumers have in their systems and networks through the use of cost-effective testing/evaluation and validation programs. To support this goal, NIAP has focused its activities in three key areas:

- Product and system security testing/evaluation and validation;
- Security requirements definition and specification; and
- IA research in security testing, evaluation and metrics.

4. Intelligence Issues

The Foreign Intelligence Community's Role in the Protection of our Nation's Infrastructure

The U.S. Intelligence Community (IC) is composed of thirteen independent intelligence organizations. It operates collectively under the leadership of the Director of Central Intelligence and is charged with acquiring information on foreign elements (e.g. rogue states, terrorist groups) that threaten the nation's infrastructure. Information is collected on their leaders, political agendas, financial supporters, capabilities to employ violence, and intentions. That information is then provided to our national leadership and those responsible for the protection of the nation's infrastructure. The community's goal is to provide information on impending attacks with such timeliness and certainty that action can be taken to thwart them before they do damage.

Progress Toward Developing an Information Assurance Plan

The IC CIO in 1999 formulated a "roadmap" for the development and employment of information technology within the Intelligence Community. Among other things, it prescribed improvements to the community's information assurance posture. In large part, those paralleled milestones established by the *National Plan for Information Systems Protection*. Those objectives included:

- Implementing a public key infrastructure for the community to improve the security of its communications.

- Establishing policy governing the configuration and operation of electronic connections among networks operating at different classification levels.
- Selectively restricting the use of "mobile code" executable computer instructions that can be transmitted by e-mail.
- Fostering the use of audit and analysis technology–automated means of identifying possibly illegal or improper use of information services.
- Establishing a computer incident response center to:
  - Identify intrusions, attacks, or outages;
  - Limit their damage; and
  - Warn others of the problem.
- Assuring that the community has the information services it needs to sustain its critical missions in an emergency. A working group has been established to coordinate that work.
- Conduct assessments of the Intelligence community's information assurance posture. The assessment is performed by a group of senior officers from throughout the community that specialize in information security.
- This year the assessment concluded that – given the known threat and the level of resources available for this purpose -- the community' information services are reasonably secure, but recognized that new problems can arise suddenly. It counseled that information assurance be conducted as a process, not an end.

Working with his counterpart CIOs from the member agencies of the community, the IC CIO regularly reviews the progress being made against each of these objectives. They have collectively judged that progress against each is satisfactory.

IV. Education and Training

IV. Education and Training

Federal Cyber Services (FCS)

Information security/assurance education and training makes good business sense. It provides cost avoidance that could be caused through loss of program productivity, reconstitution of system and data, loss of stakeholder confidence, lower staff morale, and management reaction to additional intrusion attempts. As importantly, the value of due diligence provides program operational survivability, stakeholder confidence, data integrity, higher morale and staff retention.

The *National Plan for Information Systems Protection* announced a new Federal program aimed at addressing the shortage of skilled information assurance/information technology (IA/IT) professionals. The Federal Cyber Services (FCS) training and education initiative is designed to ensure an adequate supply of highly skilled Federal information systems security specialists.

The FCS initiative encompasses five broad programs that will identify 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 information systems personnel shortfall is documented by numerous sources, and the nation's reliance on information systems capability is critical to our economic growth.

The FY2001 budget for the FCS civilian program is contained within the National Science Foundation (NSF) and the Office of Personnel Management's (OPM) appropriations. Program planning and coordination within the Federal government is ongoing with the CICG, the CIO Council, the Chief Financial Officers Council, the Human Resource Technology Council, and agencies. Partnership opportunities with industry, non-profit organizations, states, and other professional groups are being initiated.

In addition to the NSF budget request, the National Defense Authorization Act for FY2001 includes a provision authorizing DOD to conduct a program similar to the FCS. This authorization bill includes $20 million for the scholarship program, with a portion of the funds providing financial assistance to build university programs.

OPM Information Technology Occupational Study

One cornerstone of the FCS program, the *OPM IT Occupational Study*, is nearing completion. OPM has issued a Draft Job Family Position Classification Standard for Administrative Work in the Information Technology Group, GS-2200A. (The GS-2200 is a new occupational group for information technology occupations replacing the 0334 occupation series as well as some positions in other series where IT knowledge is paramount.) One of the 11 classification specialty titles in the new guide covers Information Systems Security Specialists, who are estimated at four percent of the current Federal IT workforce. [1] OPM is now conducting a study to validate the competency profiles through a government-wide survey of 22,000 IT employees and supervisors.

[1] Federal IT workforce statistics compiled by OPM: Customer Support positions 14%; Communication and Network services 10%; Data Management 10%; Information Systems Security Specialists 4%, Policy, Planning and

Compilation of agency information gathered by OPM, through close coordination between agencies'[1] IT and human resources staff, shows that Federal IT specialists are an aging workforce. Thirty-five percent of the identified IT workers are over 50 years old, while 52 percent are between 36 and 49. Only 13 percent of the Federal IT workforce is less than 36 years old. With the rapid rate of change within technology, much more attention must be placed on recruitment, retraining, and retaining these workers. OPM estimates show that Federal civilian agencies alone will need to hire 37,000 IT workers over the next six years. The Department of Defense (DOD) employs 43 percent of Federal IT staff, therefore the DOD recruitment need will almost match that of the civilian agencies.

OPM is using the raw data from their study, as well as that developed by the National Security Agency and the National Security Telecommunications and Information Systems Security Committee (NSTISSC) composed of 21 Federal agencies, to develop competency based job profiles for IT personnel including security specialists. The competencies identified for security specialists will become the basis for the Centers for Information Technology (training) Excellence program within FCS. Additionally, OPM has added specific information security competency factors to the competency requirements of all Federal IT positions within the new classification standards.

OPM is using agency ranking and staffing data to review differences in recruitment and retention problems by specialty or work level category (e.g. entry/developmental, full performance, supervisory/managerial position), as well as geographical area. This data will assist OPM in determining additional pay flexibility and/or an IT compensation system to assist agencies to recruit and retain IT employees. As of January 2001 OPM has authorized a special pay rate for IT workers through grade 12. Agencies are currently offering hiring and retention bonuses in order to recruit and retain IT workers.

Scholarship for Service (SFS)

Scholarship for Service, the second of the FCS initiatives, was funded for the first time in FY2001 ($11.2 million). This program will address the shortage of IA/IT professionals by establishing a pipeline for training and recruitment. Specifically, it will provide participants with up to two years of tuition and fees for information security education in exchange for an equal amount of service to the federal government. It will also provide support for faculty and institutional development to increase the number of educational institutions qualified to offer SFS opportunities. The NSF and the OPM are jointly administering SFS. The review of university grant proposals is in progress, with university awards to be announced in spring 2001. The first cohort of SFS students will begin studies in fall 2001.

NSF has developed and coordinated with the CICG the application requirements and project design for the SFS grant program. The NSF Board of Directors approved the SFS program and management plans, and the program announcement is completed. Three tracks are included in the SFS program announcement: student scholarships, faculty development and facility development. Collectively these tracks will assist the development of a strong cyber security program at numerous colleges and universities.

Management 10%; Software Engineering Applications 18%; Software Engineering Systems 6%; Systems Administrators 10%; Systems Analysts 9%; Web Developers 2%; General 5%; unclassified 2%.

[1] OPM received reports from 38 agencies plus the President's Council on Integrity and Efficiency, representing agency Office of Inspect General. Approximately 90% of the actual Federal IT workforce is included in the reports.

The SFS start-up funding in the FY2001 budget provides two-year scholarships for up to 100 M.S. candidates or two-year scholarships for promising juniors and seniors working towards a B.S. in an accredited information security program. The target for the program is to produce 300 bachelors and/or masters' degree graduates annually with an emphasis in information security. Other benefits to the program will be outreach to under-represented and economically disadvantaged students, an increase in the information security expertise in academia, support for continuing education, and support for R&D at universities.

University outreach will be conducted through NSF's normal grant proposal process, direct contact with the fourteen universities recognized by NSA as Centers of Excellence in Information Assurance Education, direct contact with the participants in the FY2000 National Colloquium for Information Systems Security Education (Colloquium), and direct contact with all other schools who have inquired to NSF about the grant program to date.

Center of IT (Training) Excellence (CITE)

The third program within the FCS initiative is the *Center of IT (Training) Excellence* (CITE) for information security skills. The CITE will provide high-caliber, cutting-edge information security training and certification for current Federal IT security employees, Federal contractors, and FCS candidates. The CITE is conceived as a virtual, nationwide network of "recognized" public and private training centers that meet information security competencies defined by OPM and based on OPM, NSF, NSTISSC, CIO Council, industry, and other requirements. These competencies will be part of OPM's IT Occupational Survey, to be completed spring 2001, and will be used as the basis for development of the competency requirements for security positions. Initial development of the CITE will focus on providing training for Systems Administrators and Information Systems Security Officers (ISSOs).

A proposed project plan for the CITE program was developed. Multiple forms of training delivery are included in order to provide high-caliber, cutting-edge information security training any time, any place, to maintain technical skills within Agencies current with the state-of-the-art technology development, and to provide growth for current Federal information security professionals.

Identified in the *National Plan*, the issue of employee certification has not been resolved at this time. Employee certification is actively encouraged at Federal agencies, some of which are paying bonuses to workers with such official skills recognition. A Federal-wide policy mandating certification of workers has not been adopted. However, four universities are experimenting with inclusion of the SANS education/certification programs as part of their undergraduate and graduate programs in FY2001. SANS education/certification programs require both testing and practical work.

High School and Secondary School Awareness and Outreach Program

The fourth program in the FCS initiative, the *High School and Secondary School Awareness and Outreach Program*, has a large, future payback for the nation. Outreach to high schools and secondary schools will ultimately expand information security awareness into homes and communities. Numerous programs have begun to address this issue, with industry taking the lead. Programs are being developed to increase awareness of the vulnerability of information systems and institute a cyber ethics curriculum for high school and secondary schools. In order for these programs to be successful, they provide teaching standards in computer security practices and ethics.

The National Academy Foundation (NAF)[1] launched a new Academy of Information Technology (AoIT). The program will prepare high school students for careers in IT fields. AoIT will provide ninth through twelfth grade curriculum, with opportunities to partner with community colleges, universities, and businesses. Twelve pilot sites were chosen for implementation in fall 2000, to reach a total of 350 to 400 students. In fall 2001, 40 new schools will be added, with an increase of 40 to 50 per year depending on full industry support.

The Department of Justice, through the Information Technology Association of America, initiated the Cyber Citizen program to raise security awareness and teach cyber ethics. Also, the Defense Information Systems Agency (DISA) has met with many agencies and non-profit organizations offering their security awareness materials, especially the Cyber Protect "game" they developed to simulate practical application of security techniques. The Department of Commerce is partnering in a national media campaign to promote a positive image of technical jobs. This campaign was launched this fall in connection with the second annual National Techies Day on October 3.

Federal Information Assurance Awareness Campaign

The fifth program in the FCS initiative, the *Federal Information Assurance Awareness Campaign*, is designed to ensure that all IT systems users are aware of security threats, their personal responsibilities to deter threats, and the security practices that will help safeguard critical information. The CIO Council conducted a Critical Infrastructure Protection (CIP) Day to foster increased emphasis on CIP. In addition, the CIO Council determined that most agencies need updated training materials. Activities have focused on sharing materials or, in some cases customizing quality programs from DISA. The Federal Information Systems Security Educators Association (FISSEA) and the Federal Computer Security Program Managers Forum are sharing information about agency programs in order to assist this process.

Finally, the Office of Science and Technology Policy is researching the shortage in the number of academic professionals who are teaching and performing basic research in information security. The purpose of their report is to "increase the number of people both graduating with advanced degrees and teaching and performing basic research in the field of information security/assurance and critical infrastructure protection (ISA/CIP)."[2] Suggested findings are that "there are not enough ISA/CIP experts currently teaching and performing basic research to meet the current demand; there are not enough Doctoral students currently specializing in IS to meet future demand; short-term applied research is being emphasized over long-term basic research; and industry-efforts alone will not solve these problems."[3] When this research is completed, the OSTP will publish a full report with recommendations to alleviate the problem.

[1] President Clinton and Sanford I. Weill, Chairman of Citigroup and the National Academy Foundation, announced the program on July 6, 1999.
[2] OSTP draft Academic Initiative Proposal, revised September 5, 2000, in review at this time.
[3] Ibid.

V. CRITICAL INFRASTRUCTURE PROTECTION R&D

V. CRITICAL INFRASTRUCTURE PROTECTION R&D

Since the publication of Version 1.0 of the *National Plan for Information Systems Protection* in January 2000, an aggressive and fruitful investigation of the need for and solutions to CIP R&D issues has taken place under the auspices of the CIP R&D Inter-Agency Working Group (IWG). Each subgroup has aggressively addressed areas of concern and posed solutions. A description of these, and of the concept for the Institute for Information Infrastructure Protection (I3P) follows.

Information and Communication

The information and communications (I&C) sector of the nation's critical infrastructures generates more revenue than most nations produce. The potential of the new technologies has enabled the U.S., far more than any other nation, to reshape its governmental and commercial processes. We have led the world into the Information Age, and in so doing have become critically dependent on information technologies to conduct national and international commerce, governmental functions, and military operations. These technologies enable us to keep our economy competitive, our government efficient, and our people safe. Thus, as the Honorable Neal Lane recently testified before a joint meeting of two Subcommittees of the House Committee on Armed Services, ensuring the robust and reliable operation of our critical infrastructures " is truly a national challenge - one that goes way beyond the traditional bounds of national security as our economic security, competitiveness, and our way of life rest upon the continuous and assured availability of the services provided by our infrastructures..."[1]

Implementing I&C infrastructure protection through various means such as a viable R&D effort is neither an entirely public nor an entirely private responsibility. The risks to the infrastructure are common to government, business, and citizen alike. Reducing those risks will require coordinated effort within and between the private and public sectors. The need for I&C CIP creates a zone of shared responsibility and cooperation among industry, government, and academia. If we are to retain and build upon the competitive edge information technology has given us, we need to work together on CIP R&D and in other pursuits to substantially improve the trustworthiness of our information systems and networks.

Major Efforts Underway

For FY 2001, nine Federal departments in the President's budget submission to Congress requested funds for 84 ongoing I&C CIP R&D programs. Some of these activities, however, are funded out of program base in other programs and therefore do not appear as separate line items in the budget. The research areas or topics these programs address run the gamut from public key infrastructure and Internet security to mobile agents and advanced authentication systems. As part of the strategic oversight of these programs, the CIP R&D interagency working group has worked with other interagency, Government/industry, and industry groups in sponsoring several Government/private sector workshops. Many of these programs are cooperative endeavors or joint efforts between and among different departments, and a few are joint efforts between Government and universities. For example, the DOD is sponsoring research at universities in its *University Research Initiatives - Centers of Excellence* program in a well-established method of focused research programs on a wide range of topics. Under this initiative, a broad area announcement was issued for CIP and information assurance research proposals

[1] Statement of Dr. Neal Lane, Assistant to the President for Science and Technology and Director of the Office of Science and Technology Policy, before a joint hearing of the Readiness Subcommittee and the Research and Development Subcommittee of the U.S. House of Representatives Committee on Armed Services, March 8, 2000.

from universities, and the research will be funded in FY 2001after review and selection of the proposals on a competitive basis.

Major Challenges in the I&C Area

Gaps and shortfalls have been identified after mapping the currently funded R&D against identified vulnerabilities and shortcomings in the U.S. I&C infrastructure. Those gaps and shortfalls fall into four primary thrust areas:

- Threat/Vulnerability/Risk Assessments - focusing on threat, vulnerability, and risk assessments of the I&C critical infrastructure, to include modeling and simulation programs, metrics, and test beds;
- System Protection - cyber protection of individual systems, to include programs such as encryption, public key infrastructures, network security products, reliability and security of computing systems, robust I&C control systems, and secure supervisory control and data acquisition (SCADA) systems;
- Intrusion Monitoring and Response - technologies to detect and provide immediate responses to intrusions or infrastructure attacks, to include such programs as network intrusion detection, information assurance technologies, mobile code and agents, network alarm systems, forensic tools for electronic media, and network defensive technologies; and
- Recovery and Reconstitution - those technologies required to reconstitute and restore the I&C critical infrastructure in the aftermath of disruptions, to include such programs as risk management studies and tools, system survivability technologies, and consequence analysis tools and supporting technologies.

Banking and Finance

While there are some vulnerabilities and threats unique to the banking and finance sector, the sector's critical infrastructure exposure is essentially an overlay on the I&C infrastructure. One issue facing the sector is that there has been little R&D of any kind done in this community. The only work that fits the traditional definition of R&D would be the development of new derivatives and financial forecasting tools.

In order to address the new and expanding threats from foreign nation states, criminal enterprises and terrorists, the community has sponsored, with the support of the Treasury Department, a number of initiatives. In addition to the Information Sharing and Vulnerability Assessment Center (FS/ISAC) there is a R&D working group under Mr. Charles Blauner – J.P. Morgan & Co. This working group has identified what work is being done within the community and vetted the efforts underway within the government and I&C sector.

The major focus of the FY 2001 program is a modeling effort to identify the vulnerabilities in the banking and finance sector critical infrastructure. This activity builds on work of the National Communications System (NCS), which has completed an extensive model of the United States backbone communications network. This object-oriented model is aimed at understanding the properties, vulnerabilities and required remediation for our national communications infrastructure. As mentioned before, almost all banking and financial services travel over some portion of the communications infrastructure. Accordingly, this effort overlays essential services such as funds transfer, clearing houses, stock markets, refunding, etc. in order to identify the inherited vulnerabilities from the communications infrastructure and best remediation approaches. For example, we may know that there is an existing or pending attack against a certain type of switch. Examination of the model will show where the switches are and which essential financial services depend on them, further examination will show the extent of the impact and what alternatives are available. As the sophistication of the tool develops a better understanding of

financial processes, the model will also be able to identify malicious intervention or criminal activity. While this level of sophistication will take time to develop, the simple mapping of financial transaction and funds flow to the communications model will reap tremendous results. This tool brings a number of benefits: identification of potential vulnerabilities; the testing of remediation alternatives to find the best option; and a tool for executive crisis management training and exercises. During an actual crisis or information warfare attack, the extent of impact can be quickly identified and responses evaluated in real time. This effort will serve as a model technology for identifying infrastructure interdependencies with other sectors.

The sector's secondary focus is on the development of the forensic tools need by the United States Secret Service and other law enforcement agencies in combating electronic crimes and attacks on the banking and finance sector critical infrastructure. This work is being done in coordination with efforts at the Justice Department, but focuses on the specific nature of electronic financial crimes.

The total budget request for fiscal year 2001 was $4 million, which will only provide "seed money" for these efforts. The task of examining the vulnerabilities and interdependencies of the entire banking and finance sector is so overwhelming that there is no meaningful alternative to the efforts to develop mature modeling tools. Once we have the resources and develop the modeling tools, then we can start the R&D efforts to develop remediation for the vulnerabilities that will be identified by the modeling efforts.

Energy

Our nation's energy infrastructure—composed of increasingly interdependent industries that produce and distribute electric power, oil, and natural gas— is undergoing rapid and dramatic changes. Advances in information technology, an increased reliance on electronic commerce, restructuring and deregulation initiatives, and other market forces are motivating much of these changes. The purpose of the energy subgroup is to develop an agenda for a R&D program that will address a wide range of needs related to protecting this critical energy infrastructure. Applicable R&D encompasses the physical and cyber components of the electric power, oil, and gas infrastructures, the interdependencies among those components, and the interdependencies with the other critical national infrastructures. The energy R&D program is aimed at developing cost-effective technologies and capabilities (e.g., databases, methodologies, tools) that can be used to achieve several goals:

- Increase our understanding of physical and cyber disruptions (natural, accidental, deliberate) to the energy infrastructure that could result in cascading or widespread regional outages;
- Develop energy infrastructure assurance "best practices" through vulnerability and risk assessments; and
- Protect against, mitigate the impacts of, and improve our ability to recover from disruptive incidents within the energy infrastructure.

Major Efforts Underway

The R&D agenda consists of two primary thrust areas: Analysis and Risk Management, and Protection and Mitigation Technologies. Specific topical areas include:

- Infrastructure Interdependencies - Development of methodologies and tools for characterizing and analyzing interdependencies among the energy infrastructures and with other critical infrastructures. This capability will help DOE and others within the energy sector identify critical system nodes and assess the technical, economic, and national security implications of energy technology and policy decisions designed to ensure the security of our nation's interdependent energy systems.

- Vulnerability Assessment - Focus on collaboration with the energy sector to conduct physical and cyber vulnerability assessments that identify infrastructure vulnerabilities, raise awareness about these vulnerabilities, and enable the development of guidelines and best practices for industry to use in limiting vulnerabilities.

- Scale and Complexity Analysis - Research on the fundamental operational characteristics of large-scale, complex, nonlinear energy infrastructures. Development of technologies and capabilities that focus on stability, countermeasures, reduction of complexity, the effects of uncertainty, and behavior.

- Consequence Analysis and Management - Development of data, methodologies, and tools for evaluating the public health and safety, national security, and economic consequences of disruptions to energy infrastructures and the processes needed to assist in restoration and reconstitution following such disruptions.

- Risk Management - Development of risk management methodologies and tools to assist decision makers in quantifying system risks and in planning and implementing critical infrastructure protection strategies.

- Policy Effects and Institutional Barriers - Examination of the barriers between government and industry stakeholders in sharing CIP-related information (e.g., threat and vulnerability information) and identification and implementation of solutions to barriers that may inhibit our ability to protect our nation's critical infrastructures.

- Real-time Control Mechanism Technologies - Identification of vulnerabilities inherent in real-time energy control systems and development of technologies for protecting against disruption to, unauthorized control of, or intrusion into these systems.

- Integrated Multisensor and Warning Technologies - Improvement of existing integrated systems and/or development of new ones to warn of attacks and impending failures at critical nodes. Focus on anomaly detection and failure warning technologies.

Major Challenges in the Energy Area

R&D task areas are structured to complement and reinforce each other and related efforts. Capitalizing on the links and synergies across the initiatives to meet requirements is a major technical and programmatic challenge. Additional challenges in the energy sector which complicate the R&D picture include:

- Inadequate information to determine susceptibility to disruption of the energy infrastructure;
- Lack of a coordinated process to collect and distribute threat information;
- Inadequate response and recovery procedures and technology;
- Interdependence of energy infrastructure and other infrastructures;
- Increasing system interconnectedness and complexity of the energy system;
- Increasing reliance on real-time system control;
- Gaps in physical protection for energy infrastructure facilities;
- Limited cyber security for SCADA systems;
- Inadequate protection of energy-related information;
- Reliance on unique, hard to procure equipment and materials;
- Susceptibility to cascading failures; and
- Reliance on rapid access to accurate information.

Conclusion

Coordination and partnerships among agencies and the private sector are of paramount importance. Identifying and developing mechanisms to transfer the technologies, capabilities and best practices developed through this program to industry and public organizations at the Federal, state, and local levels are key to the success of the program and to protection of our nation's critical infrastructure.

Transportation

The Transportation Subgroup of the National Science and Technology Council (NSTC), Committee on Technology, Interagency Working Group on Critical Infrastructure Protection (CIP IWG) R&D includes representatives from a number of DOT offices, as well as several Federal agencies. Incorporating relevant projects and proposals from these organizations, the subgroup formulated the Interagency Transportation Infrastructure Assurance (TIA) R&D plan. This plan provides a coordinated Federal government response to the PCCIP (1997), White House Commission on Aviation Safety and Security (1997), the DOT Surface Transportation Vulnerability Assessment (1999), the National Research Council report, *Improving Surface Transportation Security: A Research and Development Strategy* (1999), and related Presidential Decision Directives (e.g., PDD-62, PDD-63, PDD-67). These activities and initiatives are deemed essential to protecting the nation's transportation infrastructure, operators, and users against future acts of terrorism and crime and will enable the transportation system to adapt rapidly to natural or intentional disruptions. Critical transportation infrastructure elements include: aviation, space transportation, highways, mass transit, pipelines, rail, waterborne shipping, intermodal connections, and interfaces with other transportation-dependent infrastructures, such as energy and telecommunications.

The goal of the Interagency TIA R&D Plan is to develop a comprehensive approach to assessing threats to the security of the nation's transportation system and to preparing R&D projects that provide integrated security solutions (e.g., technologies, procedures) tailored to these threats. It addresses the:

- Physical security of transportation modes and intermodal connections (e.g., roads, railroad lines, bridges, tunnels, terminals, locks and dams, piers, etc.);
- Security of vital communications, navigation and information systems and networks (e.g., GPS);
- Susceptibility of transportation operators and users to weapons of mass destruction (WMD); and
- Development and dissemination of information about system threats, vulnerabilities and best practices to transportation system developers, operators and users.

Major Efforts Underway

Traditionally, aviation, through the Federal Aviation Administration, has conducted the bulk of transportation CIP R&D. This trend continues today as aviation assumes approximately 79 percent of on-going transportation CIP R&D in the area of aviation security (FY 2001). Aviation security projects include:

- Explosives and weapons detection;
- Airport security technology integration;
- Airport security human factors; and
- Aircraft hardening.

Other current major transportation CIP R&D efforts include:

- Analysis on GPS vulnerabilities;
- Intelligence and security risk assessments;
- Threat assessment/information dissemination;
- Infrastructure assurance training/awareness;
- Vulnerability and risk analysis of transportation systems;
- Chemical/biological agent detection;
- Intermodal terminal security at major transportation nodes;
- Human factors analysis for transportation systems;
- Research on operational methods for improving performance of transportation systems;
- A pilot study to determine the ambient environmental background, using high efficiency particulate arresting (HEPA) filters, to establish a "clean air" baseline in certain public areas of transportation facilities in the event of chemical or biological attack and subsequent decontamination clean-up efforts;
- An on-going vulnerability assessment of the interstate roadway system, rail lines, and bridges to determine their susceptibility to disruption by conventional or other means, and what ancillary effects might occur to the national surface infrastructure system and regional or national economies; and
- An analysis to determine current DOT information cyber security gaps in computer networks vital to transportation cyber information systems and subsequently conduct R&D to remedy current cyber information security gaps.

Major Challenges to the Transportation Sector

Responsibility for assuring the safety and the security of the nation's transportation infrastructure and its continued operations is scattered among thousands of private companies and government agencies at all levels (from local to Federal). This decentralized approach to transportation has caused gaps in transportation system security, especially in areas where both responsibility and resources are divided or uncertain. A second major challenge involves information control of vulnerability assessments. The crux of the challenge involves the following questions: How can vulnerability assessments remain classified in such a manner to not allow inappropriate Freedom of Information Act distribution, yet allow private companies to obtain the needed information? Additionally, many vulnerability assessments could involve the gathering of sensitive, proprietary information, which, if provided to competitors, would be damaging to the participating private company. How should this information be protected? Many private companies fear that vulnerability assessments of their operations could open the door for tort liability. Although these questions have yet to be fully resolved, efforts are underway to address these concerns.

Conclusion

Aviation has a strong history of robust R&D efforts with regard to transportation infrastructure assurance and security. This will continue. But, because of surface transportation's importance and vulnerability, as highlighted by several recent studies and high-profile incidents, improving surface transportation security is essential given emerging 21st Century threats – cyber terrorism and chemical and biological weapons. The interagency development of the TIA R&D plan addresses and coordinates these challenging tasks of protecting our nation's transportation infrastructure from terrorist threats. The plan's next stage will include heightened involvement of private industry in developing and honing transportation infrastructure assurance R&D.

Vital Services

The Vital Human Services (VHS) sector includes three of the critical infrastructures: water supply, emergency services, and government services. The three VHS infrastructures differ from other critical infrastructures in that they are focused largely at the state and local level and are largely governmental responsibilities. In spite of these differences, the VHS infrastructures face similar problems and vulnerabilities in communities across the country. This section of the report highlights the research and development efforts underway in the water supply and emergency services sectors.

The water supply sector CIP effort is primarily focused on the 330 large water supply systems, which serve more than 100,000 people. The U.S. EPA, as lead agency for the water supply sector, is working in cooperation with various associations, especially the American Water Works Association (AWWA) and the Association of Metropolitan Water Agencies (AMWA). Through these partnerships, EPA hopes to raise awareness of water sector vulnerabilities, encourage information sharing, and develop remediation protocols for the vulnerabilities that are discovered. The initial research effort is small and is focused on developing a vulnerability assessment methodology. Additional Federal agencies including the Department of HHS and FEMA also assist with efforts in the water supply sector.

HHS has requested funding to focus on emergency services infrastructures. Efforts include identifying key areas of interdependence between hospital and health care response and communications and transportation infrastructures and working with hospitals and related emergency services to identify operational vulnerabilities and to determine ways to mitigate those vulnerabilities.

Major Efforts Underway

In FY 2000, EPA entered into an inter-agency agreement with the Department of Energy's (DOE) Sandia National Laboratories to develop a vulnerability assessment methodology for the water supply sector. This methodology is an extension of the methodology developed for the Federal dam community. The Federal dam community includes the Corps of Engineers, Bureau of Reclamation, Bonneville Power Authority, and TVA. The AWWA–Research Foundation, a private not-for-profit organization, which sponsors research for the drinking water industry, has also entered into a contract with Sandia to further support this vital work. Funds requested by HHS are also expected to assist in this effort. In the fall of 2000, a workshop with six to eight representatives of large water utilities outlined a methodological approach. This effort will extend into FY 2001 and, if funded, the effort will be expanded to include field-testing and training for users.

In August 2000, EPA held a joint meeting on the water supply infrastructure with DOE at their Argonne National Laboratory. Most of the major Federal water agencies and approximately 30 water utilities were represented. Meeting attendees reached an agreement on the approach and the priorities for water supply sector research. The recommendations from that meeting will be available shortly.

For FY 2001, funds were requested in the President's budget submission and appropriated by Congress to initiate a more robust water sector CIP program. The direction from OMB to the EPA is as follows:

> "Through partnerships with AMWA and AWWA, EPA will work with water utilities undertaking measures to safeguard water supplies from terrorist and seditious acts. EPA will also implement an assessment of the vulnerability and methods to reduce vulnerability of the drinking water supply to terrorists acts."

Other areas of interest include remediation measures, threat analysis and communications techniques, methods to identify and characterize chemical and biological agents, and a university or industry-based center of excellence in risk assessment and risk reduction. Specific efforts are underway, in cooperation with FBI, to develop an ISAC for the water supply sector to facilitate the exchange of threat and vulnerability information.

FEMA is also leading an effort to produce valid and verified databases of water distribution systems and to develop assessment tools for evaluating the threat to public health and safety posed by the introduction of a biological or chemical agent into a water system. Two prototype databases and assessment tools will be developed covering: broad area populations at risk (statewide) and local area populations at risk (citywide). The broad area prototype will allow the user to track an agent, under variable flow conditions, from the point of introduction to downstream water supply intakes and will determine the concentration and decay rate of an agent as it is dispersed within the water source. The local area prototype will allow the user to model the flow and concentration of an agent within a city or municipal water system, will assess the effects of water treatment on the agent, and will model the flow and concentration of an agent through the water distribution system.

The funds requested by HHS will focus on three of the VHS sector's high priority research and development issues identified by the interagency CICG. First is the previously mentioned effort to develop a vulnerability assessment methodology for the water supply sector. Emergency services infrastructure issues include studying critical interdependencies between hospital and health care response systems and the communications, essential transportation, public safety, and emergency medical systems. This effort will look at how threats or damage to communications and transportation systems may affect the response capabilities of the hospital and health care community. A related effort will look at protection of hospital infrastructures. This effort will focus on critical hospital operations in response to a chemical or biological incident including decontamination, preventing cross-contamination, hospital capacity, etc.

Major Challenges in the VHS R&D Area

On-going water sector research is a small effort and leaves gaps and shortfalls in addressing identified vulnerabilities and shortcomings relative to U.S. water supplies. EPA is coordinating its efforts closely with other Federal agencies and the private sector to identify the highest priorities and to work jointly to develop solutions to vulnerabilities and shortcomings.

Gaps and shortfalls exist in four major areas:

- Threat/Vulnerability/Risk Assessments – Focusing on threat, vulnerability, and risk assessment of the water supply sector critical infrastructure to include methodologies, benchmarks, field-testing and analysis and communication of results.

- Supervisory Control and Data Acquisition (SCADA) Systems – Application of information assurance techniques to water supply SCADA systems and development of appropriate, cost-effective protocols. Since the SCADA systems used in water utilities are similar to those used in the gas, oil, and electric power sectors, this work will rely heavily on efforts being conducted by DOE.

- Identify and Characterize Biological and Chemical Agents – In conjunction with CDC and other agencies, identify and characterize the behavior of chemical and biological agents in water. Determine the effects of water treatment on these agents and characterize the actual risks posed by these agents to the nation's water supply.

- Center of Excellence for Risk Assessment of Water Supplies – Establish a center of excellence to support communities in conducting vulnerability and risk assessments and in making decisions regarding water supply assurance.

Conclusion

The cooperation of the water supply industry is essential in developing realistic research needs and in developing the tools that they need to evaluate and correct vulnerabilities. EPA has succeeded this year in establishing a good relationship with the major water association and has an agreement with them as to future priorities.

Interdependencies

The economy and national security of the United States are becoming increasingly reliant on a spectrum of highly interdependent U.S. and international infrastructures. This trend has accelerated over the last ten years with the proliferation of information technology and concomitant infrastructures, and shows no signs of abating.

This development is relatively recent: while the U.S. economy has long depended on several critical infrastructures, the coupling among them had historically been rather loose. However, during the past few years, important technological, economic, and regulatory changes have dramatically altered the relationships among infrastructures. At the same time as the IT revolution led to substantially more interconnected infrastructures with generally greater centralization of control, "just-in-time" business practices have reduced margins for error in infrastructure support. Deregulation and growth of competition in key infrastructures has eroded spare infrastructure capacity that served as a useful "shock absorber" in key infrastructures. Furthermore, mergers among infrastructure providers have led to further pressures to reduce spare infrastructure capacity as management has sought to wring "excess" costs out of merged companies to realize savings. Any one of these trends would be a cause for uneasiness. The collision of all four has no precedent in American economic history. While important steps have been taken in individual infrastructures, the issue of interdependent and cascading effects among infrastructures has received almost no attention. This situation is starting to change, as the government launches activities designed to yield a greater understanding of the nature and implications of these infrastructure connections.

Major Efforts Underway

Several efforts are underway to try to tackle the difficult issues of interdependencies. These include efforts to learn about the secure operation of complex interactive networks/systems, and furthering the understanding of the dynamics of complex interactive networks/systems; technology development and vulnerability analysis capability R&D, aimed at analyzing national and defense infrastructures and their critical interdependencies; efforts to develop an easy-to-use, deployable state-of-the-art hazard and consequence prediction, digital databases, and a Geographic Information System (GIS), within a Graphical User Interface (GUI); collaborative work between the Disaster Research Center at the University of Delaware and the Research Center for Disaster Reduction Systems, a unit within the Disaster Prevention Research Institute at Kyoto University in Japan to better understand various aspects of damage caused by earthquakes; and interagency efforts to build upon a number of ongoing programs and laboratory testbed facilities.

Major Challenges in the Interdependencies Area

The major efforts underway, as well as those being investigated for the future, are designed to meet the following challenges.

- Building a theoretical framework for understanding and predicting the nature of interdependencies and their effects on the country as a whole.

- Developing the capability to model and simulate in real time the behavior of the nation's interconnected infrastructures by developing an architecture and related enabling technologies that can be used to integrate infrastructure-specific and interdependence databases and analysis tools to study the linkages among the interdependent critical infrastructures, the interdependencies associated with those linkages, their impacts, and their likely causes.

- Developing a set of quantitative metrics for measuring the scale of impacts of interdependency-related disruptions.

- Developing new technologies and techniques to contain, mitigate, and defend against the effects of interdependency-related disruptions, such as escalating, cascading, latent, and cross-infrastructure failures.

- Developing capabilities to adequately and realistically test new methodologies, techniques, and technologies.

- Defining a set of tasks for further work on specific national security policy issues that could be analyzed using these tools and methodologies. This could include, for example, characterizing the potential interdependence implications, from national security and economic perspectives, of current trends within the private sector (e.g., restructuring, deregulation, increased reliance on cyber monitoring and control systems) and their implications for national security; identifying interdependency vulnerabilities in the U.S. economy; and developing metrics for interdependencies.

- Developing the ability to characterize and incorporate new critical infrastructures into the models and methodologies as such infrastructures develop.

Conclusion

Growing interdependencies between critical infrastructures make this set of problems significantly different than those we have faced in the past, and it is what makes them difficult. A significant amount of work is now being done in government, the national labs, academia and private industry to build an understanding of these issues, and tools to solve these problems.

International R&D

Just as our critical infrastructures are inherently international, so too is the global science and technology base that will generate solutions to current and future infrastructure protection vulnerabilities. In general, the U.S. has no monopoly over the relevant technologies. Research and development in the field of information technology is a fully international enterprise today. In fact, it is even difficult to define a "domestic" science and technology base, given the substantial technical contributions made by foreign scientists and engineers within the U.S., by firms in overseas laboratories, and by foreign or multinational firms with U.S. research facilities.

Moreover, the technologies relevant to infrastructure protection are largely unclassified, having been developed in the commercial sector or academia rather than in government or its contractors. Therefore, unless a particular R&D project involves classified material or is identified by its sponsoring U.S. government agency as raising particular sensitivities, it can serve the U.S. national interest to draw on the global science and technology base, and to have the project done by the most qualified technical experts, wherever they may be. Indeed, the U.S. has a history of pursing international science and technology collaboration as a means of stretching development dollars, broadening and deepening the talent pool that can be brought to bear, and building an international constituency for our views. Many of the international science and technology activities now considered to be CIP-related reflect longstanding, and continuing, collaborative efforts of private industry, academia, and government to resolve emerging information technology issues.

The Department of State has undertaken a variety of activities in response to PDD-63, including multilateral negotiations in the European Union, Asia-Pacific Economic Cooperation, Organization for Economic Cooperation and Development and other fora that addressed existing and emerging threats and vulnerabilities to our economic security. The Department of State also led and coordinated bilateral negotiations and meetings with Canada, United Kingdom, and Australia aimed at identifying, developing and facilitating science and technology solutions for CIP.

Multilateral Agenda

EU*:* A United States and European Union Task Force on Science and Technology was established in October 1998 to enhance the security of critical infrastructures by identifying, developing, and facilitating technology and policy solutions to existing and emerging threats and vulnerabilities. The Department of State Co-Chairs this Task Force with a senior EU representative from the Directorate General for Information Society. Over the past year the task force has sponsored a series of workshops and conferences resulting in cooperative exchanges between U.S. technical agencies and EU research organizations; reciprocal exchange of information on cyber security research programs on an annual basis; coordinated research projects; visits and exchanges of scientists; and mutual exchanges of scientific and technological information.

APEC*:* Within the APEC forum, the Department of State succeeded in establishing a dialog on CIP-related telecommunication issues. At the APEC Telecommunications 21 Working Group meeting, in March 2000, the Department worked closely with the Business Facilitation Steering Group (BFSG) to address the relationship and importance of infrastructure protection to e-commerce in each of the economies represented. By working closely with other APEC economies the Department was able to get infrastructure protection added to the APEC Telecommunication Program of Action during the Fourth Ministerial Meeting, held in Cancun, Mexico in 2000. The Department continued to expand the APEC agenda on infrastructure protection science and technology issues and arranged for State sponsorship of a half-day workshop at TEL 22 in October 2000 to develop a forum and advance proposals to facilitate awareness and sharing of information with regard to critical infrastructure science and technology issues in the Asia-Pacific region. At the APEC Telecommunications 22 Working Group meeting in October 2000 the State Department sponsored a proposal, along with Australia and Canada, for development of cyber security training modules to be used by member economies at both undergraduate and graduate level to increase the level of information security awareness and ultimately the protection of critical infrastructure. In the APEC Industrial Science and Technology Working Group, working collaboratively with Department of Commerce, the Department of State has successfully laid the groundwork for introduction of CIP technology cooperation with the aim to identify all relevant research and development in the Asia-Pacific region.

OECD*:* The Department of State initiated a discussion on cyber security issues within the OECD in 2000. At the last meeting of the OECD Working Party on Information Security and Privacy (WPISP) the Department sponsored a presentation highlighting global aspects associated with information security, the economy's dependence on the internet, technical vulnerabilities of the internet, and possible solutions such as the concept of a center for analysis of global incidents, global intrusion detection and identification, research and development, and awareness raising through education and media. This resulted in a discussion among economies and agreement for future work in this area. The Department was also successful in obtaining WPISP agreement in the Work Program for 2001-2002 to examine the present and future state of cyber security including emerging threats and vulnerabilities. The Department's efforts in subsequent meetings of the OECD have resulted in widespread agreement on the importance of cyber security and the role that OECD should take in progressing work in this area including an early review of security guidelines.

Bilateral Agenda

Canada: The Department of State led a bilateral meeting in September 2000 to discuss CIP cooperative efforts at the national and departmental/agency levels and in international fora. There was agreement to establish a CIP R&D Working Group to take stock of current efforts and to identify potential synergies and a short list of areas of further cooperation/joint action. There was also interest expressed in the idea of developing an International Center for Analysis of Global Incidents.

United Kingdom: The Department of State met with representatives from the UK Information Assurance Advisory Council (IAAC) to discuss critical infrastructure protection science and technology issues and to exchange information on respective national and international policies on information assurance. The IAAC, whose membership includes the Cabinet Office, CESG, private industry and academia, has created five working groups to address CIP issues: threat assessment & attack warning, risk assessment and critical dependencies, standards, R&D, education and outreach. The IAAC stressed the importance of industry involvement in addressing the increasing volume of attacks on infrastructure and expressed a desire to work cooperatively with US information sharing and analysis centers.

Australia: The Department of State met on several occasions throughout 2000 to coordinate strategy for promoting both science and technology research and policy. Presidential Science Adviser Dr. Neal Lane and the Australian Minister of Industry, Science and Resources issued a Joint Statement on Scientific and Technological Cooperation in Canberra on November 1 to signal the two countries' intention to negotiate a new S&T agreement. The Australian government agreed separately to conduct a survey of all ongoing CIP R&D and meet over the next year to identify areas for possible joint projects.

Conclusion

The globalization of technology is a dominant force shaping today's world economy. In fact, calls for a more activist Federal technology policy stem in large part from the recognition of this shift in the geographic distribution of the world's technological capabilities. What is not always noted, however, is that the very process of globalization calls into question the notion that technologies, industries, or even corporations have distinctive nationalities. It is impossible for any country to achieve its national science and technology objectives in isolation from other countries. Increasingly, the development of many high-payoff technologies is a high-risk, and costly venture, which exceeds the capacity and capabilities of individual firms, and even of countries. International S&T relations have become an integral part of overall U.S. foreign policy and play a vital role in meeting the challenges of infrastructure protection.

VI. INDUSTRY INTERIM PROGRESS REPORTS

VI. INDUSTRY INTERIM PROGRESS REPORTS

The reports that follow were voluntarily provided by several industry sectors and partnerships, representing a sample of progress and activities within industry over the last year and a half on critical infrastructure protection. The critical infrastructure industries vary widely in their cultures, industry structures, and ways of operating, reflecting and responding to their different market structures, current competitive processes, and regulatory regimes. These reports reflect those differences and at the same time reflect a common business perspective and approach to the issues, starting with a development of an industry business case for action, and including finding the most efficient ways of addressing the issue, such as learning and joining with each other to address common issues and concerns.

This section includes reports from:

Banking and Finance Sector

This joint report by the sector and the Department of Treasury was provided through the Department of Treasury and describes the accomplishments and activities supporting PDD-63 by the banking and finance industry.

Electric Power Sector

The Secretary of Energy asked the North American Electric Reliability Council (NERC) to take on the sector coordinator role for the electric power sector. Because of its long history of providing a forum for electric operations representatives from all parts of the industry to come together to work on reliability issues, it already had an organizational and procedural structure to address the issue of electric infrastructure protection. Its report, originally provided to NERC's Board of Trustees in October 2000, documenting its progress and activities follows.

Oil and Gas Sector

The National Petroleum Council (NPC), a CEO advisory council to the Secretary of Energy, was asked to take on the role of sector coordinator for this industry. It tasked a working group consisting of executive management representatives from a wide range of industry institutions to develop a plan and approach to addressing the concerns addressed in PDD-63. The following report represents the substance of the progress of that task force that was presented to the NPC in the fourth quarter of 2000.

The Partnership for Critical Infrastructure Security (PCIS)

The Partnership provides a forum for cross-sector dialogue. The Coordinating Committee of the Partnership, consisting of representatives from all the active industry sectors, and other founding industry representatives, provided an interim status report on its organizing activities and progress. The Coordinating Committee has also provided as part of their report an interim report from their working group on Policy and Legal Issues that are of particular concern to industry.

Banking And Finance

Introduction

Presidential Decision Directive 63 assigned Treasury "lead agency" responsibility for working with the banking and finance sector of the economy, a responsibility managed by Treasury's Office of Financial Institutions Policy. Treasury Assistant Secretary Gregory Baer serves as Sector Liaison. After consultation with the industry, Treasury named Steve Katz, Chief Information Security Officer of Citigroup, as the industry's Sector Coordinator. Together, Treasury and the industry are responsible for carrying out a number of tasks, including:

- Assessing the vulnerabilities of the sector to cyber and physical attacks;
- Recommending a plan to eliminate significant vulnerabilities;
- Developing an information sharing system for identifying and preventing major attacks;
- Proposing an agenda of research and development for information systems security;
- Developing an education and outreach program to increase awareness of industry infrastructure security risks; and
- Providing content for the industry's contribution to the *National Plan*.

The Banking and Finance Sector

According to the Federal Reserve, at year-end 1999, total credit market assets held by U.S. financial institutions amounted to about $19.6 trillion. The largest institutions by category were commercial banks ($4.6 trillion in assets), insurance companies ($2.4 trillion in assets), mutual funds ($2.3 trillion), pension funds ($1.8 trillion), and thrift institutions ($1.3 trillion); the remaining assets were distributed among finance and mortgage companies, securities brokers and dealers, and various other financial institutions. Banking and finance also includes, and is critically dependent upon, a variety of specialized service organizations such as securities and commodities exchanges, funds transfer networks, payment networks, clearing companies, trust and custody firms, depositories, and messaging systems. These systems are increasingly deployed globally, among institutions, utilities (such as exchanges and clearing entities) and counter-parties.

Moreover, driven by competitive pressures to acquire increasingly sophisticated and costly technology, banking and financial firms have become progressively more dependent on outsourcing certain activities and relying on third-party providers of systems and applications software, as well as technically skilled personnel. Although not members of the banking and finance sector as traditionally defined, the latter firms now have become an indispensable part of the banking and finance infrastructure.

Early studies of banking and finance concluded that this sector is probably better prepared than most other sectors of the U.S. economy to protect itself against cyber and other infrastructure threats. This "preparedness" is largely attributed to the pervasive understanding in the industry that consumer confidence in the safety and reliability of the financial system is absolutely

essential for continued success and to the long legacy of federal regulation of major categories of financial institutions, such as insured depositories and securities brokers and dealers.

The fact remains, however, that the environment evolves, and infrastructure protection measures must evolve in tandem. In the case of banking and finance, a number of major trends have been identified that almost certainly will mean new or altered vulnerabilities, thereby requiring that existing infrastructure protection measures be modified and strengthened and that additional ones be implemented. These trends include:

- *Consolidation*. Ongoing mergers and acquisitions have led to substantial consolidation throughout banking and finance, resulting in greater concentration of assets and fewer sources of support services. This may mean potentially more risk to the financial system in the event of difficulties at individual entities.

- *Globalization*. Financial transactions and activities now routinely "follow the sun," in that they are carried out "24 by 7," at times with little regard for political or national boundaries. The ubiquity of the Internet allows customers, counter-parties, intermediaries, principal institutions, and others to interoperate and intercommunicate on a global basis. More consolidations are cross border and cross cultural, projecting risks and vulnerabilities onto a global stage.

- *Reengineering*. Financial institutions continue to eliminate redundant operations and facilities, simplify systems and processes, and generally to reduce personnel costs. This may increase the risks associated with facility concentration, the use of "off-the-shelf" software, and dissatisfied employees.

- *Decentralized Technology*. Traditional centralized, limited-access computer systems are rapidly being replaced or supplemented by decentralized, open-access systems. This may increase the risk of unauthorized, potentially malevolent access to financial institutions' data and/or control of institutions' computer systems.

- *Alternative Channels*. Financial services increasingly are distributed via channels other than traditional brick and mortar offices. Points of entry into an institution's systems now often include card-activated terminals, wired and cellular telephones, and personal computers, wherever located. This may increase the risk of unauthorized access.

- *Public Infrastructure*. Financial institutions have increased their reliance on public shared data networks to receive and transmit information and funds, and to provide services to consumers. Shared networks are unlikely to be as secure as proprietary or leased, dedicated networks.

- *Interdependencies*. Banking and finance increasingly depends on external service providers, both basic and specialized in nature. Basic services include electrical energy and telecommunications, both being absolutely essential to the provision of financial services. Specialized services include those provided by information and data processing firms, systems and applications software firms, and firms providing sophisticated

information on financial markets worldwide. Denial of service from any of these external service providers may increase vulnerabilities in the banking and finance sector.

Recent Cyber Attacks

The urgency of addressing the issues outlined above is made clear from even a brief accounting of cyber incidents that occurred just this year. For example:

In December, Creditcard.com was the victim of an extortion attempt by a cyber thief accused of hacking into its site and exposing more than 55,000 credit card numbers on the Internet.

In September, Western Union customer information was exposed while the website was undergoing maintenance. Hackers made electronic copies of credit and debit card information of 15,700 customers.

In August, two Kazakhstan men were arrested in London for breaking into Bloomberg L.P.'s New York computer system in an attempt to extort $200,000 from the business news service and its owner.

In May, the "Lovebug" virus was unleashed by an individual residing in Manila, overloading corporate e-mail systems in numerous countries and causing damages estimated at up to $10 billion.

In March, two British teens were arrested for breaking into e-commerce Internet sites in five countries and stealing information from 26,000 credit card accounts.

In February, major U.S. e-commerce sites were disrupted with distributed denial of service attacks, causing over $1.2 billion in damages. Also, a disgruntled Chinese national employee at Deutsch Morgan Grenfell in New York planted a "time bomb" in a computer program that cost DMG $50,000 to fix.

Industry Activities and Accomplishments

As a first step toward the private sector outreach mandated by PDD-63, former Secretary Robert Rubin convened a Treasury information security conference on October 7, 1998. Attendees included a large number of industry information security officers and representatives of the financial regulatory agencies and others with a direct interest in critical infrastructure protection.

Industry representatives at the October 7 conference readily agreed that the goals of PDD 63 were worth pursuing, and they agreed to create and support what is now known as the *Banking and Finance Sector Coordinating Committee on Critical Infrastructure Protection* (the Coordinating Committee), chaired by Sector Coordinator Katz. The industry representatives also established four working groups to address the issue areas they considered to be of highest priority: vulnerability assessment; research and development; education and outreach; and information sharing. This blueprint has defined the activities of the industry since October 1998.

The second meeting of the Coordinating Committee, on March 11, 1999, was a "nuts-and-bolts" type of meeting that established specific agendas for each of the working groups going forward. At that meeting it also was decided that the creation of an industry information sharing and analysis center (ISAC) was especially important, largely because of impending Y2K concerns among government and industry leaders and other signs of an increase in cyber threats. The third meeting, held on April 10, 2000, focused on assessing the vulnerability of the financial services sector to attack and on research and development priorities.

Each of the working groups is at a different stage in their activities. The R&D Working Group is consulting government, academic, and industry experts to develop priorities for government- and private sector-funded research. The Vulnerability Assessment Working Group is reviewing a vulnerability analysis prepared for the President's Commission in 1997, and working on a plan for a follow-up vulnerability assessment of its own. The Outreach Working Group has worked with the Critical Infrastructure Assurance Office at the Commerce Department to help raise awareness of these issues, and is working on a plan for industry education and outreach. The recently established National Plan Steering Committee is drafting the sector's preliminary infrastructure assurance plan and coordinating with the Partnership for Critical Infrastructure Security.

The Financial Services Information Sharing and Analysis Center (FS/ISAC)

One of the most important goals of PDD 63 was the establishment of private sector information sharing and analysis centers (ISACs). These centers would be designed to detect and analyze actual or potential cyber attacks, and distribute alerts about, and suggested remedies for, such attacks to their respective industry sponsors, the actual owners and operators of the critical infrastructures.

The financial services industry was the first to respond to PDD 63's call for the establishment of an ISAC. After an arduous period of technical, legal, and organizational negotiations, approximately a dozen major financial services firms and industry utilities established the Financial Services Information Sharing and Analysis Center – the FS/ISAC. Its official opening was announced by Treasury Secretary Summers on October 1, 1999, with assistance from Chairman Arthur Levitt of the Securities and Exchange Commission, Vice Chairman Roger Ferguson of the Federal Reserve Board, and Richard Clarke of the National Security Council.

The FS/ISAC can be described briefly as follows:

The FS/ISAC is a mechanism for developing and sharing a secure database of information on cyber threats, incidents, vulnerabilities, resolutions and solutions. This information can be shared in an authenticated and anonymous manner, so that member institutions can participate without taking on reputational and other risks.

The FS/ISAC is a limited liability company owned by its members, who include the largest banks, securities firms, insurance companies, and investment companies in the country. The FS/ISAC is not in any way funded or governed by the Treasury Department or any other government agency. Treasury staff attends board meetings solely as observers.

Information comes into the FS/ISAC either from its participating members or from the vendor that operates the center, Global Integrity Corporation, a subsidiary of SAIC. Information contributed to the FS/ISAC can come from publicly available sources, government sources (local, state, and federal), members submitting anonymously, members submitting in an attributable manner, and others. Importantly, no customer account information is shared. No one at Treasury or any other agency sees the input or output of the FS/ISAC.

The sharing of information directly from the government to the FS/ISAC, and eventually from the FS/ISAC to the government and other sector ISACs is under discussion. For example, the FS/ISAC and the Pentagon's Joint Task Force/Computer Network Defense have been discussing such an information sharing agreement; and the FS/ISAC has made it known that it will consider sharing information with other industry ISACs subject to the appropriate protocols.

Participation in the FS/ISAC does not absolve any individual financial institution of its obligation to report criminal activity involving an institution's computer and information systems to the appropriate regulatory and law enforcement authorities.

Although just a year old, the FS/ISAC already has gained notice for outstanding performance during the various denials of service and computer virus attacks of recent months. In Congressional hearings in May, the U.S. General Accounting Office cited the FS/ISAC as the best performing of the various existing public- and private-sector mechanisms intended to provide alerts and countermeasures in defense against information system threats and incidents.

The BITS Financial Services Security Laboratory

Another impressive industry initiative is the financial services security laboratory established in July 1999 by BITS, the technology group for the Financial Services Roundtable, to test products and services that strengthen the security of electronic payments and e-commerce technologies. The goal of the laboratory is to provide the industry and consumers with assurance that financial products have been tested by an unbiased and professional facility and that they meet a prescribed level of security, a fact certified by the issuance of a *BITS Tested Mark*. Like the FS/ISAC, the BITS laboratory is an important, innovative approach to *ex ante* security assurance, and it is another example of the financial sector's commitment to protect providers and users of financial services.

Regulatory and Legislative Initiatives

Several months ago the four Federal depository institution regulators issued a request for comment on a proposed rule establishing standards for safeguarding confidential customer information. Public comments were due this past August 25, and the final rule is now pending. The rule would implement section 501(b) of the *Gramm-Leach-Bliley Act*. Among other things, the rule would provide that financial institutions establish a security program that would require them to: (1) identify and assess the risks that may threaten customer information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in

technology, the sensitivity of customer information, and internal or external threats to information security.

In addition, proposed legislation to reduce disincentives to information sharing was introduced in the House earlier this year. The *Cyber Security Information Act* (HR 4246) would encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection. It would do this by reducing the risk of antitrust, Freedom of Information Act (FOIA), and liability actions related to cyber security information sharing. Hearings on this bill were held in June, but no further action has been taken. Banking and finance industry representatives intend to address these and other legal issues in the sector's contribution to the *National Plan, version 2*.

Next Steps: Drafting the National Plan

For the immediate future, the banking and finance sector will focus almost exclusively on drafting its contribution to the *National Plan, version 2*. Industry representatives have agreed that topics to be addressed in the sector plan will most probably include information sharing, vulnerability assessment/interdependencies, research and development requirements, education and awareness, sector defense against an attack (continuation of business), reconstitution (how to rebuild after an attack), and legal issues (such as antitrust, FOIA, liability, and privacy).

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

THE ELECTRICITY SECTOR RESPONSE TO

THE CRITICAL INFRASTRUCTURE PROTECTION CHALLENGE
STATUS REPORT AS OF NOVEMBER 2000

The North American Electric Reliability Council (NERC) has been asked on a number of occasions during the past decade to serve as the electric utility industry (Electricity Sector) primary point of contact for issues relating to national security. Since the early 1980s, NERC has been involved with the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Y2k rollover impacts, and now the threat of cyber terrorism. At the heart of NERC's efforts has been a commitment to work with various federal government agencies to reduce the vulnerability of interconnected electric systems to such threats.

The Report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to a May 1998 Presidential Decision Directive (PDD-63)[1]. PDD-63 called for government agencies to become involved in the process of developing a National Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical systems through public-private partnerships. The PCCIP specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. In September 1998, Secretary of Energy Bill Richardson wrote to then NERC Chairman Erle Nye seeking NERC's assistance, on behalf of the Electricity Sector, in developing a program for protecting the nation's critical electricity sector infrastructure. Responding to the U.S. Department of

[1] The Presidential Decision Directive 63 (PDD-63) states in part:

> *"No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the signing of Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:*
>
> — *the federal government to perform essential national security missions and to ensure the general public health and safety;*
> — *state and local governments to maintain order and to deliver minimum essential public services;*
> — *the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.*
>
> *Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."*

Energy's (DOE) critical infrastructure protection initiative, NERC agreed to participate as the Electricity Sector coordinator.

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison, worked through its Infrastructure Assurance Outreach Program to performed an information assurance assessment for a small number of nodes on NERC's industry information system. The purpose of this assessment was to help NERC and the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. A second follow on information system assessment will be performed in late 2000 and early 2001. The product of this study will be recommendations that will form the basis of a draft NERC policy on information assurance. In addition, to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America, DOE has provided clearances for several industry personnel and clearances for other key industry personnel are anticipated. These clearances compliment those obtained through another government program, which is discussed below.

Critical Infrastructure Protection Working Group (CIPWG)

After several exploratory scoping sessions with the DOE and the National Infrastructure Protection Center (NIPC), NERC created a Critical Infrastructure Protection (CIP) Forum to evaluate the value of sharing cyber and physical incident data affecting the bulk electric systems in North America. The meetings of this group were widely noticed and the participants included all segments of the electric utility industry and representatives from several government agencies including the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, DOE, and NIPC. As a result of their deliberations, NERC created a permanent group within the NERC committee structure. The Critical Infrastructure Protection Working Group (CIPWG) reports to the Operating Committee, with Regional and sector representation and participation by CIAO, DOE, NIPC, American Public Power Association (APPA), Canadian Electricity Association (CEA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), Electric Power Research Institute (EPRI), National Rural Electric Cooperative Association (NRECA), and Power Marketers.

Indications, Analysis, and Warnings Program

One of the first tasks of the Forum was to develop the incident data types and event thresholds to be used in an information-sharing program with NIPC. Information sharing (electronic and telephone) mechanisms have been developed for use by electric transmission providers, generation providers, and other industry entities for reporting on a voluntary basis to both NIPC and NERC. Assessments, advisories, and alerts prepared from analyses by NIPC (with NERC's support) based on the data provided by the Electricity Sector (ES) together with data from other sectors, will be stated in an actionable manner and will be transmitted to ES entities. This proposed process was successfully tested within one Region during the fall 1999 and winter 1999–2000. Because of the nature of some of the analyses, government security clearances have been acquired for key industry personnel (three NERC staff members currently hold U.S. clearances) and other industry personnel are in the process of obtaining security clearances.

The Indications, Analysis, and Warnings Program, which evolved from this work, was presented in July 2000 to the Operating Committee. The Operating Committee approved a motion to establish the program in the Electricity Sector (Canada and United States) with initial emphasis on reporting by Security Coordinators and Control Areas. Marketers and the other electric power providers are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings. Workshops were conducted during the fall 2000 to provide program details to the sector.

The Indications, Analysis, and Warnings Program is a voluntary first step toward preparing the Electricity Sector to meet PDD-63 objectives.

Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

The PCCIP recommended that each of the critical sectors establish an Information Sharing and Analysis Center (ISAC) to help protect the infrastructures from disruption arising from coordinated intrusion or attack. The ISACs would gather incident data from within their respective sectors, perform analysis to determine potential malicious intent, share findings with other ISACs (private and government) in a manner that assures, as required, target identity protection and disseminate useful warnings to the personnel identified to take appropriate action within each sector. ISACs would serve as points of contact between sectors to facilitate communications, especially during a time of stress. ISACs would study cross sector interdependencies to better understand and be prepared for the possible impacts of an "outage" of one sector on another.

The CIPWG has endorsed, and NERC has accepted, the naming of NERC as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The functions performed are essentially the same as those functions that have been required of NERC for physical sabotage and terrorism. The ES-ISAC's duties are:

1. Receive voluntarily supplied incident data from ES entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.
3. Assist the NIPC personnel during its analyses on a cross private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts to all those within the ES who are able to take action.

Duties one and four have been assigned to the existing NERC staff. More definition is being established for duties two and three. The ES-ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will likely request support for a 24- hour-seven days a week staffed facility.

NERC will establish relationships with the other ISACs as they form.

Critical Infrastructure Protection Planning

The CIPWG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the ES. Separate papers have been prepared for CEOs, COOs, CIOs, and a NERC general overview. The purpose of the Business Case is to persuade ES participants of the need to report cyber intrusion incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPWG is developing what may become a basic and fairly comprehensive plan to address the CIP issues in the ES. The Working Group is concerned about generating an overly prescriptive plan too early in the process and is proceeding with a format that can assist in developing each entity's own plan. The prototype plan addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, reconstitution, and interdependencies between and among sectors.

The essence of this "Approach to Action" will be considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government. Richard Clarke,

Special Assistant to the President and National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, recently discussed the importance of establishing and maintaining a National Plan to the health of the government and private sectors, companies, and the nation. Version 1.0 of the Plan did a good job covering the threats and the government response, but it did not detail private sector response. The need for private sector participation is engendered by the fact that the government lacks private sector expertise and needs private sector "buy in" to CIP initiatives. The National Plan version 2.0, which will include private sector input, is scheduled for spring 2001.

Partnership for Critical Infrastructure Security (PCIS)

The Partnership for Critical Infrastructure Security was proposed in late 1999 by members of several private sectors; the PCIS is supported by CIAO and the U.S. Chamber of Commerce. The PCIS Mission:

> Coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

The PCIS held two general forums in 2000 and is planning two general forums in 2001 — March 20–21 and September 6–7. The PCIS has formed six active working groups: Interdependency Vulnerability Assessment and Risk Management; Information Sharing, Outreach and Awareness; Public Policy and Legislation; Research and Development and Workforce Development; Organization Issues and Public-Private Relations; and National Plan.

NERC is participating in the PCIS. The opportunities presented by PCIS include gaining a better perspective of the sector interdependencies, facilitating ISAC formation, and sharing of common research and development efforts.

NATIONAL PETROLEUM COUNCIL

COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

Progress Report to the
National Petroleum Council

January 10, 2001

The National Petroleum Council began its study on Critical Infrastructure Protection in late 1999 in response to a request from Secretary of Energy Bill Richardson. The Secretary asked the Council to provide advice on cooperative approaches to protecting the critical infrastructure of the oil and gas industry. The Secretary's letter states:

> The Federal Government is aggressively pursuing a variety of approaches through which the critical infrastructures of the United States can be protected from physical and cyber threats. To be effective, however, these approaches must be developed and implemented in partnership with the industry because the private sector owns and controls the vast majority of the Nation's critical infrastructures.
>
> Accordingly, I request the National Petroleum Council to review the potential vulnerabilities of the oil and gas industries to attack--both physical and cyber--and to advise me on policies and practices that industry and Government, separately and in partnership, should adopt to protect or recover from such attacks.

(The complete text of the Secretary's request letter is attached.)

SCOPE OF WORK

At the outset, the Council developed the following broad scope of work to focus and guide its study efforts:

- Develop a thorough understanding of the emerging overall federal program on Critical Infrastructure Protection and coordinate with other sectors (electric, telecommunications, transportation, finance, etc.) to benefit from their experience and analyses.

- Develop the Business Case for proceeding with discussion of "Cooperative Approaches" with industry and/or government.

- Define asset criticality and security risk in the context of Critical Infrastructure Protection for the oil and gas sector.

- Assess the vulnerabilities of the oil and gas sector to cyber and physical attacks. The assessment is to be a generic overview of potential vulnerabilities based on threat capabilities.

- Develop potential policies and practices that industry and government, separately and in partnership, should adopt to protect or recover from such attacks. This includes evaluating potential risk assessment models suitable for the oil and gas sector.

- Propose mechanisms through which industry can beneficially access relevant federal law enforcement and intelligence assets.

- Assess and make a recommendation concerning the need for an "Information Sharing and Analysis Center" for the oil and gas sector, similar to those that currently exist for safety.

- Study liability and legal impediments to information sharing and other concerns such as protection of confidential and proprietary information.

- Outline potential research and development requirements to enhance Critical Infrastructure Protection.

ORGANIZATION

With Secretary Richardson's approval, the Council established a Committee on Critical Infrastructure Protection to prepare a response to his request. The Committee is assisted by a Coordinating Subcommittee, which is evaluating the issues raised by the Secretary and is developing for the Committee's consideration, recommendations for alternative courses of action. (The Secretary's approval letter and the rosters of the Committee on Critical Infrastructure Protection and its Coordinating Subcommittee are attached.)

To facilitate the completion of its work, the Subcommittee has organized itself into a series of informal work groups. These groups are responsible for returning to the whole Subcommittee proposed report sections in the following assigned areas:

- Vulnerability Assessment and Reduction Measures

- Information Sharing and Analysis

- Federal CIP Program Coordination

- Legal and Liability Issues

The work groups meet as needed and the Subcommittee tracks overall progress at 30-60 day intervals. In addition, several "information sessions" have been held where all subcommittee members are given the opportunity to be briefed on the CIP activities of other industries as well as the emergency preparedness and response and recovery programs of the various federal and local agencies that may have a role.

The Department of Energy and the National Laboratories are providing significant technical and logistical support to the subcommittee and each subgroup. Additional federal support is being provided by the Departments of Commerce, Justice, Defense, and Transportation.

CURRENT STATUS

The Subcommittee has completed the basic research phase of its work and has begun analyzing this information in the context of the current realities of the global oil and gas Industry. The research has covered the plans and programs of the following government and industry groups.

Federal Level

- Office of the President
  - Presidential Commission on Critical Infrastructure Protection
  - Presidential Decision Directives 39, 62, and 63
- Department of Commerce
  - Critical Infrastructure Assurance Office
  - Partnership for Critical Infrastructure Security
- Department of Justice
  - FBI
    - -- National Infrastructure Protection Center
    - -- InfraGuard
    - -- Key Asset Program
  - Antitrust Division
- Department of Energy
  - Lead PDD 63 Agency for Electric Power, Oil, and Natural Gas
  - National Labs and Research Programs
- Department of Defense
  - Defense Information Systems Agency
  - U.S. Army
    - -- Director of Military Support
    - -- Corps of Engineers
- Department of Transportation
  - Office of Pipeline Safety
  - Coast Guard

Federal Level (Continued)

- Federal Emergency Management Agency
- Environment Protection Agency

State Level

- National Association of State Energy Officials
- New York State Energy Research and Development Authority

Local Level

- Harris County, Texas
  - -- Houston TranStar

Critical Industries and Their Information Sharing Approaches

- Electric Power – North American Electric Reliability Council
- Telecommunications – National Security Telecommunications Advisory Council
- Information Technology - Information Technology Association of America; World Information Technology Services Alliance
- Banking and Finance - Financial Services Information Sharing and Analysis Center; Banking Industry Technology Secretariat

The Subcommittee is now focusing on four major remaining areas of study:

- Legal implications of attacks and preventative and restorative measures for companies, shareholders, and employees
- Structure and operating principles for information sharing in the oil and gas industries including identification of proposed support contractor
- Role and identification factors of permanent sector coordinator for the oil and gas industries
- Overall report recommendations to government and industry.

The final attachment is the Subcommittee's current report outline. The various work groups have been assigned specific chapters and have developed initial drafts. Final drafting is being conducted concurrently with the work on the four remaining study areas. Both efforts will be brought together in the January-March timeframe in the form of the Subcommittee's consolidated draft of the overall study report.

TIMETABLE

Secretary Richardson's request of the Council fits into an overall governmental program that calls for critical infrastructure protection programs to reach "initial" operating capability in year 2000 and full capability no later than 2003. The following study timetable is consistent with that guidance:

December 1999	Scope of work approved and Coordinating Subcommittee staffed
January-June 2000	Subcommittee begins basic research and determines form of final report
June	Report progress and plans to Committee and Council
July December	Continue subgroup work and begin Subcommittee delib erations on consolidated report
January-March 2001	Complete Subcommittee analyses and finalize proposed recommendations and draft report
April-May	Subcommittee forwards its final draft report to the Committee, which then meets to review and comment
May-June	Committee forwards proposed final report to Council, which then meets to consider it as proposed response to Secretary of Energy's request. The date of this meeting tentatively has been set for June 6, 2001.

The Secretary of Energy
Washington, DC 20585

April 7, 1999

Mr. Joe B: Foster
Chair
National Petroleum Council
1625 K Street, N.W.
Washington, D.C. 20006

Dear Mr. Foster:

Thank you for your letter of December 14, 1998. I am writing to formally request the Council's advice on cooperative approaches to protecting the critical infrastructure of the United States oil and gas industry.

The Federal Government is aggressively pursuing a variety of approaches through which the critical infrastructures of the United States can be protected from physical and cyber threats. To be effective, however, these approaches must be developed and implemented in partnership with the industry because the private sector owns and controls the vast majority of the Nation's critical infrastructures. You have indicated that the Council believes it can contribute meaningfully to these efforts and can provide advice on a systematic approach to the planning process for protecting the critical infrastructures of the oil and gas industry.

Accordingly, I request the National Petroleum Council to review the potential vulnerabilities of the oil and gas industries to attack--both physical and cyber--and to advise me on policies and practices that industry and Government, separately and in partnership, should adopt to protect or recover from such attacks.

Specifically, I would like the Council to advise me on:

1. definitions of criticality and risk in the context of critical infrastructure protection of oil and gas system infrastructures;

2. remedies for legal concerns such as protection of confidential information and the ability of competing firms to participate in cooperative relationships, and

3. mechanisms through which the industry car, beneficially access relevant Federal law enforcement and intelligence assets and through which industry can both benefit from and help prioritize Government research and development programs in infrastructure assurance.

Finally, Presidential Decision Directive 63, which implements the recommendation of the President's Commission on Critical Infrastructure Protection, calls for me to designate a Sector Coordinator for the oil and gas industry. For the duration of your study, I would like the National Petroleum Council to take on the responsibility of the Sector Coordinator. At the conclusion of 'your work, I would like your advice on the permanent role of the Sector Coordinator and your recommendation on how that person or organization should be identified. The North American Electric Reliability Council has been designated as the Sector Coordinator for the electric industry and. to recognition of the growing interrelationship between the gas and electric industries. you should collaborate with that group as appropriate. Further, the Departments of Transportation and Energy have agreed to share critical infrastructure protection responsibilities for the Nation's oil and gas pipeline systems. Your advice, therefore, should consider oil and gas infrastructures from production to consumption.

Given the nature of this request, Under Secretary Emest J. Moniz will represent the Department and will provide appropriate coordination with the Department of Transportation and other branches of Government.

As always I appreciate the Council's ongoing assistance in these issues of national policy and mutual concern.

Yours sincerely,

Bill Richardson

Cc: Richard Clark
Rodney E. Slater
Erle Nye
Michehl Gent

The Secretary of Energy
Washington, DC 20585

October 15, 1999

Mr. Joe B: Foster
Chair
National Petroleum Council
1625 K Street, N.W.
Washington, D.C. 20006-1656

Dear Mr. Foster:

This letter conveys my approval to establish a Committee on Critical Infrastructure Protection and to appoint the members of the Committee as proposed in your letter of August 9, 1999.

The Government Co-chair for the Committee will be retired Air Force General Eugene E. Habiger, Director of the recently established Office of Security and Emergency Operations. The Office of Fossil Energy has substantial interest in this topic and will continue to work cooperatively with the Office of Security and Emergency Operations to address critical infrastructure issues related to the electricity, oil and gas industries.

I am pleased that the National Petroleum Council has accepted responsibility for reviewing the potential vulnerabilities of our Nation's oil and gas critical infrastructure and advising me on policies and practices that Government and industry, separately and in partnership, should adopt to ensure its integrity. The Council's willingness to additionally serve as the interim Sector Coordinator for the oil and gas Industry for the duration of your study is deeply appreciated.

Yours sincerely,

Bill Richardson

Bill Richardson

NATIONAL PETROLEUM COUNCIL

COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

CHAIR
David J. Lesar
Chairman of the Board, President
and Chief Executive Officer
Halliburton Company

GOVERNMENT COCHAIR
Eugene E. Habiger
Director
Office of Security and
Emergency Operations
U.S. Department of Energy

EX OFFICIO
Archie W. Dunham
Chair
National Petroleum Council

EX OFFICIO
William A. Wise
Vice Chair
National Petroleum Council

SECRETARY

Marshall W. Nichols
Executive Director
National Petroleum Council

* * *

Riley P. Bechtel
Chairman and
Chief Executive Officer Bechtel
Group, Inc.

David W. Biegler
President and
Chief Operating Officer
TXU

Peter I. Bijur
Chairman of the Board and
Chief Executive Officer
Texaco Inc

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Philip J. Carroll
Chairman and
Chief Executive Officer
Fluor Corporation

R. D. Cash
Chairman, President and
Chief Executive Officer
Questar Corporation

Robert B. Catell
Chairman and
Chief Executive Officer
KeySpan Energy

Hector J. Cuellar
Managing Director
Area/Industries Manager
Bank of America

Ronald A. Erickson
Chief Executive Officer
Holiday Companies

Ray L. Hunt
Chairman of the Board
Hunt Oil Company

Kenneth L. Lay
Chairman and
Chief Executive Officer
Enron Corp.

NPC COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

David L. Lemmon
President and
Chief Executive Officer
Colonial Pipeline Company

John H. Lichtblau
Chairman and
Chief Executive Officer
Petroleum Industry Research
Foundation, Inc.

Steven L. Miller
Chairman, President and
Chief Executive Officer
Shell Oil Company

James J. Mulva
President and
Chief Executive Officer
Phillips Petroleum Company

Richard B. Priory
Chairman and
Chief Executive Officer
Duke Energy Corporation

Daniel Rappaport
Chairman of the Board
New York Mercantile Exchange

Lee R. Raymond
Chairman, President and
Chief Executive Officer
Exxon Mobil Corporation

Richard E. Terry
Chairman and
Chief Executive Officer
Peoples Energy Corporation

Gerald Torres
Associate Dean for Academic Affairs
University of Texas School of Law and
Vice Provost
University of Texas at Austin

C. L. Watson
Chairman of the Board and
Chief Executive Officer
Dynegy Inc.

Daniel H. Yergin
President
Cambridge Energy Research Associates

NATIONAL PETROLEUM COUNCIL

COORDINATING SUBCOMMITTEE
OF THE
NPC COMMITTEE ON
CRITICAL INFRASTRUCTURE PROTECTION

CHAIR

Charles E. Dominy
Vice President
Government Affairs
Halliburton Company

GOVERNMENT COCHAIR

Paula L. Scalingi
Director
Office of Critical Infrastructure Protection
U.S. Department of Energy

ASSISTANT TO THE CHAIR

Forrest L. Carpenter
Manager
Computer Security and
Business Continuity Planning Global
Information Services Texaco Inc.

SECRETARY

Marshall W. Nichols
Executive Director
National Petroleum Council

* * *

Raymond W. Bergeron
Manager
Corporate Security
Shell Oil Company

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Thomas D. Carmel
Corporate Counsel
Conoco Inc.

Donald M. Field
Executive Vice President
Peoples Energy Corporation

Bobby R. Gillham
Manager Global Security
Conoco Leadership Center
Conoco Inc.

Lawrence J. Goldstein
President
Petroleum Industry Research
Foundation, Inc.

Michael C. Hicks
Manager
Security
Enron Property & Services Corp.

Thomas R. Holland, Jr.
Manager
Corporate Security – Worldwide
Phillips Petroleum Company

Harry Kremling
Managing Director ans
Client Manger
Engineering and Construction Sector
Banc of America Securities LLC

Kevin J. Lindemer
Senior Director
Refined Products
and Global Downstream
Cambridge Energy Research Associates

COORDINATING SUBCOMMITTEE OF THE NPC COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

David J. Manning
Senior Vice President
Corporate Affairs
KeySpan Energy

James R. Metzger
Vice President and
Chief Technology Officer
Texaco Inc.

Rolando D. Moss
Senior Director
Corporate Security
Dynegy Inc.

A. R. Mullinax
Senior Vice President
Global Sourcing and Logistics
Duke Energy Corporation

Frank B. Sprow
Vice President
Safety, Health & Environment
Exxon Mobil Corporation

Catherine A. Travis
Director
Information Security
Questar Corp.

Vic A. Yarborough
Vice President Technology
Colonial Pipeline Company

SPECIAL ASSISTANTS

W. R. Finger
President
ProxPro, Inc.

Ronald E. Fisher
Deputy Director
Infrastructure Assurance Center
Argonne National Laboratory

Joseph A. Gurga
Manager
Program Office
Information Technology Services
Peoples Energy Corporation

John R. Johnson
Principal Advisor
Shell Services International

Stuart L. Schertz
Senior Security Representative
Corporate Security
Shell Oil Company

Curtis R. Smith
Manager
Information Security
Conoco Inc.

Richard D. Vance
Strategic Business Consultant
Duke Energy Corporation

Peter van de Gohm
Director
Information Assets Protection
Enron Energy Services

National Petroleum Council

Securing the Energy Industry in the New Economy

Draft Report Outline of the NPC Committee on Critical Infrastructure Protection

---

I. PREFACE

II. EXECUTIVE SUMMARY

III. FINDINGS AND RECOMMENDATIONS

IV. CHAPTERS

Chapter 1. Purpose and Objectives.

A. Blueprint for Action (strategy document "go forward" view) Brief Discussion of "New Economy" and IT Revolution.

B. Motivation (why committee was commissioned - list members in appendix).

1. Assure Security and Business Continuity of Industry to Meet New Challenges.

2. Raise Level of Awareness and Understanding Within Industry and Government.

3. Identify Necessary Actions and Recommend Appropriate Implementation Steps

Chapter 2. Background.

A. Chapter Summary.

B. Energy Industry Characterization (description, structure of oil and gas industry, dependence on information technology, energy industry interconnectedness [including electric power], interdependencies with other infrastructures [telecommunications, transportation, etc.]).

C. Description of Evolving Energy Industry (market dynamics, diversification, financial posture, new customers, non-traditional competitors, new retail outlets, etc.).

Chapter 2. Background (continued):

D. Importance to Overall Economy, Quality of Life, Human Health and Safety, National Security.

E. New Challenges of the 21st Century.

1. Impacts of New Economy (internal to energy industry, external).
    a. Increased Reliance on E-Commerce and Electronic Markets.
    b. Globalization.
        1. Increase of Foreign Partnership / Ownership
        2. Socio-Economic and Political Impacts.
    c. Interdependencies (growth in electric power usage, ownership of joint infrastructures, joint vulnerabilities [common corridor]).
    d. Workforce (retention, new skill requirements, training and awareness).

2. Restructuring.
    a. Supply / Demand (natural gas as future energy of choice).
    b. New Industry Participants (marketers).
    c. Convergence of Energy Enterprise (providers, markets, systems).
    d. Deregulation of Energy Industry
    e. Lower R&D Budgets

3. Other Major Trends.
    a. Increased Utilization of Assets (JIT) Reduces Spare Capacity.
    b. Reduced Flexibility (rerouting, maintenance).
    c. Lack of Incentives for Capital Expenditures for Infrastructure Upgrades).
    d. Pipeline Maintenance and Vintage.
    e. Environmental Mandates and Barriers (can't get permits).
    f. Increase in Petroleum Imports.

F. Critical Infrastructure Protection

1. New and Broader Threat Environment and Risks
2. Public Perspectives.
3. National/ Industry Perspectives.
4. International Perspectives

Chapter 2. Background (continued):

G. Opportunity to Leverage Y2K Experience (established relationships, organizational structure, IT reliance).

1. Baseline of Information, Response, and Recovery Plans.

2. Set Up Mechanisms for Information Sharing Industry Wide.

3. Preserve and Sustain the Emergency Management Capabilities.

Chapter 3. Threats.

(Objective: gain a sound understanding of industry threats.)

A. Chapter Summary.

B. Threat Environment *(cascading disruptions to infrastructures*).

1. Information Technology based threats.

2. Physical or "Traditional" threats.

3. Natural threats.

4. Regulatory and Restructuring threats.

5. Man-made threats.

6. Interdependency threats.

C. Strategy for Developing Best Practice Methodologies, as appropriate.

Chapter 4. Vulnerabilities.

(Objective: gain a sound understanding of industry vulnerabilities.)

A. Chapter Summary.

B. Definitions of Key Terms and Industry /Government Perspectives.

C. High-Level Overview of Vulnerabilities in the Oil and Gas Sector.

D. Characterization of Criticality of Infrastructure Components from Stakeholders' Perspective (company, industry, public, government).

E. Characterization of Current Assessment Practices and Methodologies.

F. Strategy for Developing Best Practice Methodologies, as appropriate

Chapter 5. Risk Management (including mitigation).
(Objective: gain an understanding of risk management in the new economy, develop a strategy for identifying and producing best practices and methodologies, and build a business case for industry acceptance.)

A. Chapter Summary.

B. How/Why Risks are Different, Methods to Measure Risk and Risk Evaluation.

C. Characterization of Criticality of Infrastructure Components from Stakeholders' Perspective (company, industry, public, government).

1. Critical Assets (definitions, perspectives, prioritization)

D. Strategy for Developing Best Practice Methodologies, as appropriate.

1. Characterization of Current Assessment Practices and Methodologies.

2. Survey Existing Models (insurance industry, audit, accounting standards).

E. Resource Allocation To Mitigate Risks.

F. Relevant Issues.

1. Liability /Indemnification (open-ended liability, industry as target.

2. Funding.

3. Public/ Shareholder Perceptions.

Chapter 6. Response and Recovery.
(Objective: evaluate the need for enhancing response and recovery plans and procedures to meet the challenges of the new economy at the regional, national, and international level.)

A. Chapter Summary.

B. Current State of Response and Recovery Plans and Procedures Including Informal Agreements.

C. Incorporate Lessons Learned From Y2K Contingency Planning into Response and Recovery Planning.

D. Evaluate Optimal Models, e.g., Oil Spill, MMS, CDC, NRC, FEMA, IEA.

E. Gaps and Recommend Additional Enhancements.

F. Best Practices.

G. Periodic Tests (benchmarks, table tops, communications).

Chapter 6. Response and Recovery (continued):

A. Technologies and Methods.

B. Discussion of Roles/Responsibilities/Coordination/Jurisdiction/Cooperation.

1. Industry.
2. Local.
3. State.
4. Federal.
5. Public.
6. International Entities.

Chapter 7. Information Sharing.

(Objective: determine to what extent information should be shared and how.)

A. Chapter Summary.

B. What are the Drivers for Sharing Information?

C. What Information Does Industry Need to Meet the Needs of the New Economy?

D. What are Some of the Barriers to Sharing Information?

E. Ways Information is Currently Shared in Industry-Formal and Informal.

F. Ways Information is Currently Shared between Industry and Government - Formal and Informal.

G. Emerging Models for Information Sharing (Banking & Finance, NSTAC, etc.).

H. Classification Issues/ Confidentiality Agreements.

I. Outline Requirements for the Oil and Gas Sector.

J. Address Foreign Ownership or Controlling Interests.

Chapter 8. Legal and Regulatory Issues.

(Objective: discussion of barriers, incentives, and actions required.)

A. Chapter Summary.

B. Identification of Barriers.

C. Standards (Are they useful or necessary?)

Chapter 8. Legal and Regulatory Issues. (continued):

A. FOIA and Other Information Sharing Issues

1. Anti-Trust.

2. Corrupt Practices Act.

3. Lobbying Disclosure Act.

4. Foreign Agents Registration Act.

5. Privacy Act.

B. Government (federal, state, and local).

Chapter 9. Research and Development Needs.
(Objective: identify gaps, and appropriate roles for industry and government in meeting R&D needs)

A. Chapter Summary.

B. Outline a Strategy For a Needs Assessment Based on Vulnerabilities and Risk Management.

C. How to Accomplish and Keep Current.

1. Industry Roles and Missions.

a. Technology Transfer from Industry to Government.

2. Government Roles and Missions.

a. Technology Transfer from the Government to Industry.

V. APPENDICES

A. Request Letter.

B. Study Rosters.

C. ,etc. (to be developed).

December 10, 2000

Mr. Richard A. Clarke
National Coordinator, Security, Critical Infrastructure Protection, and Counter-Terrorism
National Security Council
The White House
Washington, DC 20504

Dear Mr. Clarke,

The Coordinating Committee of the Partnership for Critical Infrastructure Security is pleased to provide you this status report of its significant activities in the area of critical infrastructure assurance. We trust that this will help in your planning with the transition to a new Administration, and we pledge our support. Please feel free to call on any Coordinating Committee member for additional information or planning assistance.

On behalf of the Coordinating Committee,

Kenneth C. Watson
Cisco Systems, Inc.

Attachments:
Coordinating Committee Members
Status Report

Attachment 1. Coordinating Committee Members

William G. Bishop, III
The Institute of Internal Auditors, Incorporated

Matthew Flanigan
Telecommunications Industry Association

Richard Holmes
Union Pacific Corporation

Jeffrey M. Jaffe
Lucent Technologies

Stephen C. Jordan
U.S. Chamber of Commerce

Stephen R. Katz
Citigroup

Lou Leffler
North American Electric Reliability Council

Harris Miller
Information Technology Association of America

Roy Neel
United StatesTelephone Assocation

Marshall W. Nichols
National Petroleum Council

Richard J. Perlot
SBC Communications, Incorporated

Louis L. Rana
Consolidated Edison Company of New York, Incorporated

Ty R. Sagalow
American International Group, Incorporated

Howard A. Schmidt
Microsoft Corporation

Diane VanDe Hei
Association of Metropolitan Water Agencies

Kenneth C. Watson
Cisco Systems, Inc.

Nancy Wilson
American Association of Railroads

Robert E. Wright
BellSouth

William G. Bishop, III
THE INSTITUTE OF INTERNAL AUDITORS, INCORPORATED

Richard Holmes
UNION PACIFIC CORPORATION

Jeffrey M. Jaffe
LUCENT TECHNOLOGIES

Stephen C. Jordan
U.S. CHAMBER OF COMMERCE

Stephen R. Katz
CITIGROUP

Richard J. Perlot
SBC COMMUNICATIONS, INCORPORATED

Louis L. Rana
CONSOLIDATED EDISON OF NEW YORK, INCORPORATED

Ty R. Sagalow
AMERICAN INTERNATIONAL GROUP, INCORPORATED

Howard A. Schmidt
MICROSOFT CORPORATION

Kenneth C. Watson
CISCO SYSTEMS, INCORPORATED

Robert E. Wright
BELLSOUTH CORPORATION

Partnership for Critical Infrastructure Protection Status Report: November 2000

We, the Coordinating Committee of the Partnership for Critical Infrastructure Security, strongly believe that protecting America's critical infrastructures is and will remain an extremely significant economic and national security issue, requiring coordinated, focused, diligent effort by both the private sector and the Federal Government. Just as with the Year 2000 turnover effort, a coordinated public-private partnership, supported at the highest levels of government and industry, will help promote the actions necessary to preserve our economic and national security. Unlike Y2K, however, this threat and concomitant risk are very difficult to quantify, and there is no given end date against which to plan.

Federal Government Perspective

The US Government has approached industry for help in developing coordinated solutions to counter emerging national security threats. Malicious attacks can come from hackers inside and outside the United States or organized and funded information warriors from potentially hostile foreign governments or extra-national organizations. Unlike traditional threats, in the case of cyber attack, the national security apparatus has little ownership or control of the networks, no jurisdiction in the case of foreign threats, limited intelligence on threats and vulnerabilities, and insufficient research and development capability to develop countermeasures.

US Industry's Perspective

Businesses are just as dependent on electronic information systems and the emerging Internet capabilities for their survival, and work zealously to protect and defend their interests. The same vulnerabilities that threaten national security also threaten economic survivability and competitiveness. Additionally, the infrastructures are themselves interdependent. Banks depend on telecommunications for electronic transactions. Telecommunications companies must have electric power to operate. In turn, much of our electric grid depends on telecommunications. In the United States, individual companies and sectors have begun to address vulnerabilities and develop countermeasures, but the significant interdependencies and the national security component mandate a more coordinated approach.

Public-Private Partnership: The New "Civil Defense"

In close coordination with the Department of Commerce, we launched the PCIS on December 8, 1999, dedicating our efforts to assuring the delivery of essential services over the nation's critical infrastructures. We subsequently organized the PCIS into issue-oriented working groups, and we are collaborating with the Federal Government to write the first-ever coordinated public-private national plan. The PCIS represents a cross-sector industry partnership, but with federal, state, and local government participants, to better address issues of common concern.

The PCIS followed its kick-off meeting with a planning retreat February 22, 2000 in Washington DC, establishing initial working groups and plans. Industry responded enthusiastically. Key companies volunteered to chair the working groups and an ad hoc planning committee, and most participants devoted many hours to working group efforts, hammering out issues for resolution, courses of action, and recommendations for industry. The three major functions established for the PCIS were:

- to provide a mechanism for cross-sector coordination and dialog on critical infrastructure security issues, within industry and with government;
- to facilitate and coordinate cross-sector industry input into subsequent versions of the National Plan; and
- to provide a means to contribute to appropriate government advisory bodies.

The PCIS ad hoc planning committee established the following Working Groups:

- Working Group #1: Interdependency Vulnerability Assessment and Risk Management
- Working Group #2: Information Sharing, Awareness, and Outreach
- Working Group #3: Public Policy and Legislation
- Working Group #4: R&D and Workforce Development
- Working Group #5: Organization Issues and Public-Private Relationships

On July 25-27, 2000, the PCIS met in San Francisco to review the past six months' work, make critical decisions regarding formal organization, and outline the work plan for the next six months. Sector Coordinators, as identified PDD-63, established the PCIS Coordinating Committee as its governing body and identified tasks to:

- move toward a legal, formal organization;
- prioritize the tasks for PCIS Working Groups;
- make membership and support decisions;
- establish a National Plan Working Group (NPWG); and
- continue to make use of the services of the CIAO and US Chamber of Commerce as joint secretariat for the PCIS.

The 162 attendees represented key companies from all critical US infrastructure industries, US federal, state, and local governments, Canada, and Switzerland. Working Group reports illustrated significant work accomplished and outlined an aggressive plan for the next six months. The next meeting is scheduled for March 20-21, 2001 in Washington, DC.

Next Steps

Recognizing that some infrastructures were already at work on single-sector issues involving both government and industry, the Coordinating Committee established the following operating principles to ensure added value to the sectors:

- Build on and complement work of the critical infrastructure sectors identified in PDD-63;
- Support efficiency and add value to ongoing work by identifying and addressing critical common and shared issues across sectors;
- Take on only those initiatives that complement and provide additional efficiencies for the sectors or that otherwise cannot or will not be done; and
- Act as a catalyst for action for existing entities whenever possible.

The PCIS prioritized seven key issue areas meriting priority of effort over the next several months.

1. The next version of the National Plan for Information Systems Protection. The US Government recognized the limitations of its first version as government only, limited to the cyber dimension, and lacking an international perspective. By engaging industry, the next version will address public and private efforts, include both cyber and physical dimensions of protection, and incorporate international issues. The next version of the plan is intended to include input from all 13 Federal key agencies, the 8 critical infrastructure sectors, PCIS working groups, and state and local fire, law enforcement, and emergency services organizations.

2. Interdependency. One area the PCIS can address more easily than a single sector is interdependency risk assessment and management. Industry Sector Coordinators universally endorsed this as the second-most important task to be completed. PCIS Working Group #1 completed a "lessons-learned" study from the Y2K turnover effort and presented its results in July. It also began to identify the information needed to begin a useful study of interdependencies between sectors. It set a work plan to expand its sources of information on interdependency work that has already been done, to define a proposal for a real-world business simulation that will include all critical infrastructure sectors, and to identify a business case for developing a common interdependency risk assessment approach across sectors.

3. Inclusion of state and local governments. To date, the PCIS has had only limited representation from state and local governments. In local communities, private industry has a long history and comfort level in working with state and local governments on various critical service assurance issues. Since state and local governments also make up most of the emergency services first responders and perform the critical coordinating function in local areas for both industry and government, the PCIS is organizing outreach to the National Association of State Information Resource Executives, National Council of Mayors, National Governors' Association, and other groups. We are also encouraging businesses to join state and local chapters of the National Infrastructure Protection Center's InfraGard program.

4. Legislative and regulatory issues. Working Group #3 developed and presented a public policy white paper, "Legal Challenges for Cyber Security Cooperation", to the Partnership in July. It examines legal issues and challenges associated with cyber security risk management issues, some of the challenges seen as legal impediments to industry and cross-sector cooperation, and some of the legal risks that may undermine common sense strategies and prudent risk management activities. In addition, the group sponsored a web cast on the subjects of the white paper to garner more input and explore the issues with a wider range of participants. The group has identified specific issues on which they will explore in greater detail through white papers to be developed as part of their work plan for March 2001. Specific issues that the group will follow up on include: FOIA, antitrust, liability, state of Congressional response to issues acting as impediments to intra- and inter-sector cooperation, and international dialogue and status of cooperation. To support research needed to develop its papers, the group has developed a cooperative relationship with a local university.

5. Awareness. Building awareness and a case for action within industry and government emerges as the foundation for involvement and program implementation for all PCIS working groups, as well as a broad infrastructure security need. This issue is so complex and so basic to society that services delivered over the critical infrastructures are often taken for granted. The Partnership recognized that an intensive six-month program of conferences for chief auditors, Boards of Directors, and other executive corporate officers reached its critical audiences. However, we believe much more is needed. In July, Working Group #2 developed and presented an analysis of Critical Infrastructure Protection awareness program activities. This study resulted in a roadmap of awareness program goals and identified key audience groups. It provided a matrix of current cross-sector awareness programs, identified who is delivering them, and outlined delivery methods. Finally, the presentation included a gap analysis, highlighting efforts that the PCIS could encourage or take action on. The working group plans to move forward by:

- building a "living" repository of outreach activities that itself can provide wider access to and knowledge of awareness activities;
- implement a program specifically to improve awareness of the Partnership;
- develop metrics for effectiveness for key audiences; and
- identify additional programs to address "gaps."

6. Research & Development. The Federal Government has allocated $650 million to critical infrastructure security research, and several companies have robust research and development programs. Universities and other academic institutions are also conducting research in improving network security. However, there is no clearinghouse or mechanism to coordinate all these efforts. In July, working group #4 delivered a preliminary report on priority R&D topics. The PCIS will undertake to develop a full "CIP Research and Development Roadmap," to recommend to industry where to focus its efforts and to help government avoid duplication of effort.

7. International collaboration. This is not a US-only problem. Much of industry operates and delivers services and products on a global scale. The industry participants of the PCIS believe that the international dimension of critical infrastructure security has not been adequately addressed to date. The PCIS will actively engage in international outreach, to encourage

countries and nation unions to develop similar partnerships and to share information regarding threats, vulnerabilities, countermeasures, and best practices. We invite their attendance at our meetings, and would very much like to be kept informed of similar efforts elsewhere.

In the Internet Economy, no country or company can completely define its perimeter, and therefore we are all in this together. Working together, we can raise the bar of security worldwide, empowering the Internet generation as we move into the Internet century.

Partnership for Critical Infrastructure Security
Working Group 3
Public Policy White Paper

Executive Summary

- This working paper examines legal issues and challenges associated with cyber security risk management activities in the context of building a public policy framework to support these activities.

- There are several key assumptions underlying this framework: (1) that public-private partnerships are essential to meet challenges posed by new technologies and non-traditional threats; (2) that 20th-century government command-control policy frameworks and attitudes toward industry cooperation need to be adapted and modified to facilitate this partnership; and (3) that both the public and the private sectors have to walk a fine line in balancing security, commercial and public interests.

- The foundation of U.S. public policy should be to pursue the following: (1) establish guidelines for voluntary private sector information sharing with the government and within industry that address FOIA, anti-trust, and liability concerns. (2) establish guidelines for private sector cooperation with law enforcement that balance commercial and security interests. (3) Work toward fostering minimum global standards for law enforcement and private sector cooperation and toward establishing international conventions on critical infrastructure protection taking into account local cultural and social differences.

- At the international level, the Working Group suggests that the next Administration will have to walk a fine line between creating minimum levels of cooperation to enhance law enforcement and standards that try to impose government command and control models as opposed to models that enhance public-private cooperation. In addition, it would be very useful to develop a model template of security protections and civil measures, particularly for countries in Asia and Latin America currently lacking systematic approaches to the problem of e-security and critical infrastructure protection.

- Future issues to be addressed include: safeguarding trade secret protections, tax issues and incentives, simplifying industry-government agency relationships, clarifying government roles and responsibilities vis-à-vis industry, and identifying state and international legal and public policy issues.

Partnership for Critical Infrastructure Security

Legal and Public Policy Challenges for Critical Infrastructure Protection

White Paper

Table of Contents

Partnership for Critical Infrastructure Security

Legal and Public Policy Challenges for Critical Infrastructure Protection

White Paper

Introduction

This working paper examines legal issues and challenges associated with cyber security risk management activities in the context of building a public policy framework to support these activities.

There are several key assumptions underlying this framework: (1) that public-private partnerships are essential to meet challenges posed by new technologies and non-traditional threats; (2) that 20th-century government command-control policy frameworks and attitudes toward industry cooperation need to be adapted and modified to facilitate this partnership; and (3) that both the public and the private sectors have to walk a fine line in balancing security, commercial and public interests.

The United States currently operates under a public policy framework that is gradually shifting in response to the changed nature of economic security. However, many of the vestiges of twentieth century security structures and approaches still remain. While the U.S. is very well suited to handle conventional assaults, and has developed sophisticated strategies to deal with a wide range of military threats, more emphasis needs to be placed on integrating economic security measures into its strategic thinking.

The U.S. today is characterized by interdependence – government and industry have interwoven and entwined interests, to the point where it is estimated that almost 90% of the country's critical infrastructure is owned or administered by the private sector. As we enter the new millennium, cyber-terrorism, computer intrusions, and insider threats – whether through malicious acts or benign neglect -- may all contribute to a critical and costly problem for the U.S. business community, and by extension, to the U.S.'s economic sustainability and critical infrastructure security.

To ensure that America's critical infrastructures are protected, the government must work closely with the private sector. In the past, this was simply a question of setting up a command-and-control structure, but there are several reasons why this framework needs to be changed. First, there is a question of resources. By pooling resources, the government can leverage private sector assets, while at the same time, individual companies can tap into larger resources to better safeguard their private interests as well.

Second, there is a fundamental trade-off in economic security. Critical infrastructure protection has to be looked at, not just in terms of security, but in terms of its impact on commerce and trade as well (it goes without saying that there is also a fundamental link with civil liberties). The government should develop cost-benefit tests to determine whether a tool like the FBI "Carnivore" program is invasive/valuable. This requires a nuanced and "political" approach to the issue, and the optimal way to achieve

these benefits is by adopting a consultative approach before such tools are developed and implemented.

Third, partnerships represent a strategic choice for both the government and its private sector partners – voluntary commitments place less regulatory burdens but require more trust and openness.

Finally, there is the nature of the threat environment in a networked community. Threats and incidents can happen to anyone at any time in seemingly random patterns. If only for this reason, the ability to gather input from many sources is important.

However, to encourage private sector entities to voluntarily work with government, and to cooperate amongst themselves, protections and incentives must be given to businesses. Government agencies must recognize that while the private sector collectively may have access to vast resources, individually companies have finite resources and have fiduciary obligations to their stockholders that may constrain their public involvement. To the extent that government agencies can incentivize cooperation, reduce regulatory and security burdens, the greater the ability will be for individual companies to participate in security partnerships.

In discussions with elected officials and government agencies, the business community must be able to articulate what barriers exist that could hinder the private sector's ability to manage risks associated with cyber security – many of which are not fully understood, but all of which may result in substantial harm and liability to the commercial sector.

It is also important that security partnerships be attractive to all of the critical infrastructure industries and be inclusive rather than exclusive. In this regard, government agencies should be cognizant that different industries face different constraints and different threats and should work to make partnership models as attractive as possible for all of the critical infrastructure industries.

As Metcalfe's Law states: *the value of a network grows by the square of the size of the network*. So a network that is twice as large will be four times as valuable because there are four times as many things that can be done due to the larger number of interconnections. It is on the basis of this understanding that this public policy analysis seeks to enhance the power, and the potential, of the partnership model.

That being said, this White Paper is a work in progress. It is designed to serve as a basis for discussion for the development of public policy to enhance public-private cooperation and critical infrastructure security.

I. FOIA - Impediments to Sharing Information With the Government

Under the Freedom of Information Act ("FOIA"), there is a presumption that records in the possession of agencies and departments of the executive branch of the U.S. Government are accessible to the people. Recognizing the legitimate need to restrict disclosure of some information, and to promote cooperation with statutes and regulations, however, Congress has provided for numerous exemptions under which information is not subject to disclosure.

At present, it is not clear that any of the existing FOIA exemptions would provide the certainty of protection that many companies would require before believing that they could safely disclose threat and vulnerability information to the government. The Davis-Moran Act, currently being considered by Congress, would provide some level of protection for private sector companies that voluntarily provide cyber-security information to the government under certain circumstances. It is uncertain whether this legislation will pass.

Recommendation: Companies need to consider the FOIA issue as they work together to develop coherent and workable policies to encourage the voluntary disclosure of threat and vulnerability information to the government.

Hypothetical

The financial services industry is alerted to a pattern of internet-based attacks in which small amounts of money are wired out of numerous customer accounts and transferred overseas, where it becomes unrecoverable. In all cases, the banks have restored the funds to the customer accounts, so no individual customers were harmed; nevertheless, the reputational harm that could be caused has led to many institutions being apprehensive about their own vulnerabilities being disclosed to the general public.

Consider the case of three National Banks, Alpha Bank, Bravo Bank and Charlie Bank, who perform risk assessments, and learn of vulnerabilities to their systems under which such an attack could take place. While the type of threats, and resulting vulnerabilities are similar, the information is disclosed to the government under three very different scenarios.

Several of the Federal banking regulators, including the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision, and the Federal Reserve, have asked their regulated institutions for information about these threats to help in the Federal government's analysis of this activity. A consumer watchdog group that focuses on careless banking practices – ALERT -- learns of the losses, and files a FOIA request to make the information gathered by the agencies public.

For these examples, assume that The Davis-Moran Act has been signed into law, so there is a specific FOIA exemption for information about cyber threats voluntarily disclosed pursuant to a government request.

- Alpha Bank voluntarily shares information about a discovered software threat with the Office of the Comptroller of the Currency. Based upon Davis-Moran, the relevant agency FOIA administrator notes that the information was disclosed pursuant to a specific agency request, and *automatically* excludes Alpha Bank's disclosure from ALERT'S FOIA request without the need for further inquiry.

- Bravo Bank's software vulnerability information is inadvertently disclosed to the OCC while bank inspectors are reviewing Bravo's practices to ensure compliance with existing regulations. When ALERT's FOIA request is presented to the OCC FOIA administrator, Bravo Bank's disclosure does not fall within the Davis-Moran automatic exemption, and is not otherwise exempt under recent case law on the topic. The information is released to ALERT, which posts Bravo Bank on its "risky banks" web page.

- Charlie Bank discloses their vulnerability information at an industry conference on electronic banking. An OCC employee is present, and the information is put in a report and given to the division contemplating agency action. Charlie Bank's disclosure is not within the Davis-Moran exemption, and is not otherwise exempt under FOIA law and practice, so its vulnerability information is also released to ALERT and posted on the consumer watchdog's web page.

* * *

Companies should be advised that these are conceivable scenarios and should take suitable notice. As shown by these examples, there may not be sufficient protection currently offered to private-sector entities that disclose threat and vulnerability information to the government. Unless the Partnership acts to improve industry confidence, it is likely that some companies may view government requests for such information with a wary eye. Thus, changes to FOIA may be needed to remove private sector concerns about sharing information on critical infrastructure threats.

References:

Current Legislative proposals

H.R. 4246, Cyber Security Information Act 2000/Davis-Moran legislation

Examples of laws passed

1998 Y2K Information and Readiness Disclosure Act

Over eighty FOIA Exemptions throughout body of US law (e.g., filing patent application; submitting census information; filing IRS tax returns).

Financial Institutions, Suspicious Activity Report (SAR) form (covers financial institutions regulated by the Department of Treasury (OCC and OTS), Federal Deposit Insurance Corporation, Federal Reserve, National Credit Union Administration).

Legislative Next Steps

House Government Reform Subcommittee on Government Management, Information and Technology markup

II. Antitrust – Cyber Security Cooperation and Related Activities

Businesses need protection from unnecessary restrictions placed by Federal and state antitrust laws on critical information sharing. However, antitrust concerns reach beyond information sharing and encompass the full range of security cooperation strategies.

Neither the Department of Justice nor the Federal Trade Commission has embraced the need to develop voluntary guidelines for cyber security cooperation – similar to the guidelines the Federal government developed covering the health care industry.

Regardless of whether Davis-Moran passes, the PCIS would benefit from outlining an antitrust strategy that permits full and robust cooperation on security issues. Efforts within the administration might focus on both the FTC and DOJ staff responsible for recent guideline development (see, e.g., Antitrust Guidelines for the Licensing of Intellectual Property – (http://www.usdoj.gov/atr/public/guidelines/ipguide.htm). A similar state-based strategy may be necessary to preclude prosecution within the states.

Awareness and dialogue on security cooperation is an essential ingredient for managing legal risk associated with security cooperation. A PCIS antitrust strategy cuts across all sectors and works to limit liability in this important area.

Recommendation: Companies should inquire with the FTC and DOJ about guideline development for cyber security cooperation.

Recommendation: Companies should be aware that antitrust concerns reach beyond information sharing and encompass the full range of security cooperation strategies.

Hypothetical

Security officials from twelve petroleum companies, representing 80 percent of the industry, are meeting to form an ISAC. Possible security cooperation includes:

- Sharing of threat and vulnerability information, discussing and disseminating industry standards and practices, and sharing other relevant data;
- Using ISAC data to perform research and development activities in the cyber security area, and/or
- Licensing software products, developed by the ISAC with industry data, to identify threats peculiar to the petroleum sector.

* * *

This example is intended to highlight three distinct areas of security cooperation that may lead to antitrust liability. Federal antitrust law and policy is concerned with furthering competition in the marketplace. Certain types of agreements, cooperative arrangements, and information sharing amongst industry participants may have anticompetitive effects. This is especially the case where the agreements (or, collaborative models) have the effect of raising prices or reducing outputs – irrespective of intent.

Thus, even though the ISAC participants in the hypothetical do not intend to violate antitrust law, both the Federal Trade Commission and the Department of Justice, as the government's lead agencies for antitrust enforcement, may bring an action against the industry participants.

Both the Department of Justice and the Federal Trade Commission understand that cooperation may actually further competition and make good business sense. As a result, both agencies have carefully developed and issued several Statements of Antitrust Enforcement Policy ("Joint Antitrust Statements"), clarifying issues of cooperation among competitors. Published statements include:

- Licensing of Intellectual Property;
- Health Care Joint Ventures and Mergers;
- Collaborations Among Competitors; and
- Joint Venture Relationships – including international partners and corporations.

The Joint Antitrust Statements explicitly spell out what types of ventures, agreements, and activities fall within a "safety zone" of acceptable activities, as well as what activities are *per se* illegal; the Joint Antitrust Statements additionally provide a "rule of reason" analysis for those otherwise falling outside the safety zone.

From the PCIS perspective, we are discussing cooperation among competitors in high profile and politically charged industries, such as petroleum companies, Internet Service Providers, financial services, and insurance. The mere cooperation of large segments of various markets may raise questions by non-participating members in relevant markets, regulators, consumer organizations, and a variety of other political actors, candidates, agencies, and non-government organizations – thus increasing the risk of participation.

Although it is possible, and perhaps even likely, that DOJ/FTC analysis of security-related cooperation would ultimately be found to have a legitimate purpose, and not foster anticompetitive effects, the better course of action might be for the PCIS to consider fully the range of potential antitrust liability, and to seek guidance and statements of policy from DOJ/FTC. These statements will work to limit and manage risk associated with cooperation activities.

There are, of course, models that the PCIS may utilize in discussions with relevant agencies and regulators. For example, most critical infrastructure protection programs

will have a major R&D component. The question arises whether there is some language or provision that can be borrowed to serve as a model. There are several industry cooperation models operating under legislative provisions currently in place such as the National Center for Manufacturing Sciences and the Semi-Conductor Research Corporation, so that the private sector does have meaningful experience that can be applied. The U.S. Government has already developed antitrust policy on research and development activities, on IP licensing, and on joint ventures – and these models may easily be applied to PCIS activities as well.

Recommendation: Corporate representatives should explore existing models of legislation and apply past experience and lessons learned from these models to new CIP issues.

References:

Current Legislative proposals

H.R. 4246, Cyber Security Information Act 2000

Examples of laws passed

1998 Y2K Information and Readiness Disclosure Act

U.S. Dep't of Justice, Justice Department Merger Guidelines, 49 Fed. Reg. 26,823 (1984), *reprinted in* 2 Trade Reg. Rep. (CCH) No. 655 PP4490-4495 (June 18, 1984).

1984 National Cooperative Research Act; 15 U.S.C. 4301.

III. Liability – Managing Risk for Owners/Operators of Infrastructures

Businesses need to be shielded from legal liability for a wide range of risk management planning activity – such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information.

The PCIS should carefully and comprehensively consider liability concerns from commercial, technological, and legal perspectives. The PCIS should use the Interdependency Vulnerability Assessment Working Group's findings as it determines how to prioritize immediate/current risk concerns in terms of how they should be approached in the public policy arena. Liability issues and solution sets should complement PCIS efforts in other working groups and operate across all critical infrastructure sectors.

Current concerns for liability reach well beyond information sharing – which largely defined the legal concerns for the past two years. Information sharing is a foundation issue for the PCIS, and thus liability resulting from the sharing of threat and vulnerability information is very real. There are, however, broader, and perhaps weightier liability concerns that are of immediate commercial importance.

Recommendation: Businesses should be aware that issues to be addressed in this field include:

- Defining state-based duties of care for corporate senior management as well as directors/officers.
- Analyzing the impact of the recently released Gramm-Leach-Bliley cyber-security regulations and discussing whether the PCIS should comment on the agencies' implementation plans – especially since coverage will include entities beyond the financial services community.
- Discussing vendor-management legal issues, including whether/how due diligence models are possible to implement in the Information Age.
- Analyzing whether damages should be capped for downstream harm resulting from cascading impact. This may be an appropriate area for Federal preemption.
- Identifying appropriate roles for Federal and state government to limit liability for owners/operators of critical infrastructure facilities.
- Developing an understanding of the insurance industry and working to facilitate strategies that support cyber-security/liability insurance availability across all sectors; and
- Liability that might arise due to inconsistent state and national laws that place inconsistent requirements on national or global companies.

Hypothetical

Congress, worried about the release of corporate proprietary data and customer personal information, passes a statute requiring Federal regulators to establish Federal cyber-security guidelines. Significant portions of these guidelines focus on the importance of performing a risk-assessment analysis and on involving senior management and directors in all significant information-security decisions. The regulators mandate that cyber security cover technical, physical, and administrative areas.

Company Alpha, which provides telecommunications-related services, and stores significant amounts of non-public customer data, performs a thorough risk assessment. Company Alpha reviews a range of threats and vulnerabilities by involving company representatives from each of the major service centers and technology offices, involving both its internal and external auditors in the review. Company Alpha subsequently fixes a vast majority of the discovered gaps and security issues.

Company Alpha chooses, however, not to fix a small number of the discovered security vulnerabilities:

- Senior management reports these decisions to the CEO and Board of Directors. The Directors query senior management on their decisions, which are based on the high cost of fixing these problems, the low-risk assessment given them by the audit committee reports, and a belief that the problems can be easily managed and with compensating control.
- A shared belief exists amongst management and the audit committee that these low-level risks are not likely to undermine delivery of services essential to the business or result in the loss of customer data; general counsel agrees that the risk is not significantly large to warrant the added security costs.
- The audit committee, working closely with senior management, the Chief Technology Officer, and a newly appointed Chief Information Security Officer, prepare a written information security plan, which includes a component on managing the low-risk vulnerabilities, taking into account technological solutions and employee practices.

In contrast, Company Bravo chooses not to perform a comprehensive risk assessment focused on consumer non-public privacy data. Internal and external auditors do not involve senior management, nor is the CEO or Board of Directors involved in any of the Company's information security activities.

Both companies experience an "insider" problem, resulting in the release of personally identifiable customer information. The New York Times reports on the release of customer data at both companies, leading to a massive drop in stock prices at both Companies Alpha and Bravo. The Trial Bar celebrates as word is out on the first information-security shareholder derivative lawsuits.

* * *

The PCIS might consider addressing duty of care and standard of care issues relating to commercial information security matters. This hypothetical focuses on standards of care to protect non-public customer or privacy data – irrespective of the company's business model or service-delivery practices.

The Davis-Moran legislation, now being debated by Congress, focuses on liability resulting from information-sharing practices, but the exemption from liability is only for information-security disclosures made under certain highly defined situations involving information provided to the government.

Recommendation: Corporate representatives should consider several issues:

- Should the PCIS promote exploration of the full range of legal liability issues?
- If the PCIS, or other organizations, do not raise and move these issues forward, what is the possible harm (Court decisions will establish standards? State lawmakers will provide input into decision-making process, *etc.*?)
- If the PCIS is going to explore liability issues, what are the priorities?
- How should the PCIS identify and support industry standards and duties of care?
- Additionally, should the PCIS identify strategies to raise awareness and/or to effect political/legal change in this complex area?

References:

Current Legislative proposals

H.R. 4246, Cyber Security Information Act 2000

Examples of laws passed

1998 Y2K Information and Readiness Disclosure Act

IV. Encryption

On July 17, the Administration announced a substantial further relaxation on export controls on encryption as controlled by the latest policy effective on January 14. For a summary and links to the press release, fact sheet, and text, go to http://207.96.11.93/Encryption/Default.htm.

The January policy's significance was that licensing applications would often draw positive answers where they would have been declined before. At the same time, cumbersome existing rules and procedures largely remained in place. The European Union, however, forced a prompt reconsideration of the January policy with its decision to allow encryption exports within the EU and selected other leading countries on a license-free basis, once again putting U.S. suppliers at a significant competitive disadvantage. The October policy has the effect of removing that major advantage by allowing U.S. encryption exports on a license-free basis to the EU and eight other countries. The upshot is that, for global security solutions, U.S. firms across the board, as licensees, can now rely on U.S. vendors as well as foreign vendors. Previously, foreign systems integrators and IT vendors enjoyed a legal advantage in serving global customers, whether based outside or inside the U.S.

On October 2, Commerce Secretary Norman Mineta announced that the Department of Commerce had selected a new encryption algorithm to become a federal procurement standard. The 23-year old, 56-bit Data Encryption Standard (DES) will be succeeded as Federal Information Processing Standard (FIPS) by "Rijndael," a 256-bit algorithm submitted by two Belgian programmers who -- as IBM had done with DES -- dedicated the formula to the public domain, making no patent claims. The announcement (http://www.nist.gov/public_affairs/releases/g00-176.htm) caps a three-year search; a formal 90-day comment period will be announced soon in the *Federal Register*. Replacement of DES has become increasingly urgent, as it presents intruders with only a constant level of difficulty in penetration, in the face of processing power available to intruders advancing in accordance with Moore's Law of price-performance doubling every 18 to 24 months. The arrival of a replacement for DES is good news for all firms desiring to ratchet up their level of protection.

Both major policy developments, long in the making, largely coincide with the inception of a new Administration, thus affording the best opportunity in years to move past previous rancorous episodes in computer security issues. If government shows appreciation of the need for consultation, rather than presenting the private sector with a *fait accompli*, and industry demonstrates an appreciation of the common dangers confronting it along with government, then a fresh start is possible.

V. Cost Recovery

How will the cyberthreat defensive expenditures of U.S. firms be treated for federal corporate income tax purposes? In particular, will firms be allowed to expense these amounts or will they be required to amortize them, even if firms do not want to do so?

To the extent that firms can expense such expenditures, they are more able to undertake them. This is especially true if, in some circumstances, government authorities would have some reason for wanting a firm in question to erect higher defenses than the firm's management or board thought its fiduciary responsibilities called for. If the government wants increased cyberthreat expenditures by industry, presumably favorable rather than adverse tax treatment would be part of a larger government policy toward that end.

Nonetheless, in the last decade the Internal Revenue Service has taken an aggressive position on the expensing vs. depreciation issue. Emboldened by its success before the Supreme Court in the 1992 *INDOPCO* case, the IRS now calls for companies to amortize certain expenditures over time even when the taxpaying firm wants to expense them in one year and be done with it. The Supreme Court ruled that a target company could not deduct the costs associated with a friendly takeover by another company because the merger would lead to future benefits for the target company. Since then, the IRS has been very aggressive in applying this decision to a wide range of costs incurred by businesses. In general, the IRS takes the position that any cost that results in a future benefit to a business must be capitalized, rather than deducted currently. The IRS uses a broad definition of "future benefit" and, in many cases, has required companies to capitalize costs that they have been deducting for years. At this point, the service has applied INDOPCO to a wide range of costs incurred by businesses, including the costs related to customer acquisition, contract bidding, post-merger severance, business expansion, redoing software, equipment inspection, plant closings, equipment moving, environmental remediation and equipment removal.

Recent favorable developments are the IRS's interpretations that firms' expenditures to meet ISO 9000 quality standards and to achieve Y2K compatibility may be expensed. To the extent that firms are moving to meet recognized standards in the computer security area, then the ISO 9000 interpretation perhaps could serve as a precedent. The PCIS notes both the potential upside and the potential downside in the tax treatment area and recognizes that structuring an appropriate tax policy to incentivize the reduction of the national vulnerability to cyberthreats is an integral part of the emerging public policy framework that needs to be developed.

VI. Economic Espionage and Trade Secrets

A major motivation of commercial cyber security is the protection of a firm's trade secrets. While one can assign no precise value, about 75% of the roughly $10 trillion capitalization of today's publicly traded companies represents the "enterprise value" or increment above book value assigned to intangibles – business model, management and workforce strength, and intellectual property portfolio.

Four years ago, Congress passed the first-ever federal protection for trade secrets in the marketplace with the Economic Espionage Act (EEA; P.L. 104-294), following testimony by FBI Director Freeh that 23 countries had targeted the U.S. to steal the trade secrets of leading U.S. firms. Estimates of the annual loss run to $250 or $300 billion. The law contains harsh penalties and has been used sparingly.

The Trade Secrets Act (18 U.S.C. 1905), a much older part of the criminal code, makes it a crime for a federal employee to divulge a trade secret entrusted to that agency. At the same time, years of litigation under the Freedom of Information Act – under which one company has often sought to learn more about its competitor – have left a situation in which the case law suggests that cyber trouble reports to the government will not be released. That result, however, is not spelled out in black and white.

An attack or attempted penetration of a corporate computer system may be hard to characterize at first. Is it of domestic or foreign origin? Initially, one cannot tell; hence the serious prison penalties in the EEA, which, while aimed at foreign agents, apply equally to all offenders. Does the attacker intend to disrupt systems or to purloin files? Again, this will not be immediately obvious.

Corporate MIS, CIO, or chief security officers are working off a base of protection of highly valuable corporate secrets that lend a competitive advantage against espionage intended to purloin rather than to disrupt. Defending against deliberate disruption represents a new challenge, but presumably many of the same tools and methods will continue to apply.

Data about attacks or attempted penetrations do not represent a trade secret in any traditional sense, as they do not lend any kind of competitive advantage. To the contrary, cyber vulnerabilities, to extent they are not widely shared – which in some cases they will be – represent a competitive *disadvantage*.

At the moment, companies can divulge trade secrets to the government with greater confidence than trouble reports. Increasing the confidence of companies that trouble reports will not be made public under the Freedom of Information Act is what the Cyber Security Information Act, H.R. 4246 (Davis-Moran), is largely about.

VII. International Issues

Goals:

- Facilitate international law enforcement cooperation
- Establish minimum standards for cyber-security legislation taking into account local cultural and social differences.
- Move away from command-control concepts to expanding partnership opportunities.

At this time, the priority from an international public policy standpoint should be to establish a collaborative international regime that facilitates law enforcement cooperation, establishes a balance between commercial and security interests, and facilitates international public-private partnership.

In this view, the chief threats to economic security are sub-national terrorist groups, criminal organizations, mischief-makers and hackers. This is not to say that the U.S. should be blind to state-sponsored threats, and companies are well advised not to assume that their technologies cannot be targeted by state agents. However, all nations have a vested interest in working together to mitigate the damage caused by terrorism, crime, and mischief.

Currently, there are – broadly speaking – four different cases that need to be managed: (1) cooperation with developed countries, perhaps best captured through the framework of the OECD; (2) cooperation with emerging countries such as Brazil and the Philippines; (3) cooperation with communist and post-communist states; and (4) containment of what were formerly known as "rogue" states.

In the first case, there are a number of initiatives already underway. Perhaps the most significant of which is the Council of Europe's Draft Convention on Cybercrime.

On October 2, the Council of Europe released Version No. 22, Revision 2, of its Draft Convention on Cyber-crime, which would grant police much greater powers to access electronic information. The convention is an attempt to standardize computer crime statutes throughout Europe, and require signatories to cooperate with one another. The Council of Europe is pushing for the Convention to be agreed to by December.

The convention proposes among other things that countries adopt laws criminalizing unauthorized computer access or data interception or manipulation, as well as the possession of passwords or other common security tools if they are held with the intent to commit an offense. It also proposes laws to enable government access to encrypted information and to expand copyright protections.

(The Council of Europe "Draft Convention on Cyber-crime" is open for public comment (email: ***DAJ@COE.INT***))

However, a coalition of 28 prominent international cyber-rights organizations have come out against the current draft, stating that it could result in outlawing network security tools and would require companies to review and keep extensive logs of the message traffic on their systems. In a letter sent to the Council of Europe Secretary General, the Global Internet Liberty Campaign, which includes prominent groups from the U.S., France, Britain, Australia, Bulgaria, Canada, Italy, South Africa, Austria, the Netherlands, and Denmark, claims the treaty is little more than a law enforcement wish list. Industry has expressed similar and additional concerns related to the regulatory burden and cost of certain proposed measures. Industry representatives should advise the next U.S. government about these problems, and encourage the next government to work with the Council of Europe and the OECD to revise their current policy and move toward a more "partnership" oriented model.

The second and third cases – creating cooperative models with communist and post-communist countries and with developing countries can be treated in relatively similar fashion. In these cases, the U.S. may wish to propose basic legal formulas for treating cybercrime and establish basic ground rules for law enforcement cooperation. These formulas should be flexible and take into account social and cultural differences.

Companies should be aware that countries like Brazil, Mexico, India, the Philippines, China, and Russia have developed significant computer and technically literate populations, and either do not currently have cybercrime legislation, do not have comprehensive legislation, or do not have adequate enforcement and remedy provisions.

This is important to bear in mind, considering that the Philippine student who allegedly unleashed the "I Love You" virus did not break any cybercrime laws.

Creating a global consensus to promote the benefits of cooperating to safeguard network systems and to facilitate state-state, public-private cooperation will enhance economic stability and have other commercial and political benefits.

In the fourth case – dealing with countries such as Cuba, Iran, Iraq, and North Korea – cybersecurity discussions should be integrated into other ongoing diplomatic discussions as part of the overall set of issues involved in relations with these states.

VIII. Attachments

There are various other matters that require immediate examination and thought. As a result, attached to this White Paper are several support documents, including:

- A listing of legislative initiatives that were considered by the U.S. House of Representatives and Senate in the Fall of 2000 (Attachment 1);
- A listing of additional legal issues (Attachment 2);
- A listing of a set of principles for voluntary information sharing (Attachment 3);
- A summary of an Amendment offered by Senator Bennett to require the Defense Department to clearly define its contribution to critical infrastructure issues – both public and private sector related (Attachment 4);
- A summary of the Cyber Security Information Act, H.R. 4246 (Attachment 5); and
- A summary of the Interagency Security Guidelines published pursuant to the Gramm-Leach–Bliley Act (Attachment 6).
- Select legal definitions (Attachment 7).

Attachment 1

2000 House and Senate Legislative Proposals

In addition to HR4246 (Attachment 5), the following are a list of other measures under consideration by the House of Representatives and the Senate that could affect the public policy framework governing critical infrastructure protection. The variety of legislative proposals reflect different strands of current U.S. strategic thinking vis-à-vis critical infrastructure protection and the range and complexity of issues that need to be addressed.

Department of Defense Authorization Act (H.R. 4205) — "Bennett-Schumer" Amendment: Under this legislation the Department of Defense is:

- required to better define its role in, and explain to Congress its coordination with other governmental efforts related to, critical infrastructure and information system protection
- given $15 million to recruit cyberwarfare specialists
- given $5 million to create an Institute for Defense Computer Security and Information Protection
- authorized to provide loan guarantees to improve domestic preparedness to combat cyberterrorism.

H.R. 2413 — Computer Security Enhancement Act of 2000: H.R. 2413 would require the National Institute of Science and Technology (NIST) to serve as a computer security consultant for federal civilian agencies. NIST would offer the government guidance on protecting the security and privacy of sensitive information in agency computer systems. In this role, NIST would be encouraged to recommend "technology neutral" solutions to security problems, and to advise government agencies on which "off-the-shelf" computer security products met with the government's standards. H.R. 2413 also would require NIST to study the effectiveness of commercially available encryption products.

H.R. 4987 — Digital Privacy Act of 2000: Would ease law-enforcement monitoring of electronic communications.

H.R. 5018 — Electronic Communications Privacy Act of 2000: As substantially revised, H.R. 5018 is primarily focused on privacy concerns raised in reaction to the FBI's "Carnivore" e-mail surveillance program. Because it is vastly different from the primary Senate-passed cybercrime bill (S. 2448, below), no further action is likely at this late date in the legislative year.

Senate Bills

S. 1314 — Computer Crime Enforcement Act: S. 1314 would authorize $25 million for the Department of Justice to help states develop computer crime enforcement units.

S. 1993 (Government Information Security Act): Attempts to strengthen federal information security practices and coordinate government information security efforts with those of the civilian, security, and law enforcement communities.

S. 2430 (Internet Security Act of 2000): Broadens the scope of the existing $5,000-loss minimum required to permit federal jurisdiction over computer hacking cases, permits forfeiture of property used in computer hacking crimes, increases the availability of law-enforcement wiretapping, and eliminates mandatory minimum sentences for certain computer hacking crimes.

S. 2448 — Internet Integrity and Critical Infrastructure Protection Act of 2000: As amended, S. 2448 would, among other things, give the Secret Service jurisdiction to investigate certain computer crimes, including those against financial institutions, increase penalties for criminal activity that used encryption; authorize $5 million to establish a Deputy Assistant Attorney General to oversee the Justice Department's Computer Crime and Intellectual Property Section, and give DoJ $80 million to create 10 regional computer forensic labs that would provide education, training, and forensic capabilities to state and local law enforcement charged with investigating computer crimes, and another $20 million to establish a National Cyber Crime Technical Support Center. The bill would also permit the confiscation of equipment used to commit computer crimes, allow the prosecution of juveniles, increase various computer-crime penalties to as much as 20 years in prison, and would require the U.S. Sentencing Commission to review and perhaps revise the sentencing guidelines for computer crimes, including elimination of the six-month mandatory minimum sentence for reckless crimes.

S. 2451: Creates a National Commission on Cybersecurity, increases penalties for certain computer crimes, and broadens the applicability of those penalties.

S. 3188 — Cyber Security Enhancement Act: S. 3188 would call for more protection for U.S. critical infrastructure from hackers, terrorists and rogue nations by allowing companies to voluntarily submit information that the government would not otherwise have about weaknesses in their online systems, as well as information on threats and attacks to the federal government, without fearing that the information would be subject to disclosure under the Freedom of Information Act. In addition, S. 3188 would permit the Attorney General to issue administrative subpoenas to trace cyberattacks, and would require the A.G. to report to Congress on plans to standardize information requests to business, and efforts to encourage the technological prevention of falsifying e-mail addresses.

Attachment 2

Additional Issues for Future Consideration

- State Legal and Public Policy Issues

Current and prospective state laws should be reviewed and assessed. The extent to which such laws would be preempted by federal law should also be assessed.

- Simplifying and Clarifying Industry-Government Relations

Industry is working with a number of different government agencies on CIP issues. These relationships should be mapped out, and this may facilitate public-private engagement and streamlining practices.

- Federal Regulations

Proposed federal regulations should not be issued without first evaluating their impact on critical infrastructure, akin to an Environmental Impact Statement, and should not be finalized without attempting to mitigate any adverse effect. There are now several pending rulemakings that have serious adverse impacts on critical infrastructure providers, and there is no federal policy which requires those impacts even to be considered, much less appropriately accommodated.

- The Impact of Privacy on Security Issues

- Public and Private Access

Attachment 3

Initial Set of Principles for Voluntary Information Sharing

- Existing laws should be adapted as necessary to allow appropriate levels of voluntary information sharing among companies, and between the private sector and government.

- Industry should continue to monitor the private sector portion of the Nation's critical infrastructure and should cooperate both internally and with government in reporting and exchanging information, as appropriate, concerning threats, attacks, and protective and recovery measures. Coordination among principals must facilitate creation of responsible activities ranging from early warning systems to response, restoration, and recovery initiatives.

- The creation and operation of voluntary information-sharing mechanisms or processes should not expose participants to additional regulatory or other proximate liability. Private industry efforts to avoid or reduce cyber-threats and other harm to critical infrastructure should be given regulatory "safe-harbor" status, and should be favored under the law at least as much as "Good Samaritan" efforts.

- Distinctions should be made among cyber-mischief; cyber-crime and cyber-war to clarify jurisdictional issues and determine appropriate responses. The adequacy of current laws to prevent these threats must be reviewed. As necessary, existing laws should be adapted to take these matters into account.

Attachment 4

Summary of Bennett Amendment

- On June 20, the Senate unanimously approved Bennett-Schumer, which requires the Department of Defense, and all other agencies to report to Congress on plans and programs to organize and coordinate defense against attacks on critical infrastructures and critical information systems in both the public and private sectors.

- The legislation is principally aimed at requiring the Defense Department to define its role in PDD-63 activities. Specific requirements include:

    - Identifying the necessary definitions of a "nationally significant cyber-event" and "cyber-reconstitution";

    - Describing how the Defense Department is working within the Intelligence Community to identify, detect and counter the threat of information warfare of foreign states and transnational organizations; and

    - Explaining how the Defense Department is integrating the National Communications Systems and the Joint Task Force/Computer Network Defense into an Indications and Warning architecture.

- The proposed legislation also requires the President to submit a report to Congress by July 2001 detailing the specific steps the Federal government has taken to develop infrastructure assurance strategies, as outlined in PDD-63.

- The bill was accepted unanimously as an amendment to the Department of Defense Authorization Act, which is currently pending in the Senate.

- Keep in mind that the bill does not relate to the Computer Security Act of 1987, and the repeal of National Security Decision Directive 145, which dealt with authority to create minimum computer security standards and guidelines within the Federal government. Rather, the emphasis is wholly on identifying a clear role for the Defense Department in the on-going PDD-63 activities.

Attachment 5

Summary of "Cyber Security Information Act of 2000"

H.R. 4246, "The Cyber Security Information Act of 2000" introduced by Congressmen Tom Davis (R-VA) and Jim Moran (D-VA) accomplishes two major goals. First, it provides limited protection from unintended uses for cyber-security information voluntarily shared with the federal government. Second, it describes alternative mechanisms for sharing such information with the government.

As for the mechanisms for sharing cyber-security information with the government, the Act specifies that the government may ask for voluntary submittal, directly to the government, of detailed company-specific cyber-security information (as defined) in order to assess the cyber-security of an industry or economic sector. Further, the government may request that cyber-security data be submitted to a non-governmental entity that agrees to coordinate such data gathering and then pass on that information to the government, most likely by means of its own summary and assessment of the data. In addition, such non-governmental entity may obtain the benefits of this provision even if it performs those functions without first being asked by the government, as long as it does in fact provide such cyber-security data and/or analysis to the government.

Next, regarding the protections provided to cyber-security information , the Act stipulates that any and all cyber-security information (as defined) voluntarily provided to the government or aforesaid non-governmental entity will be given a broad immunity from forced release to any other entity or individual. This is accomplished in two ways. First, the Act specifies that all cyber-security information voluntarily provided to the government pursuant to this process is deemed to be exempted from disclosure under the Freedom of Information Act (FOIA). This exemption is similar to already-existing FOIA exemptions, such as those for trade secrets and national security, but would not be subject to the uncertainties, vagaries, and delay of case-by-case agency determination, along with any attendant litigation delays associated with making such case-by-case determinations. Moreover, to the extent that any such cyber-security data actually held by a third party could be said to be held by the government by virtue of that third party acting on behalf of the government, FOIA would still not require the release of such data.

Second, no entity may use any other means (such as a subpoena) to force the government or the third-party data-gatherer to yield up cyber-security data. However, to ensure that the government obtains the full use of any related or similar data that it receives, and that no injustice would be worked against a party to litigation, the Act further provides that cyber-security data can be used **(a)** by the government if obtained pursuant to some statutory or regulatory requirement (rather than voluntarily), or **(b)** by anyone for any purpose once the information has been made public with the permission of the originating entity. Moreover, a litigant may utilize any existing lawful means already available to it (such as a subpoena) to obtain such data directly from the originator.

Attachment 6

Summary of Gramm-Leach-Bliley Cyber-Security Provisions

- In November of 1999, Congress passed the Financial Services Modernization Act, referred to as the Gramm-Leach-Bliley Act ("G-L-B"), repealing Glass-Steagall and streamlining the financial services legislative and regulatory framework.

- In response to pressure from the privacy community, which was concerned about customer information being circulated within the newly opened financial services atmosphere, Congress included language in G-L-B to protect personal information in the possession of the financial services industry.

- Generally speaking, the statute mandates that various federal regulators "establish appropriate standards for the financial institutions subject to their jurisdiction" for identifying and protecting certain customer information (Refer to Sections 501 to 505 of the law):

  (1) To insure the security and confidentiality of customer records and information;

  (2) To protect against any anticipated threats or hazards to the security or integrity of such records; and

  (3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience of any customer.

- The law includes three distinct requirements: technical protection (cyber-security), administrative protection (social engineering policies), and physical security protection. (Collectively, "cyber-security"):

- Relevant agencies and department include: the Securities & Exchange Commission, Federal Deposit Insurance Corporation, Department of Treasury entities (OCC and the OTS), the Federal Reserve Board of Governors, and the National Credit Union Administration.

- Congress additionally requires state-based insurance regulators to issue similar standards for entities under their jurisdiction; failure to do so may result in curtailed federal funding, such as FDIC-provided insurance guarantees.

- In response to the statute, several of the listed agencies and departments cooperated to develop appropriate standards and guidance, forming the Financial Services Legal Working Group, which met during a six-month period to develop

a sophisticated collection of cyber-security guidance materials. The "Interagency Guidelines" were published in the Federal Register on June 26, 2000.

- The Interagency Guidelines establish several key responsibilities:
    - Involving the Board of Directors and Senior Management throughout the information security planning process;
    - Identifying threats and vulnerabilities to information and cyber systems;
    - Performing a risk assessment based on these threats and vulnerabilities;
    - Overseeing and carefully managing vendors that have access to customer data ("due diligence" standards); and
    - Implementing a written information security policy and program.
- In addition, the guidance materials require implementing various other due-diligence responsibilities, such as training staff, preparing emergency response programs and business contingency plans, and appointing a Chief Information Security Officer.
- While G-L-B is aimed at the financial services industry, the reach of the law is unclear; the Federal Trade Commission has jurisdiction to issue cyber-security guidelines for entities under its jurisdiction – which includes, in effect – anyone engaged in e-commerce. In addition, G-L-B applies explicitly to affiliates and service providers who maintain or process any of the targeted customer data.
- How these Interagency Guidelines will be used in litigation is also a significant issue. In particular, industry and government should monitor the extent to which the Interagency Guidelines establish a duty of care or industry standard, which may be relied on in litigation stemming from a cyber-intrusion or breach of confidential customer data.
- Comments must be received not later than August 25, 2000. Agencies will separately review the responses and publish final rules this fall. The statutory deadline is November 13, although agencies may choose to extend the deadline. Compliance is mandated by July 2001.
- One complex question is the extent to which the FTC will engage the cyber-security issue. The agency has always taken an aggressive approach to online privacy, and to the extent that security relates to privacy concerns, they, too, might issue their own regulations for a multitude of other industries. As mentioned, service providers that hold or process any of the personal information covered by the G-L-B are also subject to the regulations. This, too, may serve as a hook for the FTC – or another agency – to regulate cyber security issues. An

additional complexity is the extent to which state agencies will publish cyber-security guidelines.

- The SEC published its proposed rules on March 8, 2000 (65 Fed. Reg. 12354 (March 8, 2000)). (In sum, a *financial institution may be in compliance if it adopts measures to protect against reasonably anticipated threats and hazards*). The SEC has not developed, nor does it plan to prepare, any further regulations in this area. Similarly, the FTC has not prepared specific guidance or regulations in the security area.

- One other complex, unresolved issue is the extent to which the Interagency Guidelines will be enforced as regulations or left as voluntary guidelines by each department/agency. The regulators are seeking comment on these and other issues raised in the materials.

Attachment 7

Legal Definitions

Due Diligence. Actions expected from a reasonable and prudent person under particular circumstances. Such diligence is not measured by any absolute standard but depends upon the relative facts of a special case (see "Reasonable" below).

Duty of Care. An obligation to conform to a legal standard of reasonable conduct in light of apparent risk. In a negligence context, the word "duty" denotes the fact that the actor is required to conduct himself in a specific manner. If he does not, he becomes subject to liability to the party to whom the duty is owed for injuries resulting from the non-conforming conduct. For example, a corporate officer has a duty of care over corporate assets.

Limitation of Liability (Acts). State and federal statutes that limit liability for certain types of damages (lost profits, costs, etc.) or of certain groups or persons (liability of corporate officers for certain acts of the corporation). When used to limit damages, sometimes referred to as a "cap."

Precedent. An adjudged case or decision of a court, considered as furnishing an example or authority for an identical or similar case arising afterward or a similar question of law.

Preemption - Doctrine, adopted by the United States Supreme Court, holding that certain matters are of such national, as opposed to local, character that federal laws take precedence over state laws. In such a situation, a state may not pass a law inconsistent with the federal law.

Per se Illegal. "Per se" means: in itself; taken alone; inherently. In an antitrust context, certain types of business agreements, like price-fixing, are considered "per se" illegal because they are deemed to be inherently anti-competitive and injurious to the public. For those acts, courts do not examine whether there has been any actual damage from the activity. Liability is imposed simply because the act took place.

Reasonable – Fair, proper, just, moderate, suitable under the circumstances. For example, if two companies exchange information regarding infrastructure security, those actions would be judged based upon what other similarly situated companies would do in like circumstances.

Rule of Reason. Under the "rule of reason" test in antitrust cases, the legality of restraints on trade is determined by weighing all of the factors of the case, such as the history of the restraint, the evil alleged to exist, the reason for adopting a particular remedy and the purpose or end sought to be attained. The fact finder must weigh all the circumstances to decide whether a practice unreasonably restrains competition, and the test requires that a plaintiff show anti-competitive effects or actual harm to competition and not simply whether a given practice is "unfair."

Safe Harbor. Usually refers to a set of guidelines established so that companies can be protected from liability or regulation under a given law. For example, a statute might state that if a company takes actions "A", "B", and "C", then, depending on the statute, that company would either avoid liability, limit its potential liability or be exempt from regulation.

Trade Secret. A "trade secret" may consist of any formula, pattern, concept or device used in one's business which gives an advantage over competitors who do not know or use it. Trade Secrets are intellectual property, but do not necessarily have patent, trademark, or other formal intellectual property protection.

VII. APPENDICES

VII. APPENDICES

Appendix A
Department Of Defense

The Department of Defense has made significant progress in critical infrastructure protection (CIP) over the past year by focusing its CIP efforts in three major areas:

- Information Assurance – the identification and elimination of cyber vulnerabilities;
- Y2K – the development and application Y2K-proven processes to CIP that demonstrated that highly complex infrastructures can be understood, single-points of failure identified, and then corrected in an expeditious and affordable manner; and
- Broader CIP Development – specific CIP efforts on developing and demonstrating the viability of those remaining component elements essential to making CIP a reality with the Department of Defense.

Detailed below are the specific accomplishments in each of the three major areas. The bracketed numbers following each of the specific accomplishment listed below are the relevant milestone(s) from the *National Plan for Information Systems Protection* that a given activity pertains to.

Information Assurance

To protect our information environment, DOD is using a defense-in-depth approach consisting of layered security systems and procedures, employing active and passive defensive measures to prevent unauthorized access to information and information systems. Defense-in-depth protects critical assets and processes by creating a deterrent posture, enhancing network security programs and operations, effectively training and certifying personnel, and leveraging new technologies.

This approach will force any adversaries to defeat multiple layers of protection before they are capable of impacting our activities. It is this layered security concept that allows us to make maximum use of commercial technology and minimize the investment we must make in unique government developed solutions. This construct is focused on the integration of the capabilities of people, operations and technology to defend the Local Computing Environments or Enclaves, the Enclave Boundaries, the Networks that link these Enclaves and the Supporting Infrastructures. Although we realize that we can never fully eliminate the vulnerabilities of our systems, we can at least mitigate them. In order to protect our information environment, the Defense Department is:

- Deploying a strong, interoperable Public Key Infrastructure across the Department to provide end-to-end encryption and authentication services for "sensitive but unclassified" information and to provide improved access control to our information/computer systems. It will also provide security for classified information that must be sent over unprotected networks. Department-wide policy on deployment of a DOD PKI was signed by the Deputy Secretary of Defense in May 1999 and updated in August 2000. This policy sets a milestone of October 2002 by which all DOD active military, civilian personnel, and selected Reserve personnel will have Common Access Card (smart card) tokens hosting their PKI certificates. {1.6, 1.22, 1.25, 1.26, and 1.27}
- Modernizing our strongest encryption technology to keep pace with the rapid changes in information technology. We have programs to upgrade secure voice and data to the desktop; integrate security into the rapidly evolving set of wireless technologies; and continue development and deployment of

strong encryption capability for the increasingly higher capacity systems required by today's "video" wars. {1.25}

- Reengineering the DOD "Information Enterprise." This program, the Global Information Grid, or GIG, is under rapid development and will provide, in conjunction with other actions, the "Defense-in-Depth" necessary to protect DOD information systems. The Global Information Grid (GIG) Information Assurance Policy 6-8510, which was signed in May 2000, addresses not only the confidentiality requirement of DOD's information but also its availability, integrity, and the need for strong identification and non-repudiation services. Paralleling this effort is the capturing of IA architecture requirements in the GIG Architecture Documentation, ensuring a common architectural framework for IA throughout the DOD. {1.17, 2.7, 2.8, and 7.4}
- Advancing our computer forensic capabilities. On 24 September 1999, the DOD opened the Defense Computer Forensics Laboratory (DCFL). This is a state-of-the-art facility to process computer evidence in criminal, fraud and counterintelligence investigations, for all of the Defense Criminal and Counterintelligence Investigative organizations. The Air Force Office of Special Investigations is the Executive Agency for the DCFL. The DCFL currently has 42 positions for investigators and forensic technicians to process computer evidence as well as audio and video media in cases ranging from sexual child abuse, computer intrusions and espionage. The DOD also provided assistance to the Federal Bureau of Investigation (FBI) in order to promote a computer forensic capability that is also co-located with the DCFL to build synergy with other criminal investigative organizations. The DCFL already has been instrumental through media analysis in successful identification of computer hacking groups and the neutralization of vulnerabilities in several high profile counterintelligence investigations related to national computer network defense activities, including those known as Solar Sunrise, Digital Demon, and Moonlight Maze. {3.1}
- Improving our ability to actively defend our computer systems. We have established a Joint Task Force for Computer Network Defense (JTF-CND) and the Commander-in-Chief, US Space Command assumed overall responsibility for computer network defense on 1 October 1999. During the Melissa Virus incident in March 2000, the JTF-CND, in cooperation with the DOD Computer Emergency Response Team (CERT) and the JTF's service components, was able to quickly assess the threat, develop a defensive strategy, and direct appropriate defensive actions. Again in May 2000, the LOVELETTER virus provided another example of JTF-CND rapid action. The JTF staff rapidly identified the potential damage and provided rapid notification to the CINCs, Services, and agencies, which enabled them to effectively respond. And we are beginning to work with our allies: Canada has a desk officer working in the JTF-CND and we are developing Computer Network Defense information sharing Memorandum of Understanding (MOU) and Concept of Operations (CONOP) with Canada. {1.13 and 5.3}
- Establishing an Information Assurance Vulnerability Alert (IAVA) system for distributing vulnerability information to all DOD elements on behalf of OSD and issued 11 IAVAs (alerts), 3 IAVBs (bulletins) and 20 technical advisories in 1999. In 2000, 3 IAVAs (alerts), 3 IAVBs (bulletins) and 9 technical advisories have been issued. DISA also developed a database to immediately distribute vulnerability information to each system administrator and to track and report on his or her response to these alerts. {1.10 and 1.13}
- Establishing a comprehensive Education, Training and Awareness (ETA) program for DOD military, civilians and contract employees. All users are required to receive initial awareness training prior to issuance of an account and must receive annual refresher training. Additionally, systems/network administrators on both classified and unclassified systems are required to be trained and certified, with other personnel performing "critical" IA functions having to meet similar criteria within the next year. A series of recommendations approved by the Deputy Secretary of Defense, Mr. De Leon, in July 2000, will, when implemented, significantly improve the training, certification and personnel management of IA personnel. To assist in these training and awareness initiatives, the DISA Information Assurance Program Office (IAPMO) produces a number of IA computer-based training

CDs and videotapes available to all Federal activities. To address formal IA education, NSA initiated the Centers of Academic Excellence in Information Assurance Education in 1999 and expanded the program in 2000 to include 14 universities. These universities were selected based on the depth and maturity of their security programs in accordance with the standards developed by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

- Initiated development of a DOD-wide process and metrics through which the Secretary of Defense can objectively (1) measure and articulate the IA Readiness status of the Department, and (2) obtain information useful to identify and support IA resource requirements; This process will be applicable throughout DOD, affecting both combat and non-combat Components. Expected outputs of the process include: (1) IA Readiness status; (2) IA resource requirements; (3) inputs for DOD policy generation or revision; and (4) feedback to IT managers and community. Metrics will be structured in a hierarchical fashion, providing five aggregated, indexed executive level metrics for the Secretary. These metric will correlate to five critical success indicators organized within the following five categories: people: operations; training; equipment & infrastructure: and processes {8.3}.
- Approved the Joint Reserve Component Virtual Information Organization (JRVIO) concept of operations, which provides Information Operations support to the Defense Information Systems Agency (DISA), the National Security Agency (NSA), the Joint Information Operations Center (JOIC), the Information Operations Technical Center (IOTC), and the Joint Task Force for Computer Network Defense (JTF-CND). The structure and functions of the supporting JRVIO mirrors that of the Active Component (e.g., the JRVIO supporting the JIOC will execute functions within the scope of the JIOC's mission). There is no function, other than conducting virtual operations; the JRVIO will undertake that varies from the missions assigned to its supported unit. Any Information Assurance (IA) mission currently conducted by one of the supported organizations will be open to JRVIO tasking. As examples: (1) At the joint level, DISA conducts IA operations to protect the Defense Information Infrastructure (DII)---IA activities are executed through the DISA Global Network Operations and Security Center (GNOSC), the Regional Network: Operations and Security Centers (RNOSCs), the DOD Computer Emergency Response Team (DOD CERT), coordination with Services and other DOD agencies, coordination with civilian industry, and a number of other internal DISA elements and external contacts; and (2) the NSA Information Assurance Directorate, in coordination with DISA, and under the policy guidance of ASD/C3I, conducts IA operations in support of both DOD and other governmental departments and agencies---NSA, like DISA, owns significant IA operational capabilities because of its mission to conduct full-spectrum IA operations. JRVIO support to these organizations will expand their ability to meet mushrooming IA challenges {1.13 and 1.17}
- The Chairman of the Joint Chiefs of Staff (CJCS) issued guidance to Commanders-in-Chief of the Unified Commands (CINCs)/Services/Agencies to improve Information Assurance Vulnerability Alerts (IAVAs) compliance and requested commander involvement in the defense of their networks. {2.7, 2.9 and 5.3}
- SPACECOM was designated by the Unified Command Plan-99 to be the military lead for computer network defense (CND) and computer network attack (CAN). {1.17}
- CJCS directed that the Joint Staff and CINCs address CND in all Operations and Concept Plans. {1.17}
- The Joint Staff (J-6) has developed and is working toward implementation of an instruction (CJCSI 6510.01C) identifying the minimum IA capabilities (55 elements) required for CINCs, Services, and Agencies (C/S/As). {2.9}
- The Joint Staff (J-6) consolidated several existing IA working groups under one panel that reports to the Military Communications-Electronics Board (MCEB). Panel's work led to a significant reduction in DOD's information system's mobile code vulnerability. {1.17}

- Joint Staff is working to normalize the IA readiness metrics into the Joint Monthly Readiness Report (JMRR) process and integrate IA readiness reporting into operational readiness reporting. {1.13 and 2.9}
- The Joint Staff deployed a pilot IA capability to complement the network management capability provided to the CINCs. The pilot program enables JTF commanders to monitor the IA status of their AOR. {2.7 and 5.3}
- The Army created the Network Security Improvement Program (NSIP) as the Army strategy for implementing DOD concept of Defense in Depth (DiD). NSIP is a comprehensive set of innovative policies and procedures, state-of-the-art IA hardware/software enabling technologies, an active training program, and retention initiatives. {1.13, 1.17, 2.7 and 5.3}
- The Army created the Army Computer Emergency Response Team (ACERT) Infrastructure. The ACERT receives all intrusion reports and supports Army users worldwide in protecting against, and responding to, attacks on Army systems and networks. {1.13, 1.17 and 5.3}
- J6 and the Military Communications-Electronics Board (MCEB) sponsored a mobile code policy that was signed out as a policy memorandum by the DOD CIO on November 7, 2000. Mobile Code policy execution will reduce DOD's vulnerability to malicious attacks by web-based technology. To develop this policy, J6 worked closely with Microsoft to identify mobile code vulnerabilities and future technology. MCEB also sponsored a Ports and Protocols Management Process approved by the DOD CIO Executive Board in November. This process enables DOD to protect and control the points of vulnerability at the interfaces between networks. This process requires close coordination between systems developers and private industry as systems are developed and integrated into the DOD's information systems.
- J6 also met with the Wang Corporation to discuss the direction private industry is taking with regard to Public Key Infrastructure (PKI) technology. J-6 future plans include on-sight, physical infrastructure inspections to discuss information assurance efforts, interface as part of the Global Information Grid, DOD's Critical Infrastructure Protection efforts, and the dependencies between critical infrastructure components and military preparedness.
- As a member of the National Security Telecommunications Advisory Council (NSTAC), J6 is involved in the NSTAC directed Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force. NSTAC provides industry-based analyses and recommendations to the President of the United States regarding policy affecting national security and emergency preparedness (NS/EP) telecommunications. One of its highlighted initiatives includes coordinating with the President's Critical Infrastructure Assurance Office to support significant advances toward the goals of Presidential Decision Directive 63.
- The Army's Interim Brigade Combat Teams (IBCT) and the Digitized Division/Corps both incorporate IA into their operations. The Army updated the Protection Plan for Force XXI Systems. This plan outlines requirements for security planning, vulnerability testing, and identifies acquisition decision milestones. {5.1}
- Army is chartered to lead, consolidate, and coordinate all biometrics Information Assurance activities for DOD. The Army established the Biometrics Management Office (BMO) in FY2000. The BMO's primary mission is to develop an acquisition-based strategy to employ biometrics applications that ensure definitive access control to critical information and weapons systems in all environments. {6.4}
- The Army Intelligence and Security Command's Information Dominance Center (IDC) reached initial operational capability on 1 October 2000 and is currently in Phase II of a three-phased development process. The IDC provides the Army the technology and tools to support collaborative planning, analysis, and execution of information operations (IO). {3.2}
- The Army developed the *Army Infrastructure Assurance XXI Campaign Plan.* This plan supports critical infrastructure protection through a holistic approach focused on ensuring functional capability through the full spectrum of conflict.

- The Army is developing an infrastructure assurance strategic plan focused on supporting the "shape, prepare and respond" aspects of the National Security Strategy.
- The Army infrastructure assurance activities leverage existing and future cyber/physical protection programs as a means of supporting the Department of Defense critical infrastructure protection program effort.
- The U.S. Army Corps of Engineers completed and continues to refine the Public Works Sector Defense Infrastructure Assurance Plan.
- The Army included infrastructure assurance (critical infrastructure protection) as a discussion topic in its installation commander's course. The Army continues to find ways to increase the dialogue on the subject.
- The Army will conduct an infrastructure assurance political-military game in 2001 designed to increase Army leadership awareness and solicit high-level support for the overall Army effort.
- The Army developed and is finalizing an Army regulation addressing the policy aspects of infrastructure assurance and its role in support of the Department of Defense critical infrastructure protection program.
- The Army is coordinating with the Joint Service Security Council to ensure alignment of Law Enforcement considerations across all aspects of critical infrastructure protection.
- The Army coordinates across all aspects of critical infrastructure assurance by maintaining a viable Physical Security Program, encompassing all physical security measures, including construction standards, intrusion detection systems, security personnel, military working dogs, and others.
- The Air Force implemented a Certificate of Networthiness (CON) process. Before a system is deemed "networthy" and issued a CON by a senior USAF CIO, network risk assessment testing is conducted, potential security problems are identified, and deficiencies are corrected. {1.13, 1.7, 2.7 and 5.3}
- The Air Force conducted 41 Anti-Terrorism vulnerability assessment visits in CY 2000, using both Joint Staff Integrated Vulnerability Assessment (JSIVA) and USAF Vulnerability Assessment Teams. Forty-four assessments are scheduled for CY 2001. As in previous years, the focus of these assessments is primarily the protection of personnel, but physical security and emergency response are also addressed.
- The Air Staff worked with ASD(C3I) in developing a DOD Integrated Vulnerability Assessment (DIVA)--the USAF has provided inputs regarding integration of existing assessment processes, recommended how to schedule DIVAs, team size and composition, and DIVA protocols. The USAF set up "proof of concept" for DIVA at Malmstrom Air Force Base.
- The Marine Corps developed the Base Network Infrastructure Protection Suite, currently in field-testing. {1.13}
- The U. S. Navy is fielding secure systems that ease operations across classification levels by providing releasability without compromising security and is exploring secure solutions to support coalition interoperability requirements. {Goal 2}
- The U.S. Joint Forces Command (USJFCOM) conducted Information Systems Security, IA training, and CND for headquarters networks as well as overseeing the IA programs of 19 subordinate commands. {1.9 and 1.10}
- The U.S. Joint Forces Command incorporated additional IA play into Joint Task Force training exercises in coordination with the Joint Warfighting Center's Information Operations (IO) Planning Cell. {1.9 and 1.10}
- The U.S. Joint Forces Command updated computer network incident reporting procedures to allow quicker notification to higher echelons of identified events. {1.13, 1.17 and 2.9}
- The U.S. Joint Forces Command conducted Inspector General staff assistance visits and inspections at 6 of USJFCOM's 17 subordinate commands. {1.9 and 1.10}
- The U.S. Joint Forces Command established periodic IA Readiness reviews (IARRs) of all 5 sub-unified commands and 10 subordinate joint activities. {1.13, 1.17 and 2.9}

- The U.S. Joint Forces Command initiated use of the Defense Information System Agency's (DISA's) Vulnerability Compliance Tracking System (VCTS) on 1 July 2000. {1.13, 1.17 and 2.9}
- The U.S. Joint Forces Command installed redundant headquarters SIPRNET connections that will permit automated fail-over, and keep critical command and control systems and information available to the Joint warfighters, experimenters, and trainers. {1.13}
- The U.S. Joint Forces Command, with DISA's assistance, plans to install additional audit servers, firewalls, intrusion detection systems, and vulnerability scanners on networks. {1.13}

Y2K

As a global infrastructure reliability challenge, Department of Defense (DOD) actions taken in preparation for the Year 2000 (Y2K) Date Conversion dramatically increased the visibility and criticality of both cyber and physical Critical Infrastructure Protection (CIP) throughout the Department. The Y2K events within the Department of Defense demonstrated the ability to:

- Understand highly complex (including cyber and commercial) infrastructures;
- Identify single-points of failure; and
- Correct these vulnerabilities in an expeditious, affordable manner.

Significant CIP efforts/results included:

- The Secretary of Defense designated the Y2K event a Defense-wide operational readiness issue. {1}
- DOD shifted its Y2K/CIP focus from systems and information technologies to an integrated cyber and physical infrastructure reliability and operational readiness approach. {1.12}
- Dramatically improved integration between DOD Chief Information Officers, Chief Infrastructure Assurance Officers (CIAOs), Commanders-in-Chief (CINCs), the Services, Defense Agencies, the OSD Staff, and the Department's senior leadership. DOD personnel worked together by the thousands in integrated, Defense-wide, teams to make information systems and physical infrastructures Y2K compliant and reliable to ensure the Department's worldwide operational readiness. {1.9 and 1.17}
- Dramatically improved Defense-wide understanding of the Department's dependencies on critical domestic, Host-nation, and international cyber and physical infrastructures, which are beyond DOD control, yet required to accomplish core DOD missions. {1.11}
- Greatly reduced the risk of Y2K induced infrastructure failures through creation of a series of risk mitigation measures. These measures included requirements for: 123 major/mission critical system "End-to-End" evaluations, automated screening of computer software code, and strict configuration management policies and procedures. {1.28}
- Upgraded and improved information system, installation, and operational contingency plans to ensure continuity of operations regardless of any Y2K related infrastructure disruptions. {5.1}
- Given the global context of the Y2K challenge, the interagency infrastructure readiness and Consequence Management coordination processes were defined, refined, exercised, and were available for any action required. {1.9 and 1.17}
- Jointly developed and executed Y2K/CIP and Consequence Management related training and exercises scenarios. {1.18, 1.19, 1.28, 5.1 and 5.3}
- DOD operations personnel were prepared for the Century and Leap Year Rollovers by presenting a major number of infrastructure failures and consequence management challenges. These exercises very effectively trained people, validated response architectures, honed decision-making procedures, developed teamwork, instilled confidence, and ensured the maintenance of the global operational readiness of the Department.

- User focused and friendly IT and collaborative tools support paid off in user acceptance and efficiency. {1.9, 1.11, and 1.17}
- The functionally based operational, information and technical architectures were sufficiently flexible to change and expand, as increased demands were place on them.
- Plain English business rules controlled through a configuration management board are an efficient way to obtain mutual understanding between users and developers and ensure requirements are met.
- Prepared to Respond to Multiple Simultaneous Domestic and International Request for DOD Assistance. {1.19 and 5.1}
- Built a Strong Consequence Management Policy.
- Actively Supported by Leadership.
- Provided for the maintenance of operational readiness.
- Made infrastructure defenders equal to nuclear command and control, National Command Authority, and current Operations and Intelligence personnel.
- Created the Decision Support Activity.
- Integrated Information Assurance (IA) into Critical Infrastructure Protection (CIP) resources to provide global infrastructure performance analyses to support DOD asset allocation, Consequence Management operations, and Senior Leadership decision-making.
- "Operationalized" cyber and physical CIP in support of Defense objectives.
- Integrated the DISA infrastructure monitoring and decision support efforts with those of the President's Information Coordination Center.
- Tasked Organized the Office of the Secretary of Defense (OSD) Staff.
- Trained OSD Staff seniors.
- Provided direct infrastructure monitoring and decision support to the Executive Secretariat and Executive Support Center.
- Introduced the Automated Collaborative Decision Support Tool to accelerate the DOD consequence management coordination and decision process.
- Effectively integrated Contractor personnel and Reserve Component Officers into the infrastructure monitoring, decision support, and Consequence Management roles.

Y2K demonstrated that the Department could create an effective CIP program to protect both critical cyber and physical infrastructures and respond to the infrastructure challenges the Department and the Nation will face throughout the 21st Century.

Broader CIP Development

Building on the Information Assurance and Y2K success, the Department of Defense is taking a broader view of the CIP problem – focusing also on the underlying critical infrastructures upon which our critical warfighting capabilities and cyber systems rest. Over the past year, DOD has been developing and proving the CIP capabilities that provide the final pieces to complete the Department's CIP strategy.

At the DOD installation levels, new and current commanders are being trained and advised on the criticality of private sector support in implementing and maintaining many of their daily activities. We have found that those commanders who have been on the job for several months have realized the need for, and on several installations, developed many unique working relationships with their local communities. These include establishment of forums (e.g., council of mayors) where commanders and local/private sector leaders discuss the vulnerabilities and resolutions to many critical infrastructure problems. Such forums of information sharing have been very beneficial for both civil and military communities.

Now, more than ever before, DOD CIP efforts are focusing on the interdependencies of our infrastructures. For example, if the Army wants to move forces out of Fort Hood, there will be a need for reliable transportation, logistics, communications, power and industrial base assets and infrastructures. In addition, we must be able to determine how these infrastructures depend on each other and understand how the loss of one impacts the ability of the others to continue to function. The first step required the Department to mature its physical vulnerability analysis and assessment capabilities by enhancing its understanding of and ability to identify commercial infrastructure dependencies. With these efforts well underway, CIP focus shifted to three major areas:

- Developing a methodology linking infrastructure impacts to CINC (i.e., warfighter) mission accomplishment. By combining inputs from the CINCs with Sector and Service efforts to link warfighter mission needs to the supporting infrastructures and assets, this capability was developed. Through a series of prototypes, this capability was proven. {1.9, 1.10, and 1.11}
- Developing an integrated assessment process that leveraged the myriad of existing focused vulnerability assessments (e.g., physical security, I.A. (Cyber), Anti-Terrorism (JSIVA), commercial assessments, etc.). into a comprehensive cyber/physical, on/off base integrated vulnerability assessment that is necessary if both warfighter and core business infrastructure vulnerabilities are to be identified and corrected. Most significantly, the production of a single, integrated assessment improved the vulnerability remediation impact taken by individual assets owners and installation commanders. This construct was also field tested at several locations to refine and enhance process. {1.12 and 1.17}
- Developing a set of standardized vulnerability assessment protocols so that every DOD assessment produces comparable results. Realizing this construct enables risk management to be practiced from a DOD-wide perspective for the first time. {1.11}

By developing these three capabilities, DOD is now in a position to effectively manage consequences because we know what the impact of an infrastructure or asset failure is. In addition, over the last year, CIP efforts have:

- Developed and promulgated the *DOD Critical Infrastructure Protection Execution Plan – Calendar Year 2000*, dated 13 March 2000. {1.17 and 1.24}
- Developed *Defense Infrastructure Sector Assurance Plans (DISAPs)* to address the identification and vulnerability remediation steps necessary from a Sector perspective and to define end-to-end sector functionality and those supporting assets essential to mission success. {1.9, 1.18, 1.19, and 1.20}
- Held monthly forums (CIPIS meetings) to improve Department-wide CIP efforts and effectively develop CIP consensus and disseminate information across DOD. {1.24}
- Developed required CIP funding details for key CIP initiatives for the FY 02-07 POM. {1.29}
- Developed prototype CIP analysis and assessment capability for identifying and assessing critical assets in support of DOD missions. {1.11}
- Developed and implemented capability to analyze and assess critical information transport dependencies on commercial telecommunications infrastructures to identify vulnerabilities and actions to mitigate potential single points of failure. {1.9 and 1.11}
- Established a multi-component working group to facilitate Logistics Sector infrastructure assurance activities. {1.17}
- Developed and initiated effort to identify Logistics Sector physical and cyber assets building on the Y2K logistics end-to-end test planning process. Focused on those assets supporting logistics processes identified by the CINCs as critical. {1.9}
- Instituted new business processes to incorporate lessons learned from vulnerability identification. Lessons learned will be applied to information infrastructure upgrades and new technology insertions. {1.9, 1.15, 1.17, 1.18, 1.20}

- Successfully included CIP Planning and Programming Guidance in Defense Planning Guidance. {1.29}
- Initiated development of a risk-management framework to guide the prioritization of infrastructure protection efforts and investments. {1.28}
- Conducted the PACNORWEST Regional Assessment of DOD sites and their supporting commercial and DI Sector infrastructures and assets in the Northwestern Washington area. The assessment refined and expanded the CIP analysis and assessment process, furthered the DI Sector characterization process, and identified asset interdependencies. {1.10 and 1.15}
- Taken major steps in implementing the DOD CIP Plan. We identified a unique set of DOD Critical Infrastructures, such as Logistics, Space, Personnel, Health Affairs, ISR, and C3, as well as those that are similar to the national infrastructures but with a DOD focus – Public Works (power, water, fuel), Transportation, Financial Services and the Defense Information Infrastructure. For each of these Defense Infrastructures a Lead Component, such as DLA for Logistics, has been designated for integrating CIP activities across the Sector. The DOD plan called for, and we have established, a CIP Integration Staff responsible for integrating CIP activities across the various Sectors. {1.17}
- Taken the first steps toward implementing ASD(C3I)'s role as the "Functional Coordinator for National Defense" and coordinate the activities of the Federal Government necessary to the national defense. {1.17}
- The Joint Staff participated in Department of Defense (DOD) Multilateral CIP Contingency Exercises involving Ministry of Defense (MoD) representatives from the United Kingdom, Germany, and France. {1.11 and 1.17}
- The Joint Staff (J-5/Global Division) is working with OSD(C3I) on the CINC Outreach program. This program is designed to educate personnel at various CINC headquarters on CIP. To date, CINC Outreach program has been to SOCOM, CENTCOM, SOUTHCOM, and PACOM. {1.9, 1.10, 1.11 and 1.17}
- The Joint Staff (J-5/Global Division) nominated CIP as topic for the Quadrennial Defense Review. {1.11}
- The Joint Staff required CINC inputs addressing the format for CIP within OPLANS, CONPLANS, and FUNCPLANS. {1.11, 1.17 and 5.1}
- The Joint Staff required Joint Strategic Capabilities Plan (JSCP) inputs addressing CIP planning guidance from the CINCs and provided CIP information to the CINCs during deliberate planning conferences and other forums. {1.11, 1.17 and 5.1}
- Analysis indicates the USMC uses over 140 logistics information systems. A key vulnerability is the volume of these systems and the resulting complexities that result from processing transactions and passing data through them. USMC has initiated a Marine Corps Logistics Information Resource (LogIR) plan to reduce the number of logistics systems and increase their efficiency in response to internal requirements.
- The Department of Navy designated a Chief Infrastructure Assurance Officer (CIAO) and established a Flag Level, DON Critical Infrastructure Protection (CIP) Council comprised of key Navy and Marine Corps stakeholders. The DON CIP Council is responsible for ensuring the DON is organized to effectively respond to the requirements of PDD 63, and the DOD Critical Infrastructure Protection (CIP) Plan.
- Established an action officer level working group to ensure Defense Infrastructure Sector leads have designated Navy and Marine Corp counterparts working with them, to ensure critical DON assets are properly incorporated into Defense Infrastructure Sector Assurance Planning.
- Supported the development of a DOD Integrated Vulnerability Assessment (DIVA). The Navy participated in 2 pilot regional assessment efforts (Tidewater and Pacific Northwest). These efforts demonstrated both the value of and the requirement for a more robust, integrated vulnerability assessment standard which builds upon existing Service and Joint Staff force protection/antiterrorist

(FP/AT) oriented assessment processes to include assessment of cyber vulnerabilities and of mission dependence upon and potential vulnerability to critical commercial infrastructures.

- Developing a Naval Integrated Vulnerability Assessment (NIVA) process - a blended protocol for a comprehensive vulnerability assessment for Navy Regions and Marine Corps equivalents. The protocol will include typically-independently-scheduled CNO or HQMC FP/AT/Physical Security vulnerability assessments and related exercises as its centerpiece, with operational dependency analysis and assessment of critical non-organic infrastructures, and information warfare Red teaming to examine cyber assets. "Pilot" test of this blended protocol will be in San Diego in May 2001. The plan is to perform this comprehensive blended protocol assessment for all Navy Regions and major Marine Corps Installations FYs 2002 and 2003.
- Developed a self-assessment manual for Navy and Marine Corps Commanding Officers. A rough draft is complete, with vetting scheduled for January 2001. Ultimately, a comprehensive CIP self-assessment manual will be distributed to all DON Commanding Officers as a companion piece or alternative to Peer-review vulnerability assessments.
- DON efforts were key in framing for DOD the CIP implications inherent in current trends toward outsourcing, privatization and paperless acquisition, particularly when concerning Logistics and Public Works sectors, and life cycle support of weapons systems.
- The Air Force established a PDD-63 Coordination Group with representation from all the functional areas represented by the DOD Sectors. {1.17}
- The Air Force included CIP in its presentations to the Senior Information Warfare Applications course as part of the education process and to ensure top down support to cyber protection activities. {Goal 1}
- The Air Force worked on identifying Anti-Terrorism/Force-Protection vulnerabilities through 41 Joint Staff Integrated Vulnerability Assessments (JSIVA) and USAF Vulnerability Assessment Team visits during CY00. Forty-four assessments are scheduled for CY01. As in previous years, the primary assessment focus is AT/FP, but physical security and emergency response will also be addressed. {1.10 and 1.12}
- The Air Force is supporting the development of a DOD Integrated Vulnerability Assessment (DIVA)--the USAF has provided inputs regarding integration of existing assessment processes, how to schedule DIVAs, team size and composition, and DIVA protocols. Set up "proof of concept" for DIVA at Malmstrom Air Force Base. {1.9, 1.10 and 1.17}
- The Air Force initiated an overseas (OCONUS) space infrastructure study to evaluate dependence upon and impact of OCONUS commercial infrastructures in accomplishing military space missions. {1.9, 1.10 and 1.17}
- Air Force Major Command civil engineers have developed infrastructure assessment teams to evaluate utility and operational infrastructures. {1.9, 1.10 and 1.17}
- The Marine Corps pursued CIP initiatives in the DII/C3 Sector, the Logistics Sector, the Financial Services Sector, and the Public Works Sector. {1.9 and 1.10}
- The Marine Corps conducted analysis and preliminary identification of USMC C4 assets and infrastructure that support day-to-day operations and warfighting. {1.9 and 1.10}
- The Marine Corps developed a HQMC Continuity of Operations Plan (COOP) to ensure the viability of assets and infrastructure. {5.1}
- The Marine Corps coordinated with Joint Program Office-Special Technology Countermeasures (JPO-STC) to formulate a methodology to assess the impact of dependencies on commercial infrastructure on day-to-day operations and warfighting. {1.11}
- The Marine Corps completed the Draft Infrastructure Sector Assurance Plan (DISAP), which maps the goals and milestones for protecting facilities, utilities, and emergency services to installations. {1.18}
- The Marine Corps has briefed II Marine Expeditionary Force (II MEF) and will brief I MEF and III MEF on CIP in support of day-to-day operations and warfighting. {Goal 1}

- The Marine Corps required military construction projects to include AT/FP line items, and, where appropriate, "harden facilities" which may be vulnerable. {1.18}
- The Marine Corps and the Defense Threat Reduction Agency (DTRA) will conduct a coordinated survey of USMC installations in the southern California region in late spring 2001. {1.19 and 1.10}
- The Marine Corps has embarked on a Combat Service Support Element-Information Technology (CSSE-IT) strategy to reduce the number of logistics systems and increase their efficiency in response to internal requirements. {1.18}
- The U.S. Navy conducted a coordinated Joint/Navy CIP vulnerability assessment in the PACNORWEST region. {1.9, 1.10 and 1.17}
- The U. S. Navy and the Defense Threat Reduction Agency (DTRA) will conduct a coordinated survey of USN installations in the southern California region in late spring 2001. {1.19 and 1.10}
- The U. S. Navy increased manning to support detect and respond capabilities. {1.19 and Goal 2}
- The U. S. Navy pursued CIP initiatives in the DII/C3 Sector, the Logistics Sector, the Financial Services Sector, and the Public Works Sector. {1.9 and 1.10}
- The U. S. Navy coordinated with Joint Program Office-Special Technology Countermeasures (JPO-STC) to formulate a methodology to assess the impact of dependencies on commercial infrastructure on day-to-day operations and warfighting. {1.11}
- The U. S. Navy completed the Draft Infrastructure Sector Assurance Plan (DISAP), which maps the goals and milestones for protecting facilities, utilities, and emergency services to installations. {1.18}
- The Navy Information Assurance Program guiding instruction was updated to accommodate the growing need for organizational structure and establish technical security publications to more readily adapt to technical changes. The Navy IA Program established specific organizations with specific and non-redundant mission responsibilities for maintaining policy and publications, centralizing a technical authority to maintain and grow the expertise essential for in-depth understanding of technical intricacies requisite for the total security solution and achieving the required near-real time operational feedback.
- The Navy completed the implementation process for the commencement of no-notice On-Line-Surveys/Vulnerability Assessments of all Navy computer systems. These assessments will verify compliance with Navy and DOD IA polices and standards. Navy will continue to provide all Navy commands vulnerability assessment services upon request. During the past year over 300 requested assessments have been conducted.
- The Navy conducted a service-wide Information Condition (INFOCON) exercise at the Echelon II Command level, which provided training and assisted in development of detailed operational procedures to implement DOD policy.
- The Navy increased manning of the Navy Computer Incident Response Team (NAVCIRT) and the Navy Component Task Force for Computer Network Defense (NCTF-CND) to enhance the pro-active support required for analysis, increased intrusion detection system monitoring and the release, tracking and monitoring of Information Assistance Vulnerability Alerts.
- The Navy established the Computer Network Vulnerability Assessment as part of deploying Battle Groups (BG) Inter-deployment Training Cycle. This assessment is designed to improve the ability of the BG to defend its networks at sea, identify and react to intrusions, correctly report intrusions within established time limits and enhance the BG's overall defensive posture. The assessment is conducted in three phases with Blue Teams confirming proper system configuration during the initial phase, teams conducting training throughout the cycle, and Red Team attack simulation during the final phase which certifies the BG's IA posture is ready to support deploy operations.
- Based on the rapid development of IA policies across DOD, Navy established web pages to serve all facets of the IA community. Navy IA web page promulgation provides ease of access to the entire spectrum of IA customers, ranging from the system administrator level, with specific technical implementation policy, guidance and tools, to the Program Managers (PM) with available security products and components.

- The Navy established the Web Risk Assessment program, which reviewed and continues to review all Navy unclassified web sites on a quarterly basis to ensure security standards compliance and compliance with DOD content policy. This is a centrally managed mission fulfilled virtually from remote Naval Reserve Support Group (NRSG) drill sites. In addition to the periodic review and assessment of stand alone web pages, the Navy is also performing aggregation analysis of all information contained on Navy web pages to determine the operational and security impacts when analyzed in the aggregate.
- The Navy established and promulgated criteria for qualifying Systems Administrators for all levels mandated by the DOD. Formal schoolhouse and mobile training teams have been established to meet the established criteria. The Navy has also established formal training for the critical positions of Information Systems Security Manager and Network Security Vulnerability Technician.
- SPACECOM submitted several CIP inputs into last JROC/JWCA process along with CND and CNA inputs.
- SPACECOM injected several CIP-relevant events/scenarios into the last Global Guardian exercise.
- The SECRETARY OF DEFENSE established the Joint Task Force – Computer Network Defense (JTF-CND) in Dec 98. The JTF-CND is responsible for coordinating and directing the defense of DOD computer systems and computer networks.
- An Information Condition (INFOCON) was established in Mar 99. The INFOCON is a five level, structured approach to react to and defend against adversarial attacks on DOD computers and telecommunications.
- DOD established the Information Assurance Vulnerability Program to provide positive control methodology and mechanisms to ensure information is rapidly disseminated and corrective action is taken against new vulnerabilities and threat to DOD systems.
- CJCS directed that the Joint Staff and CINCs address CND in all Operations and Concept Plans. Computer Network Defense is included as major objectives in several CJCS and CINC exercises.
- SPACECOM drafted plans to protect the Defense Information Infrastructure and minimize the effects of malicious viruses.
- DOD and Joint Staff drafted and/or implemented policies to limit the adverse effects of new software technologies (e.g., Java, JavaScript, VBScript, and ActiveX).
- EUCOM is sponsoring a series of Critical Infrastructure Protection initiatives. Efforts include: 1) an assessment of commercial dependencies of U.S. Forces on the German communications infrastructure, 2) a Radio Frequency Threat Assessment of critical Command and Control nodes, and 3) a series of Network Operations vulnerability assessments on critical operational C2 nodes.
- EUCOM developed a Theater Information Assurance Master Plan, which provides theater guidance for development of IA among HQs, Component, and JTF activities. The plan includes identification of a vision, desired end-state, and near term achievable goals for Defense-in-Depth of theater Network Operations.
- EUCOM is establishing a Theater C4I Coordination Center (TCCC), which will provide the EUCOM command authorities with near real-time network operations situational awareness. The TCCC is being structured to help EUCOM's command authorities (i.e., the Headquarters, Components, and attached agencies) assess the operational impact of intrusions, disruptions, and anomalies affecting EUCOM's critical C4I infrastructure.
- USCINCPAC recognized the operational importance of critical infrastructure protection and placed program responsibility within the Operations Directorate (J3) in June 00. The J3 established a CIP division at that time.
- USCINCPAC established a CIP working group identifying subject matter experts from each staff directorate to maintain liaison with DOD sector leads. This group is the focal point for CIP information and has drafted the USPACOM Theater Assurance Plan.
- USCINCPAC organized and hosted a CIP conference attended by representatives from all subordinate commands, sub-unified commands, DOD sector leads, Joint Program Office, OSD CIP,

and other interested agencies. This conference provided CIP education and training for attendees and opened lines of communication necessary to meet the USPACOM CIP program requirements and goals.

- USCINCPAC drafted a CIP appendix to all OPLAN/CONPLAN's. Three CIP appendices have been completed to date.
- USCINCPAC is building a capabilities/functions/systems/assets database to be used in planning and operational contingencies; over 600 critical assets have been identified to date.
- USSTRATCOM developed an Information Resources Management Strategic Plan, which has--as a cornerstone--Information Assurance objectives. USSTRATCOM established its own Computer Emergency Response Team (STRATCERT) and is in collaboration with the Omaha cyber community and Offutt AFB to protect computer networks.
- USSTRATCOM partnered with industry, academia and other Federal agencies to establish the Omaha Cyber Security Forum and Omaha FBI InfraGard Chapter in support of Presidential Decision Directive (PDD) 63. It serves as the focal point for private-and public-sector representatives to spearhead computer security issues and share common computer security threats and vulnerabilities.
- USSTRATCOM developed an aggressive IA training program to ensure all users are certified through baseline initial training and monthly topical IA refresher education.
- USSTRATCOM in partnership with DISA conducted an IA Tabletop exercise and incorporated lessons learned into the annual command-wide strategic exercise GLOBAL GUARDIAN.
- USSTRATCOM initiated a program with NSA and DISA to expand its Command IA Operations Reviews to include its eight subordinate Task Forces.
- USSTRATCOM proactively improved its IA Defense-In-Depth by implementing both COTS and DISA provided software security tools. The installation of tools to monitor and control all incoming e-mail traffic preempted all malicious code events that otherwise affected DOD; i.e., the I-LOVE-YOU worm.
- USSTRATCOM leveraged its own Computer Security Assessment Team ("Red Team") to test software implementations proposed for command networks and verify systems are secure as possible against potential intruders.
- USSTRATCOM partnered with DISA to conduct quarterly intrusion testing against STRATCOM networks as well as conducting an annual overall assessment of the command IA program and posture.
- USSTRATCOM is the DOD Operational Manager for the Advanced Concept Technology Demonstration (ACTD) to develop, test and operate an Automated Intrusion Detection Environment (AIDE).
- USSTRATCOM's IA program was recognized as NSA's 1999 Rowlett Award winner for organizational excellence in Information Security.
- As the DOD Sector lead for Transportation, USTRANSCOM published the Transportation Defense Infrastructure Sector Assurance Plan, which addresses action plans for both physical and cyber assurance.
- USTRANSCOM and Department of Transportation (DoT) representatives met in conference to address vulnerabilities in common defense and commercial transportation activities. Continuing dialogue with DoT is critical to ensure assured access to commercial transportation assets upon which USTRANSCOM relies heavily to meet its wartime missions. A DOD-DoT integrated process team will address redundancies and streamlining of the assessment processes.
- USTRANSCOM is actively supporting vulnerability assessments in the Pacific Northwest and in the Rocky Mountain Corridor. Additionally, the command's Transportation Engineering Agency published a detailed vulnerability assessment of transportation infrastructure required to support deployment from Ft Hood, Texas, to Gulf seaports.

- USTRANSCOM identified approximately 170 DOD and Commercial transportation nodes currently considered critical to wartime mission accomplishment, and shared those findings with ASDC3I CIP Office, Joint Staff, and with PACOM in support of its CIP Program. These nodes are the foundation upon which decisions will be made to conduct future vulnerability assessments.
- As a participant in exercise POSITIVE FORCE 01 and TURBO CHALLENGE 01, USTRANSCOM is proactively incorporating both physical and cyber CIP events to raise consciousness of the subject and to test current vulnerability assessments.
- The U. S. Space Command (SPACECOM) developed the Space Defense Sector Assurance Plan and the Extract for inclusion in the National Plan. {1.9, 1.10, 1.11 and 1.18}
- The U. S. Space Command is participating in the Rocky Mountain Corridor Regional CIP Assessment. These assessments will provide insights in the Nuclear Command and Control System and many other space related system's functionality and interdependencies. {1.9, 1.10, 1.17 and 1.18}

The only way it is possible to protect our critical infrastructures is for government and industry to work together. One of the key elements of DOD's CIP approach is to use base and installation commanders around the country to establish information sharing approaches as appropriate in their work with the private sector and with local and state governments to mitigate infrastructure vulnerabilities that can be corrected at these levels.

Appendix A (continued)
National Security Agency

In addition to recognizing NSA's technical responsibility to assist Federal agencies, the *National Plan for Information Systems Protection, Version 1* (*The Plan)* assigns NSA various roles and responsibilities and recognizes several of the Information System Security Organization's (ISSO) successes as excellent examples for other agencies and the private sector to model or build upon. A brief description of NSA's accomplishments are listed below and contain a parenthetical reference to the Section of *The Plan* that contains the role, responsibility, and success.

NSA has conducted numerous vulnerability and risk assessments of its infrastructures and has invested in a modernization of its information infrastructure that will assure critical assets and functions are properly protected. (Section 1.1) Specific accomplishments over the past 18 months include:

- Appointing a CIAO;
- Developing a CIP Plan which includes investment decisions based on the security evaluation of facilities, telephone systems, and information systems;
- Defining three levels of criticality for its systems;
- Using Y2K and Continuity of Operations plans to determine which systems fell into each level of criticality;
- Investigating several risk assessment techniques and selecting an appropriate one for use within NSA;
- Performing risk assessments of the most critical assets;
- Conducting briefings for field representatives to facilitate assessments at field sites; and
- Implement the NSA Information Systems Incident Response Team.

The NSA/ISSO regularly supports DOD and Federal Government customers through a "crawl, walk, run" process focusing on INFOSEC and OPSEC assessments, network evaluations and RED Teaming. NSA/ISSO has provided over 30 combined assessments and Red Team operations to DOD organizations and about 20 to other Federal agencies when requested by the agencies. In addition, over 30 OPSEC training classes have been provided to Federal agencies through the interagency OPSEC Support Staff. (Section 1.1.2)

The interagency working group, called the Federal Security Practices Subcommittee, has been established as a sub-committee of the CIO Council's Committee on Security, Privacy and Critical Infrastructure. NSA is providing support to the sub-committee and has senior representation on the CIO Council's Committee on Security, Privacy, and Critical Infrastructure. (Section 1.2)

NSA continues to advise and assist GSA, DOD, and OMB in the development of procurement regulations, particularly as they apply to Information Assurance-related procurements. With regard to the acquisition of IA products, NSA has worked with the National Security Telecommunications and Information Systems Security Committee (NSTISSC) to promulgate NSTISSP 11, National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information technology Products. NSTISSP 11 establishes policy regarding the acquisition of evaluated COTS and GOTS products (IA and IA-Enabled) that are to be used in national security telecommunications and information systems, as defined in National Security Directive 42, July 1990. In addition, NSA assisted the NSTISSC in developing the NSTISS Advisory and Information Memorandum: Federal Information Processing Standard (FIPS) 140-1 Validated Cryptographic Modules for Use in Protecting Unclassified National Security Systems. This Memorandum provided guidance on the acquisition and use of NIST's FIPS 140-1 validated products in national security telecommunications and information systems. (Section 1.2)

The National Information Assurance Partnership (NIAP) is collaboration between NIST and NSA to meet the security testing needs of information technology (IT) producers and consumers. The long-term goal of NIAP is to increase the level of trust consumers have in their systems and networks through the use of cost-effective testing/evaluation, and validation programs. (Section 1.2) To support this goal, NIAP has focused its activities in three key areas:

- Product and system security testing/evaluation and validation;
- Security requirements definition and specification; and
- IA research in security testing, evaluation and metrics.

Specific NIAP accomplishments include:

- Product and system security testing and evaluation:

  - Development of a Common Criteria for Information Technology Security Evaluation (CC) Standard- ISO/IEC 15408.
  - Development of a U.S. commercial sector, IT security testing/evaluation industry. Five NIAP private sector labs have been approved, with several more expected to be accredited soon.
  - Completion of approximately 10 Common Criteria evaluations on commercial products. Another 10 commercial products are currently undergoing common criteria evaluation.
  - Negotiation of a Mutual Recognition arrangement with Canada, UK, Germany, France, Greece, Norway, Finland, Italy, Spain, the Netherlands, Israel, Australia and New Zealand providing recognition of U.S. issued security evaluation certificates in these countries. This eliminates the need for U.S. IT product vendors to be evaluated in more than one country and provides excellent global marketing opportunities for U.S. vendors.
  - Promotion by NSA and NIST of a government acquisition policy to support NIAP validated products (NSTISSP 11 and NIST Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products).
  - Held the first annual International Common Criteria (CC) Conference in May 2000.

- Security requirements definition and specification:

  - Host/assist the Smart Card Security Users Group (SCSUG), which includes major smart card users such as American Express, Visa, MasterCard, Mondex, and Europay to develop security requirements (i.e., called a Protection Profile in CC terms) for smart cards. This effort will result in improved security for smart cards used in financial transactions.
  - Host/assist a Health Care Forum where members from that community meet to define security requirements for health care IT systems.
  - Host/assist a Telecommunications System Forum where members of that community meet to define security requirements for telecommunications switches and other telecommunications equipment and services. NIAP has developed a telecommunications switch protection profile (PP) as a strawman set of security requirements for the group.
  - Develop and offer education and training courses on the CC and PP development to support and encourage CIP sectors to develop security requirements using the CC and to utilize the NIAP Common Criteria Testing labs for assessing product conformance to their PPs.

- IA research in security testing, evaluation and metrics:

  - Developed an automated tool to assist in defining security requirements expressed as user-defined Protection Profiles or vendor-defined Security Targets (STs). This tool guides the PP or (ST)

developer through the CC requirement specification development process and indicates when CC violations/irregularities occur.
- Developing a tool for automated testing that can be given to the NIAP labs to ensure testing consistency among the labs.
- Developing an IA security assessment accreditation program for accrediting organizations/individuals that perform security assessment services of operational systems to Federal agencies.

NSA's National Security Incident Response Center (NSIRC) continues to provide expert assistance in isolating, containing, and resolving attacks and intrusions threatening national security systems. (Section 3.4) Examples include:

- In June 2000, NSA development of Cyber "Critic" Messaging guidelines. These guidelines define the conditions under which information of cyber attacks can be distributed through the Critic network to National Security consumers.
- In May 2000, a Defense Red Switch Network telephone was installed in the National Security Operations Center, which enhances connectivity to DOD components for cyber events.

NSA participated in the IC Continuity of Operations (COOP) exercise on 1 and 2 August 2000 with several other IC Agencies. Current DIO COOP plans will be revised based on the outcome of that exercise. (Section 5.2, Milestone 5.1)

NSA is participating in several DOD, Law Enforcement (LE) and Intelligence Community (IC) Working Groups designed to share information and techniques regarding past network intrusions. Additionally, NSA sponsored a cyber workshop with DOD, LE and IC components to address agency roles in the event of cyber attack. (Section 3.4)

ISSO Activities Highlighted

The NSA National Centers of Academic Excellence in Information Assurance (IA) Education is a program, which encourages universities to examine their information assurance curricula as well as campus IA posture, against a set of national standards. Applications are received from those universities having the most mature IA/ INFOSEC education programs. Part of the criteria used in judging applicants are a set of national training standards developed originally for use within the classified community. The university submissions to date have demonstrated that those national government standards have a universal applicability, and also serve as yet another independent validation of the content of those standards. There are currently fourteen designated centers. The call for the next set of applications began Sept. 30, 2000, and culminates in May 2001 when successful applicants are presented certificates during the annual meeting of the national INFOSEC Colloquium. These centers figure prominently in the creation of The Federal Cyber Service Program called for in The President's National Plan. (Section 7.3)

The National Security Telecommunications Information Systems Security Committee **(**NSTISSC) serves as the senior policy making body for IA in the classified community. Since 1994, The NSTISSC has highlighted the need for robust IA education and training by sponsoring a working committee for IA Education, Training and Awareness. This group has spearheaded the development and ratification of training standards for key personnel in the IA arena. The standards serve as focal points for training and education development within the Federal government as well as the broader academic community. Related to these standards is the Information Assurance Courseware Evaluation Program, which seeks to validate that courses of instruction offered by schools and commercial vendors meet the criteria of the NSTISSC training and education standards. To date five programs have been certified as having curricula

meeting the NSTISSC standards. Those programs may be found at Florida State University, Information Resources Management College, The Naval Post Graduate School, University of Tulsa, and ARC Corp. Having these certified programs of instruction available will bring much needed standardization and quality in IA training to the greater Federal as well as commercial communities. (Section 7.2). The Training Standards for key personnel in the IA area include:

- Information Systems Security Professionals - NSTISSI No. 4011;
- Designated Training Authority - NSTISSI No. 4012;
- System Administrators - NSTISSI No. 4013;
- Information Systems Security Officers - NSTISSI No. 4014;
- System Certifiers - NSTISSI No. 4015 (DRAFT); and
- Risk Analyst - NSTISSI No. 4016 (DRAFT).

The National INFOSEC Education and Training Program (NIETP) provides national leadership in the IA community. The NIETP, cited in The President's National Plan as a model for the nation, offers a variety of products and services in IA education and training. Those programs include:

- Sponsorship of The Academic Centers Of Excellence in I A Education;
- Sponsorship of the Information Assurance Courseware Evaluation Program;
- Sponsorship of Visiting professors to U. S. Military and Naval Academies;
- Leadership to the national Colloquium for INFOSEC Education; and
- A variety of additional services and products, which reach out in partnership to Business, Academia and Government.

To further its goals to improve education and training, NSA, working with leaders in academic and business arenas, convened the first national Colloquium for Information Security Education in the spring of 1997. This forum brought together Industry, Academia and Government to discuss national education requirements and solutions for meeting our nation's need for increased numbers of professionals educated in information assurance. In May 2000, the Critical Information Assurance Office hosted the fourth meeting. This gathering of representatives and stakeholders is producing sharing of courseware, and defining requirements in the IA arena. (Section 7.3)

DOD Infrastructure Assurance Plan

No additional roles and responsibilities were assigned to NSA in Defense Section of *The Plan.* However, the Defense Section discusses DOD's public key infrastructure, information assurance and intrusion detection/monitoring activities. NSA has provided significant support to DOD in these areas, particularly as Program Manager for the DOD PKI effort and through the NSIRC support to the U.S. Space Command, Joint Task Force-Computer Network Defense, and DISA.

ISSO ACTIVITIES HIGHLIGHTED

NSA's Program Management Office responsibility for the DOD PKI

DOD PKI Implementation Status – 15 September 2000: In accordance with the Deputy Secretary of Defense's 12 August 2000 policy memorandum directing Public Key Infrastructure (PKI) implementation throughout the Department, DOD components have continued to field PKI technologies and issue Class 3 certificates to active DOD employees under the direction of the DOD PKI Program Management Office. A major part of these activities over the past 12 months has involved merging efforts with the Access Card Office in order to enable the Department's new Common Access Card (CAC) to serve as the PKI

hardware certificate carrier. This effort included incorporating Local Registration Authority (LRA) capabilities into the RAPIDS terminals, connecting the DEERS database to the Certificate Authority (CA), making provisions in the DOD Class 3 Certificate Policy for a new "hardware certificate" object identifier, and deriving smart card security requirements for use in the GSA smart card procurement contract. The service components continue to issue some software certificates for servers and other immediate personnel use, but will quickly migrate to hardware tokens (the CAC) beginning in October 2000. All DOD active employees (some 3.1 million) will have Class 3 certificates by October 2002. To date DOD has issued approximately 43,000 identity certs (Army-14, 600, Navy-3, 100, AF-10,300, MC-2,700, others-12,700); 26,500 e-mail certs; 2,900 server certs; 646 LRA certs; and 107 RA certs for use on the NIPRNET. Current schedules will issue certificates on the CAC in FY-01 to between 1 and 1.3 million people.

In addition to these activities the PKI PMO has also been engaged in: an update of three major DOD PKI Documents (the *Roadmap, Certificate Policy,* and *Implementation Plan)*; development of a process for creating PK-enabled applications; development of directory services in support of the PKI; interoperability testing of applications; smart card reader testing; and development of the Target Class 4 architectural strategy.

The PKI PMO has been working closely with the Federal community and GSA/Treasury to ensure that the two PKI efforts are compatible. (Public Key Infrastructure Section).

NSA's Research Activities

NSA's Information Assurance Research Office (IARO) conducts a comprehensive research program in the technologies and techniques needed for the development of future high-assurance solutions and Defensive Information Operations tools. Most relevant to infrastructure protection, and highlighted below, are those activities aimed at detecting and preventing unauthorized access to or subversion of critical information and services. The IARO's strategy of quickly transferring promising technologies to industry for product development is intended to help ensure availability of the necessary tools to the national information infrastructure as well as traditional customers within the Department of Defense and Intelligence Community. (Objective 3)

Active Network Defense provides a source of research and advanced technology for the development of Defensive Information Operations techniques. Significant effort has been devoted to community-wide coordination of a research agenda for work in this area. Specific examples of research in intrusion detection and analysis tools include:

- Thermonator, a creative new patternless detection technique which models computer networks as thermodynamic systems, using observables such as heat and entropy to detect anomalous behavior.
- A statistically based user-profiling technique for use in identifying insider misuse behavior.
- An intrusion analyst workstation which incorporates numerous analytic and visualization technologies. This was developed for in-house use and transferred to the DIO organization.
- A prototype expert system developed for use in a flexible intrusion analysis architecture.
- The VANAS intrusion visualization system, which is based upon self-organizing map technology, is being evaluated for its ability to correlate and display data from multiple sensors in an intuitive and useful format for analysts.
- Development of a deception toolkit architecture to serve as the foundation for an operational intrusion response capability.

Cryptography is an overall enabler for information assurance, and NSA, as the nation's primary resource for cryptography, continues to provide the Federal Government's cryptographic algorithms, backed by the highest level of crypto-mathematics expertise. This year, substantial resources were devoted to supporting NIST in its specification of modern cryptographic standards for the Nation. NSA completed and delivered a comprehensive performance evaluation of the various algorithms competing for selection as the Advanced Encryption Standard (AES), performance being an important factor for NIST to weigh in its deliberation. NSA also designed and furnished to NIST a new hash algorithm with security comparable to the AES, which will provide a foundation for reliable digital signatures and related cryptographic services.

Secure Network Management is the technology area which 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. NSA developed the GSAKMP security framework, a scheme that incorporates efficient compromise recovery, and transferred it to the Internet community via the IETF. This work provides a sound theoretical foundation for further work in network control. A multi-cast network testbed was created to support protocol research, and a simulation testbed was established for studying optical network survivability.

Switched Network Security: NSA experts have developed and installed in operational contexts a mapping and monitoring tool for ATM networks. This tool has great promise and has already proven useful for managing the health of the complex ATM networks, which underlie enterprise infrastructures. Substantial transfer to the National Security community is expected in the near future.

Secure Distributed Computing: NSA has participated in the development of a secure standard for object request brokerage (ORBSEC) and has successfully lobbied for its adoption. Such a standard helps to ensure the integrity of services within service-based architectures.

Identification and Authentication: NSA has continued to provide support to the Biometrics Consortium in advancing and promoting the use of biometrics for access control. NSA has continued research on the integration of biometrics and tokens, such as smart cards, and has developed guidelines for their use in conjunction with a Public Key Infrastructure (PKI). NSA also supported NIST in the development of the Common Biometric Exchange File Format.

Appendix B
Energy (Sector Lead Agency: Department Of Energy)

The Challenge of Maintaining a Secure Energy Infrastructure

The national energy infrastructure is critical to the economic prosperity and national defense of the nation and quality of life. In recent years, the energy infrastructure has undergone substantial changes concerning the way it is owned, operated, and maintained. Increased use of computer technology and telecommunications services has not only improved the reliability and economic efficiency of the energy system, but has also opened the door to new potential vulnerabilities. Virtually all energy companies now have sophisticated computer networks that support the complex operation of their equipment and facilities as well as routine business operations. These networks are heavily relied upon, and any disruption to them could severely hamper operations.

The energy industry has been subject to hacker probes and attacks, as is the case in other infrastructures. Such incidents exploit common vulnerabilities that exist in the operational and business systems that run our infrastructures, including poor personnel security practices, ports and services open to the outside, operating systems that are not patched with current releases, improperly configured equipment or software, inadequate physical protection, and vulnerabilities related to component integration.

The interconnected nature of the Nation's infrastructures increases the risks of cascading failures and diminishes the warning time for incidents. Infrastructure systems that are highly dependent upon telecommunications and information systems are especially vulnerable as the economy becomes more interconnected through these technologies. Likewise, since all infrastructures depend upon electric power, the energy infrastructure is of central importance to the health and reliability of the Nation's infrastructure.

In the context of broader infrastructure assurance, the scale and complexities of the energy infrastructure and their impact on infrastructure security and reliability are not fully understood. Furthermore, current energy infrastructure control mechanisms have not been developed or implemented with infrastructure assurance in mind. As recent events have pointed out, not only will the energy sector continue to be vulnerable to hackers, crackers, and information warfare in the future, but it is also increasingly vulnerable to acts of God, systems failure, and human error.

Department of Energy Role

The Office of Critical Infrastructure Protection (OCIP) was established in October 1999 to direct the Department's activities in accordance with PDD–63 and the priorities established by the Secretary of Energy. The primary mission of the Office is to work with the National Energy Sector in developing the capability required for protecting the Nation's energy infrastructures. This mission encompasses the physical and cyber components of the electric power, oil, and gas infrastructures; the interdependencies among those components; and the interdependencies with the other critical national infrastructures.

The mission also includes the following:

- Identifying DOE technologies and capabilities that can protect our nation's critical energy infrastructures and facilitating their use by the private sector and other Federal agencies.

- Identifying, assessing, and leveraging private sector and non-DOE technologies and capabilities to ensure the security of DOE critical assets in a cost-effective manner.

As the critical infrastructure protection focal point for the Department, OCIP performs a number of vital functions, all of which are designed to protect our national security and ensure the general public health and safety.

Other Key Functions

OCIP also performs the following CIP-related functions:

- Identifies and develops mechanisms to transfer technologies and capabilities to industry.
- Leads and coordinates efforts within the Department to expand cooperation on energy infrastructure protection with friendly nations, international organizations, and multinational corporations.
- Evaluates and recommends ways to address legal and related issues associated with CIP for the Energy Sector.
- Assesses, in collaboration with industry, the potential benefits of standards and "best practices" for the energy infrastructure.

Other DOE CIP Outreach Activities

Workshops and Exercises:

The Department held an internal tabletop exercise in November 1999 focused on an energy critical infrastructure disruption scenario. The results of the "Dragon Sword" exercise were used to develop a list of Departmental needs. As a result of this effort, a preliminary strategy was developed to significantly enhance the Department's capabilities to meet needs of industry, the states, and the Nation for large-scale energy emergencies.

Research and Development (R&D):

The Department of Energy has an ambitious R&D program under way to make rapid strides toward enhancing the nation's capability to understand, protect against, mitigate, respond to, and recover from destabilizing energy-related outages and events. Work is already under way on two of nine research and development activities: the Infrastructure Assurance Outreach Program (vulnerability assessments) and the Energy Infrastructure Interdependencies Program. The two primary thrust areas of the R&D program are (1) analysis and risk management and (2) protection and mitigation technologies. The R&D efforts cover nine program areas:

Infrastructure Interdependencies:

> Develop methodologies and tools to characterize interdependencies among energy infrastructures and with other critical infrastructures; develop interdependence tool set to analyze the implications of technology and policy decisions;

Vulnerability Assessment:

Identify and evaluate the vulnerabilities of energy infrastructures (physical and cyber components) and develop best practices methodology for industry use;

Scale and Complexity Analysis:

Research and characterize internal dynamics of large, complex, nonlinear infrastructure, focusing on stability, countermeasures, complexity reduction, uncertainty effects, and behavior;

Consequence Analysis and Management:

Develop and leverage databases, methodologies, and tools to evaluate the public health and safety, national security, and economic consequences of infrastructure disruptions and processes for restoration and reconstitution;

Risk Management:

Develop tools for cost-effective planning/implementation of critical infrastructure protection strategies;

Policy Effects and Institutional Barriers:

Evaluate real and potential impacts of public policies and organizational procedures on critical infrastructure protection policies, plans and barriers;

Real-Time Control Mechanism Technologies:

Identify vulnerabilities of real-time control systems; develop technologies to protect against unauthorized control of or intrusion into infrastructure control systems;

Integrated Multi-sensor and Warning Technologies:

Develop integrated systems to warn of attacks and impending failures at critical nodes; focus on anomaly detection and failure warning technologies; and

Systems Engineering Education (SEED):

Develop centers of academic excellence for infrastructure assurance. In collaboration with the National Science Foundation (NSF), develop systems engineering expertise necessary to address system complexities and interdependencies and identify and mitigate vulnerabilities.

FY 2001 funding for the R&D program is $3 million.

Looking Ahead

The Department recognizes that the responsibility for assuring critical energy infrastructures lies with the owners and operators. DOE also recognizes that the challenges facing industry and other affected stakeholders (e.g., state and local governments, the public) are increasingly daunting. Our dramatically

changing and increasingly interdependent infrastructures will be ever more vulnerable, as rapid advances in technology exacerbate vulnerabilities, making protection and cost-effective mitigation measures problematic.

In this environment, DOE stands ready to provide necessary policy and technical assistance as well as R&D. Looking at our future energy infrastructure assurance activities, the Department will continue current efforts and forge new initiatives with industry and other energy stakeholders to work toward ensuring safe, secure, and reliable energy. The extensive capabilities of DOE's National Laboratories will be used to provide the necessary technical expertise to address the wide range of infrastructure assurance challenges.

Appendix C
Social Security Administration

SSA PDD-63 Plan and Timeline

The CIP discussion and timeline below shows SSA FY 2000 accomplishments in more detail.

Initial Planning - SSA Organization and Strategy:

October 1999: Although SSA was not identified as a lead (Tier I) or secondary (Tier II) agency under PDD-63, SSA determined it would beneficial for the Agency to review PDD-63 and to implement appropriate elements. By voluntarily opting to conduct a PDD-63 review, SSA took a proactive posture to ensure protection of its cyber-based systems from physical and cyber attack. SSA became the second agency to perform a PDD-63 analysis; the Commerce Department was the first. SSA is one of the five original agencies (Commerce, SSA, Treasury, HHS, Energy) to work with the CIAO on PDD-63 Project Matrix.

SSA Critical Infrastructure Assurance Officer (CIAO) is designated.

November 1999: Critical Infrastructure Planning Sub-committee, better known as the EIC Sub-Committee, is established. The EIC Sub-Committee is composed of the SSA CIAO, Deputy Commissioner for Finance, Assessment and Management, Deputy Commissioner for Systems, the Inspector General, and appropriate staff.

EIC Sub-Committee performs organizational review and establishes CIP function(s) as needed.

The Deputy Commissioner for Finance, Assessment and Management (DCFAM) is directed by the Agency CIAO to establish a Critical Infrastructure Protection (CIP) workgroup to develop and carry out strategies for implementation of PDD-63, 67 and oversee that EIC subcommittee directives are carried out. The CIP Workgroup includes all stakeholders that will have an active role in developing, implementing and managing an Agency infrastructure protection program. Major stakeholders include the Office of Inspector General (OIG), Office of Systems (OS), and the Office of Operations (DCO).

The Deputy Associate Commissioner Office of Financial Policy and Operations (OFPO) is assigned as Chairperson of the CIP Workgroup and also as the Primary Point of Contact (POC) with the National Critical Infrastructure Assurance Office.

January 2000: The SSA CIAO approves recommendations to work with the CIAO for the first step of the PDD-63 process. The first step will identify Agency assets by gathering information about what assets, data and systems are critical to SSA.

Key SSA PDD-63 staff are trained by a CIAO contractor in a three-hour overview course on PDD-63. Agencies also present at this briefing were Commerce, Treasury, and CIAO staff.

SSA PDD-63 team begins formulating strategy and a timeline for Critical Infrastructure Protection Plan (CIPP) and identifies SSA resources to work with the CIAO team.

March 2000: Memorandum sent to SSA components from DCFAM requesting assistance in meeting the ongoing requirements of PDDs 62, 63 and 67.

EIC Sub-Committee Meeting held at which Short and Long Term Recommendations are made to continue effort to enhance the SSA Security/Suitability Program.

Short Term Recommendations:

- SECRET and TOP SECRET Clearances for personnel working on PDD-63;
- Background investigations for employees and contractors;
- Background investigations for volunteers/host enrollees/others; and
- Review/strengthen agency compliance with requirement for background investigations.

Long Term Recommendations:

- Systematically review all SSA positions;
- Determine DDS responsibilities and take appropriate action; and
- Explore ways to mandate that contractors fund the cost of background investigations.

April 2000: SSA signs Memorandum of Understanding (MOU) with CIAO to conduct Step 1 of Project Matrix PDD 63 review. The MOU provides that the CIAO will later assist SSA in the completion of Steps Two and Three of Project Matrix for two of SSA's critical assets.

Compile list of names of SSA component points of contact (POC).

May 2000: Developed SSA policies for classifying infrastructure protection related information.

September 2000: Revise and extend by one year the MOU with the CIAO to extend Step 2 and Step 3 analyses to two of SSA's critical assets.

October 2000: Approval of critical asset list and proposed vulnerability analyses.

Post-CIPP Implementation Actions:

In establishing priorities for implementing an Agency critical infrastructure protection plan, there are some activities that must be deemed less critical, in terms of when they must be done, than others. The activities below will be undertaken by the workgroup either in later phases of the implementation or after the basic plan is implemented:

- Work with Office of Strategic Planning to: (1) discuss inclusion of additional or new CIP Key Initiative as part of Strategic Planning and performance measure program; (2) assure that the IT training initiative in the Strategic Plan includes infrastructure protection related training (Program 7).
- Perform GAP Analysis to determine SSA final CIPP and National CIAO Plan are consistent, and that all applicable CIPP requirements are met.

STATUS OF SSA'S CRITICAL INFRASTRUCTURE PROTECTION PLAN KEYED TO THE TEN PROGRAM AREAS OF THE NATIONAL PLAN

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

"The first program is for government and private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks to attack, and then develop and implement realistic programs to remedy the vulnerabilities, while continuously updating the assessment and remediation effort." [Extract from National Plan]

A. Identification of Critical Assets:

SSA's PDD-63 Workgroup undertook the task of identifying the Agency's assets in sub-workgroup meetings. After reaching agreement on a proposed list of assets, PDD-63 staff met with the CIAO to review the proposed approach, e.g., definitions, number of assets. Assets were aligned around the Agency's core business processes, i.e., Enumeration, Earnings, Initial Claims (Title II/Title XVI), Post-entitlement (Title II/Title XVI), Informing the Public. SSA identified 41 discrete supporting assets grouped into three categories as below.

- Facilities (11 identified), which includes hardware, software and supporting personnel located in the facility
- Cyber and Telecommunications, which includes wide-area networks considered as Asset Application systems (30 identified)

As suggested by the National Plan, an Expert Review Team (ERT) was assembled to complete the asset assessment. Representatives from all of SSA components were invited to participate in the offsite exercise. Attending the offsite were senior personnel and subject matter experts from:

- Office of Communications
- Office of Disability & Income Security Programs
- Office of Human Resources
- Office of Legislation and Congressional Affairs
- Office of Operations
- Office of Policy
- Office of Systems
- Office of Quality Assessment
- Office of Publications and Logistics Management
- Office of Information Systems Security
- Office of Facilities Management

At the 4-day offsite, the ERT received training by CIAO and BAH personnel on their role in rating SSA's assets using the CIAO-designed Infrastructure Asset Evaluation Survey (IAE). Led by a facilitator, members of the ERT completed an IAE for each of SSA's 41 assets. For each asset, the facilitator walked the ERT through the questionnaire and insured the team reached consensus on each question by calling for a show of "thumbs" on whether the team agreed with the suggested response, could live with it, or was opposed. If any members of the ERT were opposed to the group's suggested response, the opposing members were given an opportunity to make their case for an alternate response. The group also argued

their case with the opposing members, and then a vote was called for again to insure the ERT had consensus on the survey response.

The data from the 41 IAEs were input into the PMT Internet-based software ranking system that assigned values to the responses. The assets were scored in accordance with national security, economic stability, and public health and safety criteria. The CIAO- provided ranking of assets resulted in identification of 8 assets that received a score greater than 1.0. The PMT regards these 8 assets as being the most important in terms of SSA fulfilling its critical national responsibilities, and therefore these 8 critical assets require priority attention in terms of robust physical and cyber vulnerability assessments.

The CIP Workgroup reviewed the 8 assets requiring vulnerability assessments to determine status of existing or planned reviews of these assets that could meet the requirements of PDD-63 vulnerability assessments. It was determined that requirements of PDD-63 could be met by modifying existing Financial Management control reviews to include more rigorous reviews for PDD-63.

- Review of the NCC—General Control Review by Deloitte and Touche
- Review of Title II Redesign – Consolidated Program Benefits Review (D&T)
- Review of SSN Establishment and Correction System (Most of Modernized Enumeration and Enumeration Verification System) – Consolidated Program Benefits Review (D&T)
- Review of Earnings Record Maintenance System (Part of OCO/Metro West and OIO) – Consolidated Program Benefits Review (D&T)

B. Master Blanket Purchase Agreement (BPA) for PDD-63: Security Contracts

The CIP Workgroup investigated several options for procuring security-related contracts to perform the ongoing work mandated by PDDs 62, 63, and 67, and decided to use a BPA for all security-related work. Use of a BPA would afford the CIP Workgroup future efficiencies in procuring security related services, i.e. 30 days maximum time to award contracts, simplified procurement process. In September 2000, a BPA was awarded to five contractors, Netigy Corporation, Booz, Allen & Hamilton, SAIC, Inc., Janus Associates, and PricewaterhouseCoopers.

Concurrent with the initial award of the BPA, the first Task Order was awarded. The Task Order sought services for penetration testing of SSA's Sensitive But Unclassified (SBU) networks and systems, and was awarded to Janus Associates.

Additional security-related contracts are planned to be procured via this BPA over the next six years and include:

- Remaining vulnerability assessments for SSA determined critical assets;
- PDD-67 related contracts, e.g. software and support services;
- DDS security improvements;
- Gap analysis; and
- Remediation.

C. Penetration Testing

"Penetration Testing" is recognized as a vital part of risk management programs and strategies for protecting critical infrastructure. Although much of the emphasis of penetration testing is upon cyber assets, penetration testing is also important for the protection of those critical physical assets. With the evolution of computers and Information Technology both in private industry and the Federal government,

conducting the Nation's business, for the most part, is dependent upon maintaining the integrity of the nation's cyber and physical assets.

From a national security perspective, it is vital that the nation's critical infrastructure be protected from threats and attacks that would compromise the critical functions of the government and private industry. From an individual Agency perspective, it is vital that those Agency functions and assets that contribute to the critical national functions, i.e. SSA's 8 critical assets identified by PMT, must be protected from threats and attacks. It is also essential that the functions critical to the ongoing performance of the Agency's core missions, SSA's remaining 33 assets identified via PMT, receive the best possible protection from internal and external threats and attacks.

The term "Red Team Testing" is synonymous to "penetration testing" when used in this Document. Basically, penetration testing is a test of safeguards of critical infrastructure to determine whether:

- Safeguards exist;
- Safeguards are functioning as intended; and
- Modifications are necessary to protect the critical assets.

Penetration testing involves live tests with the testing individuals taking on an adversary role to try to penetrate or circumvent the safeguards in place. The testing is designed to identify actions, methods and other means that accomplish penetration of the safeguards (if any) and allow unauthorized access to the critical assets.

The testing done as part of this plan will not proceed to the point of allowing SSA assets to be damaged or rendered unusable, but will demonstrate whether assets could have been compromised.

Penetration Testing of SSA's Cyber Assets:

- On September 30, 2000, SSA initiated a contract for penetration testing of its Sensitive But Unclassified (SBU) networks and systems. The contract was for a five-month period to develop and integrate a process for identifying internal, as well as external security vulnerabilities in SSA's computer architecture. The Statement of Work required testing to be done across all platforms, which includes but is not limited to Windows/NT, UNIX, telephone services, email exchange servers, Internet and Intranet access, and any other SSANet connectivity where penetration may cause a disruption in the daily business process of SSA.
- Upon finding a point of vulnerability, the contractor will electronically Document the information and process proper notifications to SSA personnel. SSA will provide for immediate remediation of identified vulnerability where feasible.
- The contractor's final report, including findings of vulnerabilities and recommendations for remediation, is due on February 28, 2001. The contractor has promised to be available for consulting with SSA if needed through March 2001.

D. Vulnerability/Risk Assessments

In general, vulnerability assessments and risk assessments are parts of an overall risk management strategy. A vulnerability assessment indicates where controls or lack of controls create an opportunity for a threat to exploit a particular resource or asset. A risk assessment provides information on the potential impact and likelihood of an asset being damaged or compromised. The information obtained from a vulnerability assessment can be used to target mitigation of the threats in the most cost beneficial manner as part of the risk management strategy.

The vulnerability assessment process at SSA will include full identification and analysis of all threats that may affect the asset, the vulnerabilities inherent in the environment of the asset, the potential impact of the threat on the asset vulnerabilities and the resulting risks. A range of remediation/mitigation measures will be examined for each risk and recommendations will be made to SSA executives. The recommendations will include, but not be limited to, identification of vulnerabilities, recommended remediation actions, including projected costs, what risks should be accepted, or mitigated in part to reduce the risk to an acceptable level.

The PDD Workgroup will:

- Develop new vulnerability assessment requirements for physical assets that include CIP review requirements;
- Develop new vulnerability assessment requirements for cyber assets that include CIP review requirements; and
- Verify and review prior vulnerability assessments of physical critical assets.

Before a plan to enhance physical security was put into place, in-house physical security staff, other SSA staff and independent contractors conducted a series of vulnerability assessments of the NCC. These assessments included the possibility of penetration by terrorists, unauthorized visitors, unauthorized employees and vehicles and were conducted by:

- Department of Transportation 1993
- Brown and Company 1994
- Office of Protective Security Services 1997
- Office of Inspector General 1997
- Cetrom 1997
- Department of the Navy 1997

After the plan was put into place, further assessments of construction progress and continuing vulnerabilities were performed by:

- Office of Protective Security Services 1998
- Office of Inspector General 1998
- Price Waterhouse Coopers 1999
- Office of Protective Security Services 2000
- Price Waterhouse Coopers 2000

If assessments identify vulnerabilities, the vulnerabilities are listed as findings in formal written reports. Recommendations for correction are also included. All accepted recommendations are corrected and the corrective action is tracked. Office of Protective Security Services performs formal risk analyses of the NCC twice yearly. Informal analyses are conducted about six times a year.

- Verify and review prior vulnerability assessments of cyber critical assets.

- Verify that the 3-year cycle for Physical Reviews meets PDD-63 requirements. If necessary update 3-year Physical Security review policy to include a determination as to whether any newly identified asset should be included as a critical asset.

- Assure there are ongoing plans and milestones for new vulnerability assessments for physical critical assets in the 3-year review cycle that include CIP assets.

- Develop plans and Statements of Work to utilize contractors to perform new vulnerability assessments/audits.

- Modify current audit/review contracts to include new vulnerability assessments that include critical infrastructure protection review criteria where possible.

- Prioritize identified risks/threats from vulnerability assessments, reviews and audits and report to EICC.

- For physical assets, assure risk mitigation plans and milestones are developed and implemented for each identified vulnerability—assure that plans identify and include level of protection necessary to mitigate vulnerability.

- For cyber assets, assure risk mitigation plans and milestones are developed and implemented for each identified vulnerability—assure plans identify and include level of protection necessary to mitigate vulnerability.

- For both Physical and Cyber assets reevaluate and test risk mitigation steps and revise as may be necessary.

- Track and monitor critical infrastructure risk remediation plans and remediation milestones. Require quarterly updates showing progress and assure compliance through the EIC Subcommittee (Lead: DCFAM/OFPO/DFPS).

- Perform vulnerability assessments of any new Agency assets or existing ones that are modified and are impacted from changes in the SSA business processes. Require remediation plans as may be needed and monitor progress.

E. Development/Issuance of Remediation Plan
Scheduled for FY 2002

F. Security Benchmarking

The term "Benchmark" means a standard or point of reference used to measure quality or value. Security benchmarking compares an organization's level of security with that of other organizations. In September 2000, SSA received the highest rating of all Federal agencies for computer security, i.e., a "B" rating by the House Government Reform Subcommittee for Management, Information and Technology. Despite this, the CIP Workgroup decided to acquire benchmarking services to compare SSA's systems security preparedness with "the best in the business" companies in the private sector such as such as large financial, manufacturing, insurance or service companies. Comparisons of similar organizations to SSA will include recent as well as historical benchmarking activity taking into account improvements in information systems security technology and procedures

- September 2000: A benchmarking contract was awarded to Atomictangerine, a company that measures against 350+ baseline controls and 17 security areas. Data will be gathered from meetings

with key component contacts responding to the benchmarking questionnaire to insure an accurate representation of the Agency's practices. Atomictangerine will provide training for key individuals prior to the completion of the questionnaire.

- The final report is expected in February 2001.

PROGRAM 2: Detect Attacks and Unauthorized Intrusions

"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 Team (CERTS) and other means, in order to analyze the attacks and assist sites in defending against attacks." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall include but not be limited to the following actions:

- Assure sufficient Cyber safeguards are in place to detect Attacks and unauthorized Intrusions.
- Assure sufficient Physical safeguards are in place to detect Attacks and unauthorized Intrusions.
- Discuss with appropriate internal specialists for physical and cyber security:

    - Sufficiency of systems security access, firewalls, etc
    - Monitoring of systems and physical assets for unauthorized intrusions
    - Adequacy of Federal Protective and Contract Guard procedures

- Revise Procedures if necessary.

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

"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." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall include but not be limited to the following actions:

- SSA Office of Inspector General (OIG) to Establish Law Enforcement liaisons with external; organizations and Federal law enforcement agencies;
- Enhance Electronic Crimes unit in SSA OIG;
- Assure OIG included in Incident Reporting Process and Emergency;
- Establish Response Team; and
- Publicize Penalties for Employee misuse and abuse of critical assets.

PROGRAM 4: Share Attack Warnings in Timely Manner

"Improved Federal Information Sharing: In the immediate term, Federal Systems administrators have extensive data on anomalies and possible intrusions. These Federal systems administrators will be required to send data on systems 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 the incident data. Having access to all-source information, the NIPC and FedCIRC can combine this reporting information with other information they have to determine the patterns of intrusions or connections among seemingly random occurrences." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall include but not be limited to the following actions:

- Review existing procedures and establish new or revised Agency Attack Warning Procedures as may be necessary;
- Develop methods to fast track global Agency warnings and alerts about cyber and physical attacks;
- Coordinate with External Organizations and agencies, such as FedCIRC, to assure sharing of CIP Attack Information is done in a timely manner; and
- Assure SSA OIG included in Warning and Alert Process.

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

"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 too deal with the information attacks." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall include but not be limited to the following actions:

- SSA already has in place capabilities for Response, Reconstitution and Recovery. The Workgroup will review these procedures from a PDD-63 perspective to assure compliance with PDD-63 requirements;

- Review, revise, and/or Enhance existing Response Procedures;

- Develop and Announce Incident Response Procedures and assure that the procedures include:
  - indicators and warnings of infrastructure attacks;
  - incident reporting process that includes collection and reporting
  - analysis of incidents;

- Response and Continuity of Operations plans;

- A process for responding to infrastructure attacks while attacks are underway and identifying and minimizing damage;

- Notification to OIG;
- Establish Agency Incident Response Team (SSASRT) and related guidance;
- Provide designated Executives briefing and related guidance on their roles as members of the SSASRT;
- Establish Requirement for Ongoing Incident Reports for EIC; and
- Review Agency Contingency Plans for Backup and Recovery from both a Cyber and Physical Asset perspective and recommend (if necessary) modifications to include PDD-63 and PDD-67 requirements.

PROGRAM 6: Enhance Research and Development in Support of Programs

"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." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) will coordinate with national-level research facilities such as NIST.

R&D programs are not normally part of SSA activity, but cooperation with other such programs is under consideration by the Administration and is essentially budget dependent. Whether selected Agencies will receive funding for independent R&D is not clear at this time. Should funding become available for selected agencies, SSA will review and evaluate any resulting research findings and apply and or implement them as part of the Agency Infrastructure Protection Program as may be appropriate or required.

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

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

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall include but not be limited to the following actions:

- Assess Agency needs for Information Technology personnel and Training;
- Review Agency Strategic Plan and include IT training initiative;
- Begin Agency CIP Awareness Program and Training;

- Provide for Physical and Cyber Infrastructure Protection Information sessions to focus upon a program to provide and enhance skills of employees to assure they have skills sufficient to develop, implement and perform PDD-63 related duties and functions. Develop and perform the following:

    - Executive Briefings;
    - Security conferences;
    - Entrance level Training;
    - Specialized Training (Certification of Information Technology Specialist); and
    - IVT Training.

- Develop and Distribute Information Media such as:
    - PDD-63 related Awareness bulletins;
    - PDD-63 related Desk Guides;, and
    - Online PDD-63 related information.

The Agency has made a concerted effort to assure the skill level of CIP professionals. The first SSA CISSP is the chief technical expert in the CIP area. The SSA Information Systems Security Officer now holds a CISSP, and four other security professionals in the CIP area now have CISSP certification.

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

"The Eighth Program will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber attack." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) will support National cyber-security awareness programs. SSA will participate as necessary in the national-level program, and the Agency will do the necessary planning and work to carry out any directives in this area.

PROGRAM 9: Adopt Legislation and Appropriations in support of Programs 1-8

"The Ninth Program develops the legislative framework necessary to support initiatives proposed under other programs. This action requires intense cooperation between the Federal government, including Congress, and private industry." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall include but not be limited to the following actions:

- Develop Key Initiative proposal for CIP;

- Develop Appropriate Budget Requests; and

- Utilize Existing Funding Where Possible.

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

"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." [Extract from National Plan]

To address the goals and objectives of this "Program" phase of the National Plan, as well as to strengthen the Agency's Management Control Program by including new infrastructure protection measures and enhancing existing ones, the Agency Critical Infrastructure Plan (CIPP) shall insure compliance with all current SSA procedures that provide for confidentiality of all SSA-maintained Privacy Act information.

Continuing attention will be given to privacy issues as they relate to implementation of this plan:

- Consider these issues as CIPP progresses, and
- Conduct review of CIPP (when completed) to assure Program 10 guidelines are accomplished.

Appendix D
Index to Acronyms

ACRONYM	DEFINITION
AAR	Association of American Railroads
ACE	Army Corps of Engineers
ACERT	Army Computer Emergency Response Team
ACTD	Advanced Concept Technology Demonstration
AES	Advanced Encryption Standard
AFOSI	Air Force Office of Special Investigations
AICPA	American Institute of Certified Public Accountants
AIDE	Automated Intrusion Detection Environment
AMVER	Automated Mutual-Assistance Vessel Rescue
AMWA	Association of Metropolitan Water Agencies
APEC	Asia Pacific Economic Cooperation
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications & Intelligence)
AWWA	American Water Works Association
BAH	Booz-Allen & Hamilton, Incorporated
BFSG	Business Facilitation Steering Group
BG	Battle Group
BMO	Biometrics Management Office
BPA	Blanket Purchase Agreement
C&A	Certification and Accreditation
CAC	Common Access Card
CAMS	Communications Area Master Stations
CC	Common Criteria
CENTCOM	US Central Command
CEO	Chief Executive Officer
CESG	Communications Electronic Security Group (UK)
CFO	Chief Financial Officer
CIAO	Chief Infrastructure Assurance Officer

ACRONYM	DEFINITION
CIAO	Critical Infrastructure Assurance Office
CICG	Critical Infrastructure Coordinating Group
CINC	Commander in Chief
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPMG	Critical Infrastructure Protection Management Group
CIPP	Critical Infrastructure Protection Plan
CIPTP	Critical Infrastructure Protection Training Program
CISWG	Communications & Information Sector Working Group
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMVP	Cryptographic Module Validation Program
CNA	Center for Naval Analysis
CND	Chief of Naval Development
CNO	Chief of Naval Operations
COMMSTAs	Communication Stations
CON	Certificate of Networthiness
CONUS	Continental/Contiguous United States
COOPS	Continuity of Operations Plans
COTS	Commercial Off-The-Shelf
CSE	Communications Security Establishment
CSIRC	Computer Security Incident Response Capability
CSN	Communication System Network
CSSE-IT	Combat Service Support Element-Information Technology
DCFAM	Deputy Commissioner for Finance, Assessment and Management
DCFL	Defense Computer Forensics Laboratory
DCIO-IA	Deputy CIO for Information Assurance
DCO	Office of Operations
DEERS	Defense Eligibility & Enrollment Reporting System
DI	Defense Infrastructure
DiD	Defense in Depth

ACRONYM	DEFINITION
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAP	Draft Infrastructure Sector Assurance Plan
DISAPs	Defense Infrastructure Sector Assurance Plans
DIVA	DOD Integrated Vulnerability Assessment
DLA	Defense Logistics Agency
DMZ	Demilitarized Zone
DOC	Department of Commerce
DOD	Department Of Defense
DOD CERT	DoD Computer Emergency Response Team
DOE	Department Of Energy
DOJ	Department Of Justice
DON	Department of Navy
DOT	Department Of Transportation
DTRA	Defense Threat Reduction Agency
EDS	Electronic Data Systems Corporation
EIIP	Energy Infrastructure Interdependencies Program
EIM	Enterprise Infrastructure Management
ELES	Emergency Law Enforcement Services
EPA	Environmental Protection Agency
ERT	Expert Review Team
ESMT	Enterprise Security Management Team
ETA	Education, Training and Awareness
EU	European Union
EUCOM	European Command
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FIDNet	Federal Intrusion Detection Network

ACRONYM	DEFINITION
FIPS	Federal Information Processing Standard
FLETC	Federal Law Enforcement Training Center
FP	Force Protection
FS	Financial Services
FUNCPLANS	Functional Plans
FY	Fiscal Year
GAO	General Accounting Office
GIG	Global Information Grid
GIS	Geographic Information System
GNOSC	Global Network Operations and Security Center
GOE	General Operating Expenditures
GOTS	Government Off-The-Shelf
GPS	Global Positioning System
GSA	General Services Administration
GSA ACES	GSA Automated Certificates Enhancement System
GUI	Graphical User Interface
HEPA	High Efficiency Particulate Arresting
HHS	Department of Health and Human Services
HQMC	Headquarters Marine Corps
HUD	Department Of Housing And Urban Development
I&C	Information and Communications
IA	Information Assurance
IAAC	Information Assurance Advisory Council
IAOP	Infrastructure Assurance Outreach Program
IAPMO	Information Assurance Program Office
IARO	Information Assurance Research Office
IARR	IA Readiness review
IAVAs	Information Assurance Vulnerability Alerts
IBCT	Interim Brigade Combat Teams

ACRONYM	DEFINITION
IC	Intelligence Community
IDC	Information Dominance Center
IFC	Integrated Facility Certification
IG	Inspector General
IIA	Institute of Internal Auditors
INFOCON	Information Condition
INFOSEC	Information Systems Security
IO	Information Operations
IOC	Initial Operating Capability
IS/CIP	Information Sharing/Critical Infrastructure Protection
ISAC	Information Sharing and Analysis Center
ISACA	Information Security Audit and Control Association
ISO	Information Security Office(r)
ISS	Information Systems Security
ISSM	Integrated Safeguards and Security Management
ISSO	Information System Security Organization
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Program
IT	Information Technology
ITAA	Information Technology Association of America
ITL	Information Technology Laboratory
IWG	Interagency Working Group
JMD	Justice Management Division
JMRR	Joint Monthly Readiness Report
JOIC	Joint Operations Intelligence Center
JPO-STC	Joint Program Office-Special Technology Countermeasures
JROC	Joint Required Operational Capability
JRVIO	Joint Reserve Component Virtual Information Organization
JSCP	Joint Strategic Capabilities Plan
JSIVA	Joint Staff Integrated Vulnerability Assessment
JTF	Joint Task Force

ACRONYM	DEFINITION
JTF-CND	Joint Task Force - Computer Network Defense
JWCA	Joint Warfighting Capabilities Assessment
KAI	Key Asset Initiative
LE	Law Enforcement
Legats	Legal Attaches
LogIR	Logistics Information Resource
LRA	Local Registration Authority
MCEB	Military Communications-Electronics Board
MEF	Marine Expeditionary Force
MEI	Minimum Essential Infrastructure
MISLE	Marine Information for Safety and Law Enforcement
MoD	Ministry of Defense
MOU	Memorandum of Understanding
MSIS	Marine Safety Information System
NACD	National Association of Corporate Directors
NACS	NEMIS Access Control System
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NAVCIRT	Navy Computer Incident Response Team
NCC	National Coordinating Center
NCTF-CND	Navy Component Task Force for Computer Network Defense
NEMIS	National Emergency Management Information
NENA	National Emergency Numbering Association
NERC	North American Electric Reliability Council
NIAP	National Information Assurance Partnership
NIETP	National INFOSEC Education and Training Program
NIPC	National Infrastructure Protection Center
NIPRNET	Non-Classified Internet Protocol Router Network

ACRONYM	DEFINITION
NIST	National Institute of Standards and Technology
NIVA	Naval Integrated Vulnerability Assessment
NPC	National Petroleum Council
NRC	Nuclear Regulatory Commission
NRSG	Naval Reserve Support Group
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSAP	National Security Assurance Partnership
NSC	National Security Council
NSF	National Science Foundation
NSIP	Network Security Improvement Program
NSIRC	National Security Incident Response Center
NSTAC	National Security Telecommunications Advisory Council
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSP	National Security Telecommunications and Information Systems Security Plan
NTIA	National Telecommunications and Information Administration
NVLAP	National Voluntary Laboratory Accreditation Program
OCIP	Office of Critical Infrastructure Protection
OCONUS	Outside the Continental United States
OECD	Organization for Economic Cooperation & Development
OFPO	Office of Financial Policy and Operations
OIG	Office of Inspector General
OIOG	Office of Inspector General
OITSP	Office of Information Technology Security and Privacy
OMB	Office of Management & Budget
OPDIV	Operating Division
OPLANS	Operations Plans
OPSEC	Operations Security
OS	Office of Systems
OSC	Operations System Center

ACRONYM	DEFINITION
OSD	Office of the Secretary of Defense
PACNORWEST	Pacific Northwest
PACOM	US Pacific Command
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PKI	Public Key Infrastructure
PM	Project Matrix
PM	Program Manager
PMO	Program Management Office/®
POC	Point of Contact
PP	Protection Profile
PSR	Personnel Security Representatives
R&D	Research and Development
RAPIDS	Real-Time Automated Personnel Identification System
RBAC	Role-based Access Controls
RNOSC	Regional Network: Operations and Security Centers
SAR	Search and Rescue
SBA	Small Business Administration
SCADA	Supervisory Control and Data Acquisition
SCSUG	Smart Card Security Users Group
SDWA	Safe Drinking Water Act
SES	Senior Executive Schedule/Service
SIPRNET	Secret Internet Protocol Router Network
SOCOM	US Special Operations Command
SOUTHCOM	US Southern Operations Command
SPACECOM	U. S. Space Command
SSA	Social Security Administration
SSL	Secure Socket Layer
ST	Security Targets

ACRONYM	DEFINITION
STRATCERT	USSTRATCOM Computer Emergency Response Team
TCCC	Theater C4I Coordination Center
TCI	Treasury Critical Infrastructure
TCIPP	Treasury Critical Infrastructure Protection Plan
TIA	Telecommunications Industries Association
TVA	Tennessee Valley Authority
USAF	United States Air Force
USCINCPAC	United States Commander in Chief, United States Pacific Command
USFA	United States Fire Academy
USJFCOM	U.S. Joint Forces Command
USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
USTA	United States Telecom Association
USTRANSCOM	United States Transportation Command
VA	Department of Veterans Affairs
VA-CIRC	VA Critical Incident Response Capability
VAPKI	VA Public Key Infrastructure
VCTS	Vulnerability Compliance Tracking System
VHS	Vital Human Services
WAN	Wide Area Network
WITSA	World Information Technology and Services Alliance
WPISP	Working Party on Information Security and Privacy
Y2K	Year 2000