STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

COMPUTER NETWORK DEFENSE FOR THE UNITED STATES OF AMERICA

BY

COMMANDER ARTHUR F. GALPIN, III
United States Navy

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

COMPUTER NETWORK DEFENSE FOR THE UNITED STATES OF AMERICA

by

COMMANDER ARTHUR F. GALPIN, III
United States Navy

Professor Malcolm Cowley
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: CDR Arthur F. Galpin, III, USN

TITLE: Computer Network Defense for the United States of America

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 50 CLASSIFICATION: Unclassified

The terrorist attacks of September 11th 2001have brought increased attention to the nation's vulnerabilities. One of these vulnerabilities is the nation's computer networks. While a level of vulnerability was acknowledged prior to 11 September, little was done to effectively implement Computer Network Defense (CND). After 11 September, the nation was energized to make improvements to homeland security. Efforts to improve CND were energized as well.

After the terrorists' attacks, the president established two key positions to address the security of the nation. He created the Office of Homeland Security to be headed by former Pennsylvania Governor Tom Ridge and created the position of special advisor to the president for cyberspace security. The creation of a special advisor for cyberspace security illustrates the new awareness of the importance of CND.

This paper examines our national policy for CND, organizations established for CND, the vulnerabilities and threats to the nation's computer networks and propose changes to improve national CND.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

COMPUTER NETWORK DEFENSE FOR THE UNITED STATES OF AMERICA

"Today, the homeland threat is from any country, terrorist organization, or hacker behind a computer anywhere in the world."

— VADM A. K. Cebrowski, USN, Commandant U.S. Naval War College

The United States of America's increased reliance on computers and computer networks has increased its vulnerability to computer network attack. Should coordinated attacks of this nature materialize, the results could be catastrophic. Security against computer attacks is critical to the nation's well being and ensuring national security. The federal government, which is chartered to "provide for the common defense,"[1] has a responsibility to defend the nation against all forms of attack, including computer based cyber attack. Countering this threat requires comprehensive changes to government policy and organization. These changes must coordinate the nation's computer defense efforts to provide comprehensive protection, minimize damage and quickly recover from any damage that may occur. In today's Information Age, protection of the nation's computers and computer networks, the computer infrastructure, and assuring its reliability is a critical component of national security.

FEDERAL GOVERNMENT COMPUTER NETWORK DEFENSE EFFORTS

The need for computer network defense was recognized by the federal government in the early 1990s. The federal government efforts have included a presidential commission to examine the problem, a Presidential Decision Directive to establish offices to address the problem, and a national plan to combat the problem. The problem of computer network defense was even mentioned in the December 2000 National Security Strategy. Despite these efforts the nation has not established an effective computer network defense. Numerous Government Accounting Office reports cite weaknesses throughout the public and private sector. A complete understanding of the federal government's efforts to date is critical to determining the next steps to ensure an effective computer network defense is attained.

PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

The first national effort to address our vulnerabilities occurred in July 1996 when Presidential Executive Order 13010 established the President's Commission on Critical Infrastructure Protection. One of the Commission's tasks was to "recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring continued operation."[2] Critical infrastructures were defined as

systems whose "incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" and included "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government."[3]

In addition to the Commission, Executive Order 13010 created myriad subgroups; a Principals' Committee, a Steering Committee, an Advisory Committee and an Infrastructure Protection Task Force. The executive order was amended on three separate occasions to increase the size of some of the committees and to provide for classification authority. The report of the President's Commission on Critical Infrastructure Protection was published in October 1997.

The report states that: "Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector."[4] The President's Commission on Critical Infrastructure Protection recommended seven strategic objectives that were aimed at facilitating this new relationship between the public and private sector. The report's seven objectives are:

- Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.

- Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.

- Establish national structures that will facilitate effective partnership between the federal government, state and local governments and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning, and programs.

- Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.

- Initiate a series of information security management activities and related programs demonstrating government leadership.

- Sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts.

- Increase investment in infrastructure assurance research from $250 million to $500 million in FY99, with incremental increases in investment over a five-year period to $1 billion in FY04.[5]

The recommendations of the President's Commission on Critical Infrastructure Protection provided a starting point for improving the nation's defense against computer based attacks. As a staring point, the recommendations focus almost exclusively on the private sector, emphasizing a need to create partnerships. The federal government's independent role was limited to providing a good example, updating legislation and increasing R&D funding. The recommendations did not address any immediate actions necessary to combat the current threats, the need for accountability, the military's role in defending the nation from cyber threats, or the differences between cyber attacks as an act of war, terrorist cyber attacks or unlawful hacker activity. Also, the recommendations did not address intelligence requirements, coordination with other nations, or assessing our nation's vulnerabilities.

PRESIDENTIAL DECISION DIRECTIVE 63

In May 1998, President William Clinton signed Presidential Decision Directive 63 (PDD-63). PDD 63 "builds on the recommendations of the President's Commission on Critical Infrastructure Protection" and "sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security to government systems by the year 2000"[6] To achieve these goals, PDD-63 formalized the framework for federal government efforts.

PDD-63 set up a new structure to deal with the challenge of infrastructure protection. It established a National Coordinator who is responsible for critical infrastructure as well as foreign terrorism and threats of domestic mass destruction. The PDD also created the National Infrastructure Protection Center (NIPC) at the FBI, the Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce, and the National Infrastructure Assurance Council (NIAC) to provide guidance in the policy formulation of a National Plan. The NIPC was manned with FBI and other department and agency investigators with experience in computer crime and infrastructure protection. The mission of the NIPC is to provide warning, analysis, law enforcement investigation and response. The CIAO was created to support the National

Coordinator's effort to develop a national plan and to coordinate a national education and awareness program, and legislative and public affairs. The NIAC is a council of major infrastructure providers and state and local government officials appointed by the president. The president also appoints a Chairman with the National Coordinator serving as Executive Director. PDD-63 also provided policy for the establishment of an Information Sharing and Analysis Center (ISAC), specializing in each of the identified areas of critical infrastructure to be protected. The private sector was encouraged to set up an ISAC with the Federal Government, modeled on the Centers for Disease Control and Prevention (CDC).[7]

Recognizing the importance of a public-private partnership required to protect the nation's critical infrastructure, PDD-63 designated various agencies to be the Lead Agency in each of the critical areas or sectors. A senior official in those agencies is to be designated as the Sector Liaison Official who will work with the private sector to identify a private sector counterpart. These two representatives are to contribute to the development of a National Infrastructure Assurance Plan. Table 1 below, shows the designated Lead Agencies for Sector Liaison and areas of responsibility.[8]

For areas in which the federal government clearly has the lead, Lead Agencies for Special Functions are designated with a senior official appointed to serve as a Functional Coordinator for that part of government. Table 2 below, shows the designated Lead Agencies for Special Functions and areas of responsibility.[9]

To coordinate the interagency efforts, PDD-63 created the Critical Infrastructure Coordination Group (CICG). The CICG is chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism with membership including the Sector Liaison Officials and Functional Coordinators of the Lead Agencies, representative from the National Economic Council, and representatives from other relevant departments and agencies.[10]

Additionally, PDD-63 directs that every department and agency shall appoint a Chief Information Officer (CIO) responsible for information assurance and they shall designate a Chief Infrastructure Assurance Officer (CIAO) responsible for the protection of all other aspects of that department's or agency's critical infrastructure.[11]

Lead Agencies for Sector Liaison	Area of Responsibility
Department of Commerce	Information and communications
Department of Treasury	Banking and Finance
Environmental Protection Agency	Water Supply
Department of Transportation	Aviation Highways Mass Transit Pipelines Rail Waterborne Commerce
Department of Justice	Emergency law enforcement services
Federal Emergency Management Agency	Emergency fire service Continuity of government services
Health and Human Services	Public health services, including prevention, surveillance, laboratory services and personal health services
Department of Energy	Electric power Oil and gas production and storage

TABLE 1 - LEAD AGENCIES FOR SECTOR LIAISON

Lead Agencies for Special Functions	Area of Responsibility
Department of Justice	Law enforcement and internal security
Central Intelligence Agency	Foreign intelligence
Department of State	Foreign affairs
Department of Defense	National defense

TABLE 2 - LEAD AGENCIES FOR SPECIAL FUNCTIONS

In establishing a new structure to administer the federal government's efforts to improve critical infrastructure protection, PDD-63 has increased the federal bureaucracy. Not only has it created new positions and offices, it has also divided up the problem into sectors and functional areas, assigning responsibility to a number of different departments and agencies. Establishment of new offices to address a new problem is a method of providing specific resources to address a specific problem, however, the new offices were not chartered under the direction of a single leader, but placed within different existing departments. The structure

established by PDD-63 presents a coordination challenge. Maintaining unity of effort is extremely difficult when the efforts are led by different organizations with different leadership and potentially differing priorities.

The stove-piped effort established by PDD-63 is a recipe for disaster. Randy Barrett, senior correspondent for Interactive Weekly wrote:

> It is also increasingly clear that cyber attackers don't think like stovepiped bureaucrats. The automated Code Red worm brought down servers across industry and government indiscriminately. In this light, critics say, PDD-63 offered a dysfunctional blueprint.[12]

Unity of effort under PDD-63 is further diluted because the National Coordinator responsible for pulling together this disjointed critical infrastructure protection effort is also responsible for foreign terrorism and threats of domestic mass destruction.[13]

There are some good attributes to PDD-63. It went beyond the recommendations of the President's Commission on Critical Infrastructure Protection and established a specific goal to be achieved; reliable, interconnected and secure information system infrastructure by the year 2003. The directive also went beyond the commission's recommendations by recognizing that there is an immediate threat, directing the federal government to address vulnerabilities, and recognizing the need for a comprehensive national plan.[14]

In developing the national plan, PDD-63 directed that each Lead Agency designate a Sector Liaison Official to team with a private a sector counterpart and contribute to a National Infrastructure Assurance Plan. These individuals were to assess the vulnerabilities of the sector to cyber or physical attacks; recommend a plan to eliminate significant vulnerabilities; propose a system for identifying and preventing attempted major attacks; and develop a plan for alerting, containing and rebuffing an attack in progress and then rapidly reconstituting minimum essential capabilities in the aftermath of an attack.[15]

The National Infrastructure Assurance Plan, called for by PDD-63, was to provide milestones for accomplishing the following subordinate and related tasks.

- Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates.

- Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

- Warning: A national center to warn of significant infrastructure attacks will be established immediately.

- Response: A system shall develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

- Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

- Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

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

- Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

- International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

- Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding

critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.[16]

The call for a national plan and the guidance provided in developing that plan was a significant improvement over the recommendations made by the President's Commission on Critical Infrastructure Protection. The guidance provided was more comprehensive and included important items overlooked by the commission such as intelligence and international cooperation. The title of the plan limits the scope of issues being addressed to national infrastructure assurance, but it does not address some of the larger issues. Larger issues include cyber attack as an act of war, distinguishing between types of cyber attack, and the role of the Department of Defense to defend the nation against international cyber attack. The document makes it appear that the Department of Defense does not have a significant role to play. Additional issues that are not part of the guidance is to determine the interdependencies among the critical sectors as part of the vulnerability analysis, the need to examine the organizational structure being built to ensure that it can be effective, the need for incentives and sanctions to guarantee implementation of the plan, and failure to identify resources to implement the directive's requirements.

EXECUTIVE ORDER 13130

Executive Order 13130, signed July 14, 1999, created the National Infrastructure Assurance Council (NIAC) to enhance the partnership of the public and private sectors in protecting our critical infrastructure. The NIAC was directed to propose and develop ways to encourage private industry to perform periodic risk assessments, and monitor the development of private sector Information Sharing and Analysis Centers and provide recommendations to the National Coordinator and the National Economic Council on how these organizations can best foster improved cooperation. Members of the Council were to be appointed by the president from the private sector, state and local government and were to serve without compensation.[17] The NIAC was created to address the lack of private sector participation in efforts laid out in PDD-63. One may wonder if participation in the Council was achieved given that the Council was to serve without compensation. Regardless, participation in the federal government's efforts did not meet expectations as is evident in the national plan that was required by PDD-63 and released the beginning of the following year.

NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION

"A concerted attack on the computers of any one of our key economic sectors or governmental agencies could have catastrophic effects."

— President William J. Clinton, President of the United States

The "National Plan for Information Systems Protection Version 1.0 – An Invitation to a Dialogue," was released by The White House on January 7, 2000. The plan sets out two overarching goals: the establishment of the U.S. government as a role model in information security, and the development of a public-private partnership to defend the nation's infrastructures.[18] The Plan does not quite meet the objectives delineated in PDD-63. The title's mention of "An Invitation to a Dialogue" relates to the continuing need for participation from the private sector. In the National Coordinator's opening message, he states that "the Plan, at this stage, does not lay out in great detail what will be done to secure and defend private sector networks, but suggests a common framework for action." He also states that "We will follow up our plan for cyber defense with a second plan focusing on how Government can work with the Nation's infrastructure sectors."[19]

The National Coordinator's message mentions goals set by the President. These goals are significantly different than those promulgated in PDD-63. In PDD-63 the goals were to significantly increase security to government systems by the year 2000 and to achieve a reliable, interconnected, and secure information system infrastructure by the year 2003. The new direction is to have "a Plan for defending our cyberspace be initially in effect by December 2000 and be fully operational by May 2003."[20] Obviously the ambitious goals of PDD-63 will not be met. Having a fully operational plan in effect is significantly different than PDD-63's requirement for a reliable, interconnected, and secure information system infrastructure.

The Plan is designed around three broad objectives and proposes 10 programs to achieve those objectives. The objectives are; (1) to prepare and prevent a significant and successful attack on our critical infrastructures, and be able to remain effective in face of such attacks, (2) detect and respond to an attack in a timely manner to contain the attack, recover and reconstitute, and (3) build strong foundations as a nation to enable the ability to prepare, prevent, detect and respond to attacks on our critical information networks. Objectives one and two encompass capabilities required for an effective computer network defense. Objective three enables objectives one and two by providing the trained experts, organizations and laws required.[21]

The 10 programs proposed by the plan are specifically designed to support the objectives. These programs are:

- Identify critical infrastructure assets and shared interdependencies and address vulnerabilities.

- Detect attacks and unauthorized intrusions.

- Develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with law.

- Share attack warning and information in a timely manner.

- Create capabilities for responses, reconstitution, and recovery.

- Enhance research and development in support of programs one through five.

- Train and employ adequate numbers of information security specialists.

- Conduct outreach to make Americans aware of the need for improved cyber-security.

- Adopt legislation and appropriations in support of programs one through eight.

- In every step and component of the Plan, ensure the full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data.

Programs one through nine flow directly from the direction provided in PDD-63. However, the programs do have a couple very interesting changes. The first major change is the inclusion of the need to fully protect American citizens' civil liberties, rights to privacy, and rights to the protection of proprietary data. This addition goes to the core of our national values. Program 10 may be included to appease private sector and individual citizen concerns. Individual's concerns stem from the fear that the federal government will become "Big Brother" as in George Orwell's book 1984. The private sector is very concerned about proprietary data and has been

reluctant to participate in the government's partnering efforts. Barrett writes that security incident reports are rarely passed "on to a federal agency such as the NIPC because of fear the data could be made public via a bureaucratic blunder, or would surface via a Freedom of Information Act (FOIA) request."[22]

The second major change, between the Plan and direction from PDD-63, is the deletion of international cooperation. The Plan focuses on domestic infrastructure protection and has no provisions for expanding cooperation outside the United States. This omission may be due to the fact that full cooperation within the United States has not been achieved. We must first get our efforts coordinated within the nation before we can venture outside the nation. A second explanation stems from the increased difficulty in protecting citizens' privacy rights in an international forum.

The Plan appears to be a pause in the trip down the road to a comprehensive national policy and plan on computer network defense. Although the plan details the federal efforts to shore-up its systems, it does not include details on how to fix the national vulnerabilities. In fact, it appears to take a step backwards for fear of infringing on the rights of the American people. In President Clinton's message, in the opening pages of the plan, he defines the role of the Federal Government as including "research and development efforts in the field of computer security, educating a corps of young computer scientists to help defend our federal cyber systems, and assisting in the private sector as it creates defensive measures for its information technologies."[23] This statement has the government protecting the federal computer systems while abandoning its role to protect the nation against attack, leaving the private sector to its own initiative. It creates a "federal" plan, rather than a "national" plan. This tactic is extremely dangerous. The federal government must ensure the protection of both the federal and private infrastructures, particularly since much of the critical infrastructure is in the private sector. The federal government cannot abandon portions of the national infrastructure simply because it is not under federal control. The problem with abandoning the private sector is compounded by the fact that the federal systems are heavily dependent on the private sector's systems. Should the private sector's systems fall to attack, the federal systems will be severely degraded.

In conjunction with the release of the Plan, the White House also announced that the President had developed and funded new initiatives to defend the nation's computer systems from cyber attack.[24] These initiatives are directly supportive of the programs outlined in the Plan. President Clinton's initiatives to protect the federal government's computer systems, as stated in a White House press release, included:

- Working to Recruit, Train and Retain Federal IT Experts.

• Conducting federal agency vulnerability analyses and developing agency critical infrastructure protection (CIP) plans.

• Designing a Federal Intrusion Detection Network (FIDNET). To protect vital systems in Federal civilian agencies, we are providing funding for development of a cyber "burglar alarm" which alerts the federal government to cyber attacks, provides recommended defenses, establishes information security readiness levels, and ensures the rapid implementation of system "patches" for known software defects.

• Piloting Public Key Infrastructure (PKI) Models. The Clinton Administration funded seven PKI pilot programs at different federal agencies in FY2001.

• Developing Federal Research and Development (R&D) Efforts.

• Building the Public-Private Partnership. The President committed to building partnerships with the private sector to protect our computer networks through the following initiatives:

- Institute for Information Infrastructure Protection. Building on a Science Advisory Panel, we are proposing to create an Information Infrastructure Institute which would combine federal and private sector energies to fill the gaps in critical infrastructure R&D that are not now being meet in the private sector or the Department of Defense. It would also provide demonstration and development support in key areas like benchmarks and standards, and curriculum development.

- Partnership for Critical Infrastructure Security. This alliance of more than ninety Fortune 500 companies is spearheaded by Secretary Daley and had a successful kickoff in New York on December 8th. We will build on this partnership to provide public education and cooperation with the private sector on a wide variety of information security issues

- Information Sharing and Analysis Centers (ISACs). Two of the proposed six private sector computer security centers have been

established (banking and finance and telecommunications). We are working with the other four sectors to get their proposed ISACs operational in 2000.

- National Infrastructure Assurance Council. The President signed an Executive Order creating this advisory Council, last year. Its members are now being recruited from senior ranks of the IT industry, key sectors of the corporate economy, and academia.[25]

The "National Plan for Information Security Protection" falls short of the mark set for it by PDD-63. The Plan focuses on the federal government almost to the point of excluding the private sector and state and local government. The vulnerability analysis called for under the Plan limits its scope to the federal government, it does not extend to each sector of the economy as called for by PDD-63. The Plan does not call for international cooperation as required by PDD-63. The Plan softens the goals set by PDD-63 and includes direction to ensure that actions taken under the Plan are consistent with law and civil liberties of citizens. The need for a national plan was recognized in PDD-63, but the plan that was published fails to meet the requirements set.

Simply increasing public awareness, as called for by the Plan, is not enough to build an effective computer network defense. The federal government must take a more proactive role to move the nation forward. Awareness does not guarantee action. The government must provide direction and incentives to encourage progress. When efforts in the public and private sectors do not move toward increasing computer network defense, the government must hold the responsible parties accountable and take punitive action.

A critical shortfall in the Plan is the lack of a new organizational structure with a clear, enforceable chain of command. The Plan restates the structure that was established under PDD-63 and the need to coordinate among offices in different departments and agencies.

The good points of the plan must be capitalized on to move the nation toward better computer network defense. The first two objectives of the plan are on the mark for what the entire nation needs to be able to do. The entire nation must be able to remain effective in the face of computer network attacks. This requires the ability to detect, contain, recover, and reconstitute in a timely manner. Recognizing these basic needs is a first step, developing a process to ensure that this capability is resident in all areas of the nation is the second step. The plan does not provide for this second step.

One of the initiatives associated with the Plan came under attack shortly after the January 7, 2000 announcement. The FIDNET initiative was to be administered by the General Services

Administration to provide the federal government with automated intrusion detection. Privacy advocates saw this effort as a monitoring system that could violate privacy laws.[26] This resulted in the canceling of the FIDNET initiative. In place of FIDNET, the General Services Administration has established the Federal Computer Incident Response Center (FedCIRC) which is a central coordination facility that "deals with computer security issues affecting civilian agencies and departments of the federal government."[27]

NATIONAL SECURITY STRATEGY

Computer network defense is of such a critical nature to the nation that it was included as part of the National Security Strategy (NSS). The current NSS was published by President Clinton in December 2000 and entitled A National Security Strategy for a Global Age. This document contains the "first-ever national strategy for cybersecurity."[28] The national objective of the NSS for CND is critical infrastructure protection. The NSS acknowledges that a "sophisticated information technology infrastructure fuels America's economy and national security." And that "These infrastructures are highly interconnected, both physically and by the manner in which they rely upon information technology and the national information infrastructure." The NSS recognizes that hostile hacker attacks and cyber conflict is ongoing and that "We must understand the vulnerabilities and interdependencies of our infrastructure, accept that such attacks know no international boundaries, and work to mitigate potential problem."[29]

REPORT OF THE PRESIDENT ON THE STATUS OF FEDERAL CRITICAL INFRASTRUCTURE PROTECTION ACTIVITIES

In January 2001, the president provided a congressionally requested report on the status of federal government and industry programs on cybersecurity. The "Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities" stated:

> The potential problems are even more significant than first thought. More of the American economy has become dependent on 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.[30]

The report details the organizational structures that were established by PDD-63 and additional organizations that have been established within the federal government. These additions to the cybersecurity bureaucracy include:

> The Cyber Incident Steering Group (CISG) and Cyber Incident Working Group (CIWG). These are 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 Joint Telecommunications Resources Board (JTRB). The 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 Security Telecommunications and Information Systems Security Committee (NSTISSC). The NSTISSC provides a forum for the discussion of policy issues and to provide operational guidance for the protection of national security systems.
>
> The National Information Assurance Partnership (NIAP). The NIAP is an initiative designed to meet the security-testing needs of both information technology producers and users. This effort is a collaboration of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).
>
> The Federal Cyber Services (FCS). The FCS is a training and education initiative designed to ensure an adequate supply of highly skilled federal information system security specialists.[31]

The president's report on the Status of Federal Critical Infrastructure Protection Activities described a cybersecurity problem that had not been solved. The report points out that not only is the nation more vulnerable, but that the threat has increased. Obviously, the incremental actions taken by the Clinton administration between July 1996 and January 2000 have not effectively addressed the problem. In the report, recognizing more action is needed, President Clinton announces the creation of additional organizations within the federal government. This was yet another step in addressing the problem with more bureaucracy.

IMPACT OF SEPTEMBER 11, 2001

The terrorist attacks of September 11, 2001 graphically demonstrated the nation's vulnerability to terrorist attack. The rude awakening that took place that day opened the eyes of the leadership to the nation's vulnerabilities and provided the impetus for action. On 16 October 2001, President George W. Bush signed Executive Order 13231, "Critical Infrastructure Protection in the Information Age." The Executive Order created the Office of Homeland Security, the position of Special Advisor to the President for Cyberspace Security and new policy on infrastructure protection.[32]

Executive Order 13231 stated the United States' policy on critical infrastructure protection as "to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, the economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[33] The new policy focuses the computer infrastructure protection effort on critical areas, similar to efforts under the Clinton administration, and not the nation as a whole. The policy should have been expanded to include all computer infrastructures, both critical and non-critical. All computer infrastructures are vital at some level. The Executive Order does expand the list of sectors that are considered critical. The Executive Order adds manufacturing as being supported by critical infrastructure and mentions corporate and academic organizations as critical infrastructure supporting programs.[34]

In addition to creating the Cyberspace Security Advisor, the Executive Order created the President's Critical Infrastructure Protection Board. The Board's membership includes the president's cabinet and advisors, most of the heads of federal government agencies, the Director of the CIAO, the Director of the NIPC, Chairman of the Joint Chiefs of Staff, and others. The Board's responsibilities include:

- Outreach to the Private Sector and State and Local Governments
- Information Sharing
- Incident Coordination and Crisis Response
- Recruitment, Retention, and Training Executive Branch Security Professionals
- Research and Development

- Law Enforcement Coordination with National Security Components
- International Information Infrastructure Protection
- Legislation
- Coordination with Office of Homeland Security[35]

With the exception of legislation and coordination with the new Office of Homeland Security, these responsibilities cover areas already addressed in the National Plan for Information Protection. President Bush's Executive Order is not really breaking new ground, but is more comprehensive in areas that concern the federal government.

As with all the previous efforts the federal government has made to address the problem of infrastructure security, this effort creates more bureaucracy. This Executive Order creates a multitude of "standing committees". Additionally, the Executive Order allows the Board to establish even more standing and ad hoc committees of its own. The following are standing committees required by the Executive Order.

- Private Sector and State and Local Government Outreach
- Executive Branch Information Systems Security
- National Security Systems
- Incident Response Coordination
- Research and Development
- National Security and Emergency Preparedness Communications
- Physical Security
- Infrastructure Interdependencies
- International Affairs
- Financial and Banking Infrastructure[36]

Two of these standing committees are existing committees that have been renamed and given additional duties. The other eight committees were created "out of hide" as additional duties of current federal government departments and agencies. This action does not create larger government, but it does create more bureaucracy and it does create additional work for an already overworked system.

This Executive Order also "establishes" the National Infrastructure Advisory Council and discretely revokes Executive Order 13130 of July 14, 1999. Of particular interest in this action is the fact that the wording to establish the National Infrastructure Advisory Council in President Bush's Executive Order is nearly identical to the wording in President Clinton's Executive Order 13130 establishing the National Infrastructure Assurance Council.[37]

The events of September 11, 2001 prompted the federal government to take action and shore-up defenses for the nation's vulnerabilities. Cybersecurity was one of the nation's obvious vulnerabilities. The executive order signed by President Bush would appear to be a move in the right direction if it was viewed as a single action. Examining the executive order with knowledge of previous efforts taken by the federal government reveals that the executive order, for the most part, restates what has already been done and what is already known. If anything, the order complicates the entire cyber security effort by renaming existing efforts and creating more bureaucracy.

The creation of Special Advisor to the President for Cyberspace Security appears to be a good idea at face value, however, like the rest of the Executive Order, it fails upon further examination. First, the person appointed to the new position is Richard A. Clarke, the same person who was filling the job of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism under Clinton. He was already working the infrastructure protection problem. The appointment of Wayne A. Downing as National Director and Deputy National Security Advisor for Combating Terrorism simply relieved Clarke of his counter-terrorism duties.[38] Second, the power of the newly created cyberspace security position is limited. As the Chair of the President's Critical Infrastructure Protection Board, his duty is limited to coordinating the efforts of the board within the federal government. He has no direct control over budgets, regulations, or enforcement. With the exception of his "appropriately sized staff within the White House Office," the Cyberspace Security Advisor does not have any direct authority to effect broad-based change.[39]

GAO REPORTS

In response to congressional committee meetings on critical infrastructure protection, there have been a number of GOA reports relating to the issue. Of particular interest are two reports released in September 2001. These reports are entitled "Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer Based Attacks" and "Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities." Both of these reports describe numerous weaknesses in federal computer systems that put critical operations at risk and state that the federal government efforts are not keeping pace with the growing threats. These GOA reports see the solution to the problem as strict compliance to existing computer security practices, increased analytical and information sharing capability in the NIPC and a national plan with a fully defined strategy, clearly defined roles and responsibilities with performance measures and accountability.[40]

RECOMMENDATIONS

Clearly the efforts made by the federal government thus far have not achieved the level of computer network defense the nation requires. The federal government must make a number of changes to ensure the establishment of an effective computer network defense. Foremost in these changes is an increased commitment from the leadership. Without this commitment, the substantial changes in government organization, laws, regulations, incentive systems, accountability and sanctions cannot be enacted. The leadership must fully endorse a change in government policy toward computer network defense and create an agency for computer infrastructure assurance and protection to carry out that policy. The new policy should call for an increased level of federal government involvement and empower the new Computer Infrastructure Assurance and Protection Agency. The need for computer network defense is essential to the security and economic well being of the nation and must be addressed as such.

CHANGE THE FEDERAL GOVERNMENT'S POLICY

The federal government's policy on computer network defense must change. The federal government must take a more active role in shaping the efforts in the private sector as well as the current effort of increasing the defensive posture of the federal government. The national policy should incorporate the following ideas:

> Every citizen of the United States of America should feel safe. Safe from attack, both physical and computer based. Every citizen should be confident that their government is doing everything in its power to ensure that safety. The

> federal government must be capable of defending the nation's computer infrastructure as well as it can defend its shores. To accomplish this, the nation needs a focused effort to establish a comprehensive defense and the capability of identifying an attack, isolating the attack, minimizing damage, and rapidly recovering should a successful computer infrastructure attack occur. The focused effort must include the institution and enforcement of protection policy, plans, and programs. To carry out the task of this computer infrastructure assurance and protection effort the nation must establish a Computer Infrastructure Assurance and Protection Agency (CIAPA). This agency must be empowered to institute regulations and incentive systems, and enforce accountability and sanctions. In conjunction with legislation to form the agency, there must be an amendment made to the Freedom of Information Act (FOIA). The amendment is needed to facilitate the agency's work with the private sector in establishing private-public partnerships. Specifically, the amendment would protect cyber security information being provided by the private sector from disclosure under the FOIA.

The new policy would form the foundation from which government would step out to take a greater role in protecting the nation's computer infrastructure from cyber attack. Although the military has the duty to defend the nation's shores from attack, cyber attacks may originate from and pass through any location in the world, including the United States. The Posse Comitatus Act severely restricts military activities on U.S. soil and against U.S. citizens. For this reason the federal government should empower the Computer Infrastructure Assurance and Protection Agency (CIAPA) with the duty of ensuring the nation is properly defended against computer based attacks. The CIAPA would be the sole agency with overarching CND responsibility. The military, and all other federal departments and agencies, would be responsible to the CIAPA for ensuring compliance with computer infrastructure assurance and protection legislation and regulations within their organization. The military should maintain the capability to conduct computer based attacks in case those capabilities be required by the President of the United States as Commander in Chief.

COMPUTER INFRASTRUCTURE ASSURANCE AND PROTECTION AGENCY

As we enter the information age, with networked computers and networked vulnerabilities, the CIAPA needs to be created to protect the nation from information age vulnerabilities. The

new agency would be able to make a concerted, national effort at computer network defense. The agency would be able to address the shortfalls the government has experienced to date. The new agency would be able to eliminate stove-pipes and coordinate the efforts between the public and private sectors, it would provide the resources needed to improve the security of computer infrastructures throughout the nation, it would be able to influence legislation, budgets, and coordination efforts with other nations, it would be able to regulate the nation's computer infrastructure and enforce those regulations, it would be able to coordinate vulnerability and intelligence efforts to fuse the information into a picture that would provide better situational awareness. A new agency would be able to provide the increased level of computer infrastructure assurance and protection the nation requires.

Creating a new department or agency within the federal government may seem a bit unusual today, but our history shows that many new problems faced by the federal government have been solved by the creation of new departments or agencies. When the nation was faced with the new agricultural age in 1861, the federal government created the Department of Agriculture. In the Industrial Age the government created the Department of Commerce. In 1958, as we entered the jet age of aviation transport, the Federal Aviation Act created the Federal Aviation Agency.[41] The legislation gave the Agency the power to regulate the aviation industry. As the country entered the "space age" the government created the National Aeronautics and Space Administration. As the nation enters the information age, the federal government must create an agency charged with the regulation and oversight of information technologies. Given that the new information technologies have created significant nation wide vulnerabilities, this new agency must also be responsible for tackling the vulnerabilities.[42]

The CIAPA can be initially formed by bringing together the cyber security efforts that are currently spread throughout the federal government, reorganizing the resources, and forming a cohesive, focused effort. The stove-piped efforts that need to be brought into the new agency include; the cybersecurity advisor to the president and his staff, the NIPC, the CIAO, the ISACS, Lead Agency Sector Liaison Officials, the Institute for Information Infrastructure Protection, and all cybersecurity related programs. The myriad councils, groups, and committees formed by PDD-63, Executive Orders, and the National Plan can be disbanded. If necessary, new coordination groups can be reformed under the CIAPA. Consolidating the numerous efforts and the associated resources into one agency will reduce the budgetary impact of creating the new organization. Bringing the disparate efforts together under a single leadership will facilitate a symbiotic relationship through increased coordination. This relationship will also ease the budgetary burden of the new agency. Despite these economies, there will be a need for

additional funding. A study should be conducted to determine what funds should be transferred with existing organizations and the specific level of additional funding required. Cross walking the current funding of organizations and efforts to the CIAPA should be sufficient to create the new agency, however, an increase in funding will be required. The largest portion of these funds will be needed to support an incentive system.

In creating the CIAPA, the agency should be chartered to carry out the national policy for computer infrastructure protection. The chartering legislation should specify the following duties and responsibilities for the agency:

- Execute executive level authority to establish and enforce computer infrastructure assurance and protection regulations.
- Establish and maintain a partnership between the federal government and private sector computer infrastructure owners and operators. Ensure the continuous sharing of information relating to computer infrastructure threats, vulnerabilities, and interdependencies.
- Ensure computer network infrastructure owners and operators and all levels of government accomplish their infrastructure protection roles.
- Establish national computer infrastructure assurance and protection policy, plans, and programs.
- Elevate national awareness of computer security standards, computer based threats, vulnerabilities, and interdependencies.
- Establish information security management standards, incentives, monitoring programs and disciplinary procedures.
- Champion legislation to increase the effectiveness of national computer network assurance and protection efforts.
- Fund computer network assurance and protection research, development, testing and fielding.
- Conduct recurring vulnerability analyses for each sector of the economy and government that might be a target of computer based attack intended to significantly damage the United States. The vulnerability analysis should include the identification of critical dependencies. (Critical dependencies are supporting functions from other areas of the economy or government that are critical to continued operations). Vulnerabilities discovered should be identified and addressed in a remediation plan that would establish timelines for implementation, responsibilities and funding.

• Establish a national center to monitor, collate and analyze information on computer based attacks. The center should issue alerts, warnings, and corrective actions to combat attacks on computer infrastructures. The center should be capable of identifying an attack, isolating the attack and minimizing damage. Information on confirmed attacks originating from outside the United States should be forwarded to the National Security Advisor for action.

• Establish public and private sector procedures to rapidly recover from a successful computer infrastructure attack. Critical infrastructures should be capable of reconstituting minimum required capabilities nearly immediately.

• Establish an intelligence organization dedicated to the collection and analysis of threats to our national computer infrastructure, to include, but not be limited to, threats from foreign nations, organized crime, terrorist and hackers.

• Establish a concerted effort of international cooperation to combat computer based threats.

• Establish budgetary priorities and control budgetary funding of federal computer infrastructure assurance and protection efforts.

• Administer programs to ensure adequate numbers of qualified information security specialists to support both the private and public sector. Programs should include funding of education through grants, loans and other incentives. Establish a certification program to ensure security specialists in the private and public sectors are qualified to accomplish their duties.

• Ensure the full protection of American citizens' civil liberties and their rights to privacy.

• Develop and maintain a comprehensive National Computer Infrastructure Assurance and Protection Plan.

The CIAPA should be empowered to make the changes necessary to assure and protect the nation's computer infrastructure. The Agency should be able to effect change in the public sector through a combination of incentives and sanctions. Change in the private sector should be enabled through increased cooperation and a combination of regulations and economic incentives. The Agency should work closely with the Department of State to establish procedures with other nations to track cyber attacks to their source and to bring the guilty parties to justice.

The recommendation to form the CIAPA can be adopted through the creation of an independent agency, but it could also be adopted as an effort that supports homeland security. Adopting the CIAPA as part of the homeland security effort should be conditional on the creation

of a department for homeland security. If the Office of Homeland Security were expanded to a department of the federal government, the CIAPA should be an agency within that department. The CIAPA would be the focus of the department's cybersecurity efforts. Without the formation of a Department for Homeland Security, the agency should be independent. The Office of Homeland Security does not have the budgetary and enforcement powers the CIAPA requires to accomplish its mission. Placing the Agency within this office will wrap it with a layer of weak bureaucracy that will hamper its ability to accomplish its mission. Having the appropriate level of power throughout the organization's chain of command is critical to mission accomplishment.

RECOMMENDED CIAPA ORGANIZATION

The figures below describe the proposed organization needed to carry out the duties and responsibilities of the CIAPA. Figure 1, below, shows the basic organizational structure. The Agency should have four key departments. The Plans and Policy department would be responsible for major administrative interfaces with key areas of the federal government such as planning the budget, developing legislation and international coordination. The Operations department would be where the bulk of the work gets accomplished through a national center and a number of regional centers. The Public Support department would be critical to ensuring public awareness and an adequate supply of qualified computer security experts. The Future Technologies department would be responsible for ensuring the agency stays current on computer security technology while developing the tools needed to meet future security

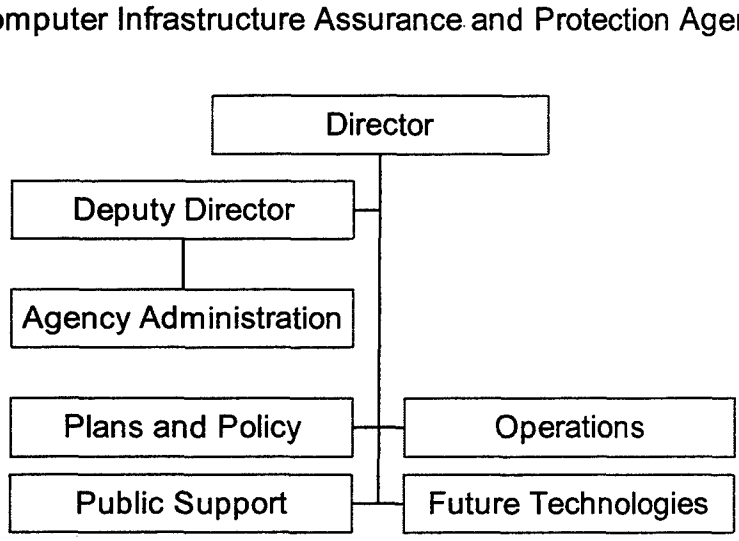

FIGURE 1 - COMPUTER INFRASTRUCTURE ASSURANCE AND PROTECTION AGENCY ORGANIZATION

requirements. These departments would work together under a single, unifying, leadership to establish a comprehensive computer infrastructure assurance and protection program.

The CIAPA Director should be empowered to institute regulations, create and administer incentive systems, and enforce accountability through sanctions. Having these powers is essential to establishing an effective CND for the nation. The power to institute regulations is at the core of improving CND. The regulations should be aimed at improving CND at every level, from household computers to government networks to critical infrastructures. The ability to create and administer incentive systems should assist in gaining compliance with regulations. Should incentives fail, the director should be able to hold organizations and individuals accountable. The Director's authority to enforce rules and regulations should be delegated to the Center Director and Sector Coordinators for execution.

Figure 2, below, depicts the proposed Plans and Policy department. The department should have three divisions. The Plans and Budgeting division would develop future plans for the Agency and construct the budget required to support those plans. The Policy division would be responsible for establishing computer security standards, developing regulations and championing legislation. The International Coordination division should work closely with the Department of State and other agencies to coordinate an international effort in combating

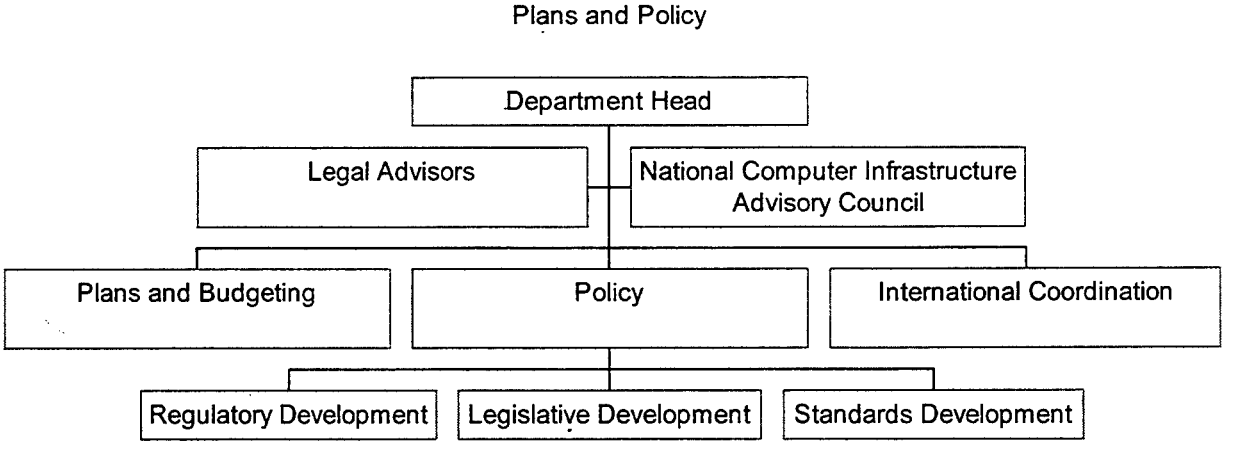

FIGURE 2- PLANS AND POLICIES DEPARTMENT

hackers and cyber terrorists. The department should be supported by a legal staff to ensure all actions taken conform with law and do not violate the rights of citizens. The department's National Computer Infrastructure Advisory Council would advise the department head on policy, plans and budgeting decisions. The membership of the council should be key members of Congress, federal departments and agencies, state and local government, and the private

sector. The purpose of the council would be to ensure the departments' efforts will be viable and executable from a political, social, economic, cultural and organizational stand point.

Figure 3, below, depicts the proposed Operations department. The Operations department should have two divisions responsible for areas of coverage. The overarching national effort should be covered by the National Center for Computer Infrastructure Assurance and Protection. To bring the effort to the nation requires a second division which should administer a number of Regional Centers for Computer Infrastructure Assurance and Protection through out the country. Operationally, the branches in the regional centers should report to their respective branches in the national center.

Operations

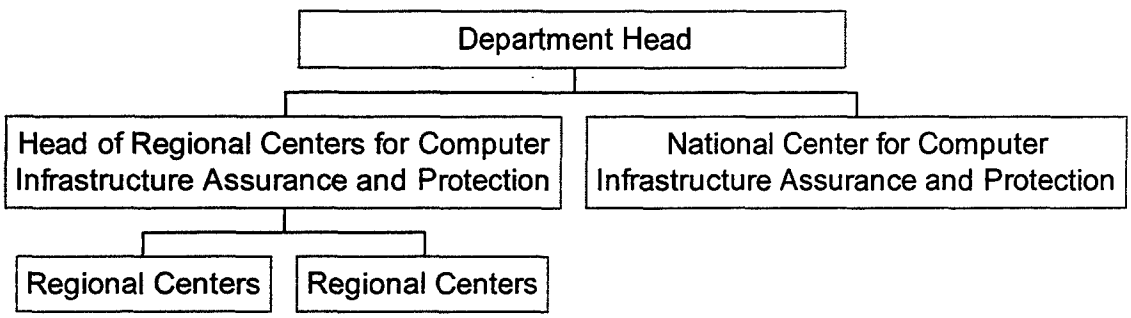

FIGURE 3 - OPERATIONS DEPARTMENT

Realizing that many parts of the nation have specialized computer infrastructure requirements and different ways of doing business, both the regional and nation centers should spread their efforts over "sectors" of responsibility. Splitting the effort into sectors will allow the federal employees working each sector to be experts in that area. The sectors are very similar to the critical infrastructure sectors established by PDD-63, however, the CIAPA's sectors are designed to provide comprehensive coverage. Figure 4, below, depicts the proposed sectors. The government sector should be responsible for state and local government at the regional centers and the federal government at the national center. The military should be separated out from the federal government at the national center due to the comprehensive effort it has with Joint Task Force – Computer Network Operations (JTF-CNO). The home users sector should be created to work assurance and protection issues for the general public.

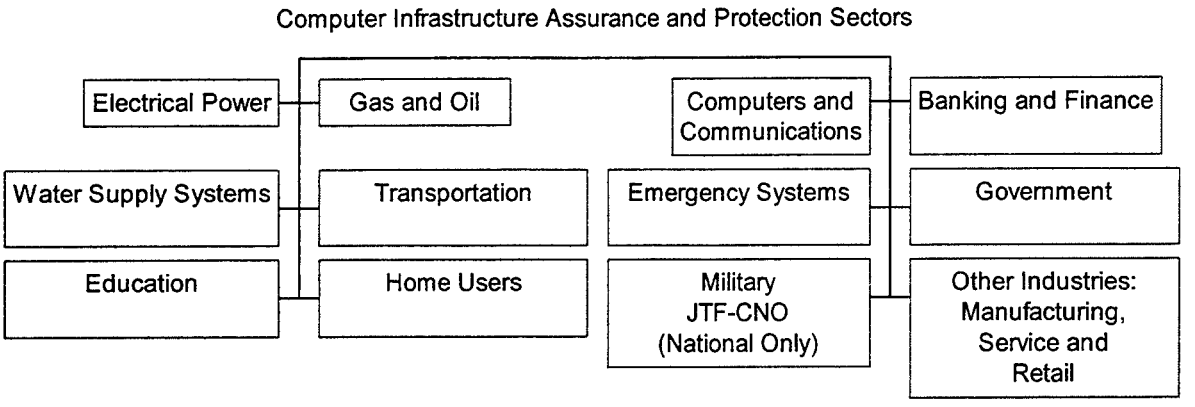

FIGURE 4 - COMPUTER INFRASTRUCTURE ASSURANCE SECTORS

The proposed organization of the Regional Centers is described below in figure 5. Every regional center should have its own operations center to provide operational reports to the national center, Emergency Response Teams to the region, and Law Enforcement. The regional centers should have an Information Sharing branch that would be responsible for information sharing in each of the sectors. Each of the sectors should have Assistance Teams available to provide help with ensuring computer security. The Assistance Teams should also verify regulation compliance for incentive qualification.

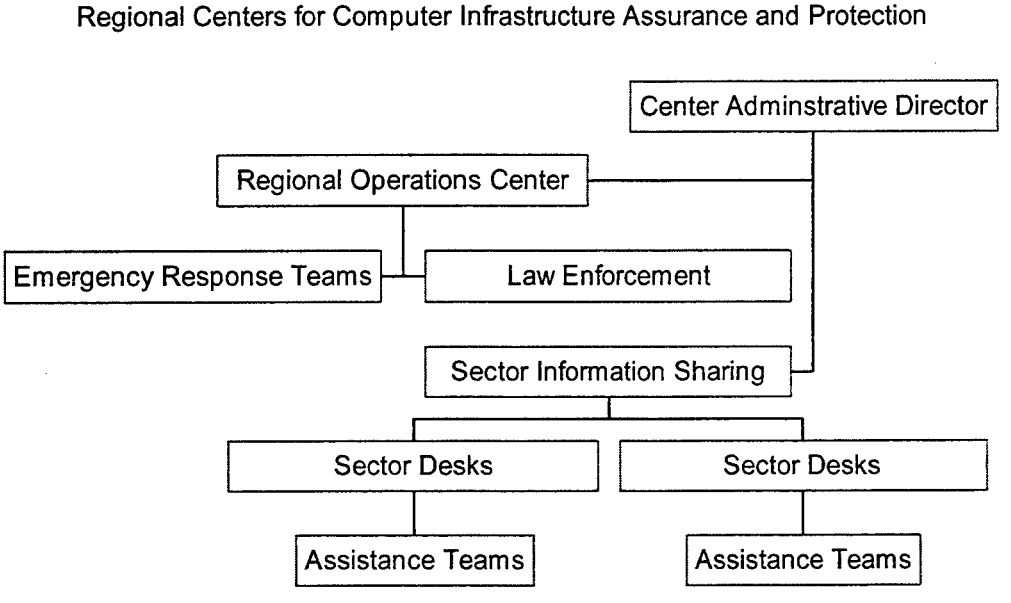

FIGURE 5 - REGIONAL CENTERS

Figure 6, below, describes the proposed organization of the National Center for Computer Infrastructure Assurance and Protection. The national center should coordinate efforts in all the sectors through a sector coordinator who would be responsible for all the sectors. Each sector

office should work with each of the respective regional field offices and, if applicable, the ISAC for that sector. The National Operations Center should be the hub of real time infrastructure assurance and protection. The center should operate the National Computer Infrastructure Simulation and Analysis Center, intelligence and law enforcement branches, and work with all the regional operations centers. The Center Director and Sector Coordinators should be delegated authority to enforce rules and regulations.

National Center for Computer Infrastructure Assurance and Protection

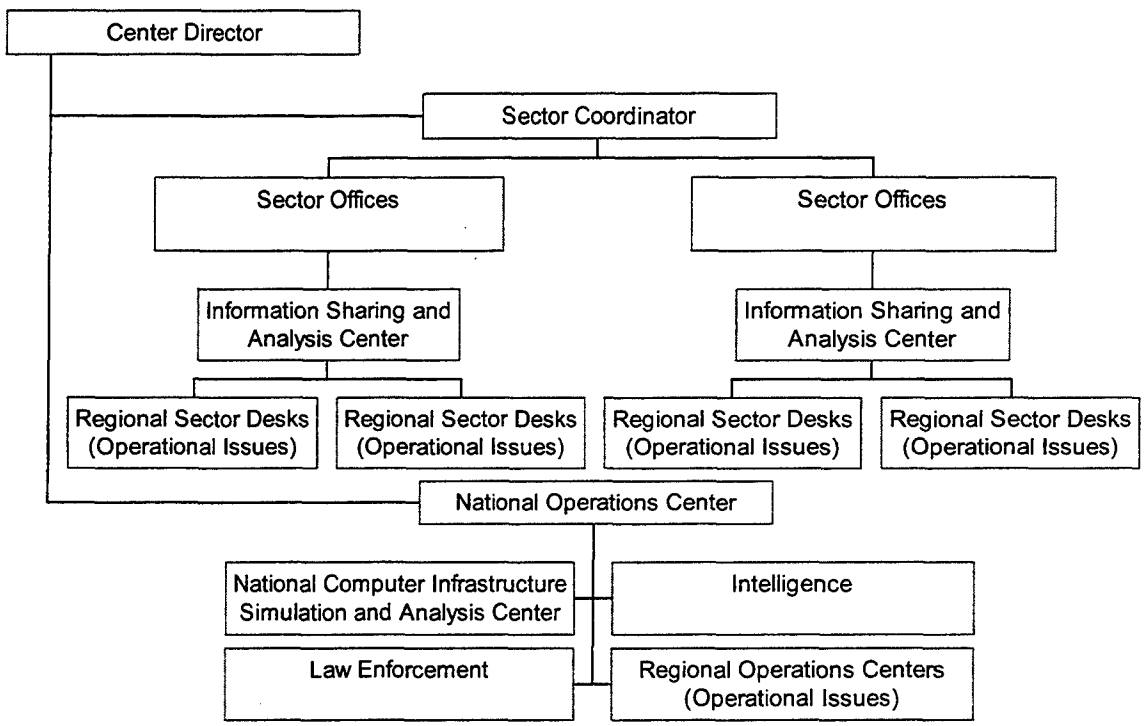

FIGURE 6 - NATION CENTER FOR COMPUTER INFRASTRUCTURE ASSURANCE AND PROTECTION

The proposed Public Support department, depicted in figure 7 below, should administer the bulk of the support to the general public. The Public Awareness branch should be the means to inform the public of how critically important computer infrastructure protection is. This branch should embark on a significant public information campaign to energize the population to action. This branch should also develop processes and procedures to distribute information and other required items to the home computer user. The Education branch should administer programs aimed at creating a work force of computer security experts that is large enough to answer the nation's call to computer network defense. The Professional Certification branch should institute certification procedures to ensure the computer security work force is qualified.

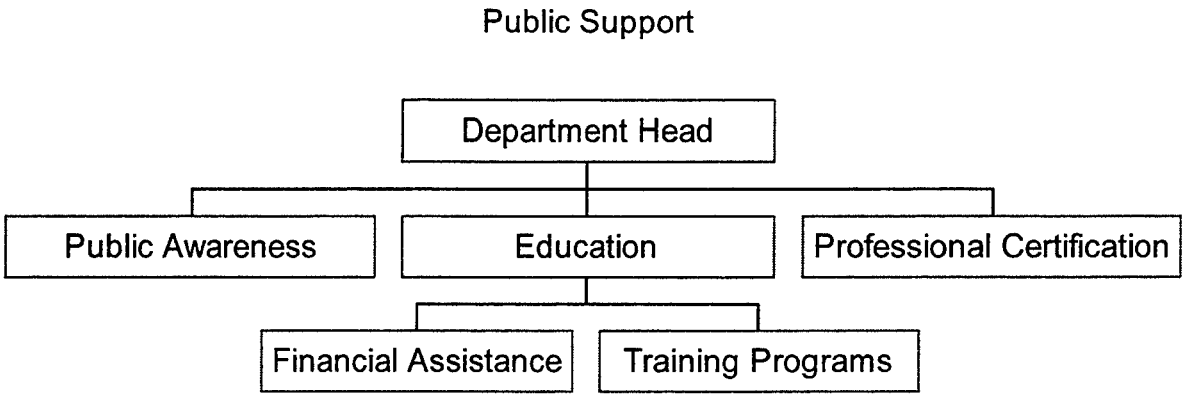

FIGURE 7 - PUBLIC SUPPORT DEPARTMENT

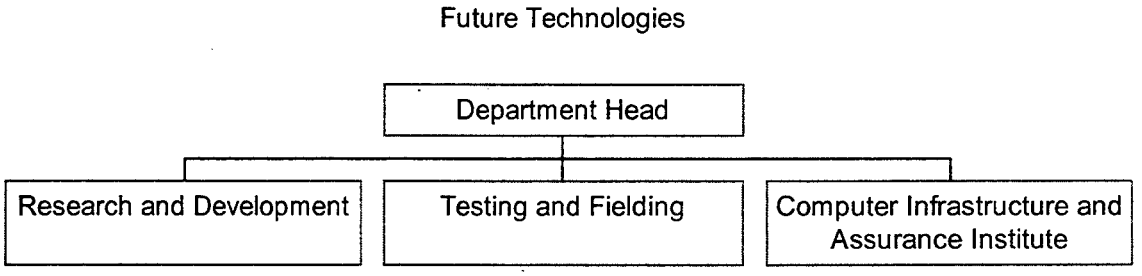

FIGURE 8 - FUTURE TECHNOLOGIES DEPARTMENT

The proposed Future Technologies department, depicted in figure 8 above, should be responsible for federal government efforts in research, development, testing and fielding. This department would stay on the cutting edge of modern computer security technology administering the Computer Infrastructure and Assurance Institute.

CONCLUSIONS

Our nation's increased reliance on computers and computer networks has increased its vulnerability to computer network attack. Despite the federal government's significant effort in infrastructure protection, the nation remains extremely vulnerable. To achieve the level of assurance and protection the nation needs, necessitates a major change in policy and the creation of a new agency. The new policy, outlining a more aggressive role for the federal government, must have the support of the nation's leadership to be successful. The policy must endorse the formation of an agency specifically chartered for computer infrastructure assurance and protection. The new agency is essential to effectively orchestrate the nation's computer defense efforts. These efforts should not be limited to critical infrastructure, but should strive to protect the entire nation's computer infrastructure.

Care must be taken to ensure the new agency is properly resourced and empowered. Without adequate funding and enforcement powers, the agency will be limited in its ability accomplish its mission and unable to attain the level of computer assurance and protection required.

Today's Information Age requires the protection of the nation's computers and computer networks as a critical component of national security. Without comprehensive computer infrastructure assurance and protection, a concerted computer based attack could be catastrophic. It is the federal government's inherent responsibility to ensure the nation is secure and protected against such a catastrophe. A federal government policy that aggressively sets high goals in the protection the nation's computers and a new federal agency designated, empowered and resourced to protect the nation's computer infrastructures is what this nation needs to ensure computer network defense for the United States of America.

WORD COUNT = 9300

ENDNOTES

[1] U.S. Congress, House, Committee on the Judiciary, *The Constitution of the United States of America, as Amended,* 100th Congress, 1st session, 1987, H Doc 100-94.

[2] William J. Clinton, "Executive Order 13010," (Washington, D.C.: The White House, July 15, 1996), 3.

[3] Ibid, 1.

[4] President's Commission on Critical Infrastructure Protection, Critical Foundations – Protecting America's Infrastructures, October 1997; available from <http://www.terrorism.com/homeland/PCCIPreport.pdf>; Internet, accessed 20 January 2002.

[5] Ibid.

[6] Office of the Press Secretary, Protecting America's Critical Infrastructure: PDD 63, (Washington, DC: The White House, 22 May 1998); available from <http://www.ciao.gov/CIAO_Document_Library/WhiteHouseFactSheet_PDD63.html>; Internet accessed 13 October 2001.

[7] Ibid.

[8] White Paper, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 1998; available from <http://www.ciao.gov/CIAO_Document_Library/paper598.htm>; Internet; accessed 13 October 2001.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Randy Barrett, "Trust Me! Government and Corporate Infighting Cripples Federal Cybersecurity Efforts," *Interactive Weekly* 8 No 32 (20 August 2001): 20.

[13] White Paper.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] William J. Clinton, "Executive Order 13130," (Washington, D.C.: The White House, July 14, 1999), 1-2.

[18] William J. Clinton, "President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century," (Washington, D.C.: The White House, 7 January 2000); available from <http//www.epic.org/security/CIP/WH_pr_1_7_00.html>; Internet; accessed 14 October 2001, 1.

[19] William J. Clinton, National Plan for Information Systems Protection Version 1.0 – An Invitation to a Dialogue (Washington, D.C.: The White House, December 2000), iv-v.

[20] Ibid, iv.

[21] Ibid, xi.

[22] Barrett, 19.

[23] Clinton, National Plan for Information Systems Protection Version 1.0 – An Invitation to a Dialogue, iii.

[24] Clinton, "President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century," 1.

[25] Ibid, 2.

[26] Keith Perine, "Senators, Privacy Advocates Spar Over FIDNet Plan," The Industry Standard, 1 February 2000, available from <http://www.thestandard.com/article/0,1902,9327,00.html>; Internet; accessed 29 January 2002.

[27] Barrett, 20.

[28] William J. Clinton, A National Security Strategy for a Global Age (Washington, D.C.: The White House, December 2000), iv.

[29]Ibid, 24.

[30] William Clinton, Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, (Washington, DC: The White House, January 2001), iv.

[31] Ibid, 6-7.

[32] George W. Bush, "Executive Order 13231," (Washington, D.C.: The White House, October 16, 2001), 5-6.

[33] Ibid, 1.

[34] Ibid.

[35] Ibid, 3-5.

[36] Ibid, 7-8.

[37] Ibid, 9-11 and Clinton, "Executive Order 13130," 1-3.

[38] Mike Allen and Eric Pianin, "White House Names Cyberspace Security Adviser," Washtech.com 10 October 2001; available from <http://www.washtech.com/news/regulation/13049-1.html>; Internet; accessed 14 October 2001.

[39] Bush, "Executive Order 13231", 6-7.

[40] Joel C. Willemssen, "Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer Based Attacks" and "Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities," (Washington, DC: United States General Accounting Office, September 2001).

[41] Federal Aviation Administration, "A Brief History of the Federal Aviation Administration and its Predecessor Agencies," available from <http://www.faa.gov/apa/history/briefhistory.htm>; Internet; accessed 25 February 2002.

[42] The remarks in this paragraph are based on those made by a speaker participating the Information Warfare elective lecture series.

BIBLIOGRAPHY

Allen, Mike and Eric Pianin. "White House Names Cyberspace Security Adviser." Washtech.com 10 October 2001. Available from <http://www.washtech.com/news/regulation/13049-1.html>. Internet. Accessed 14 October 2001.

Barrett, Randy. "Trust Me! Government and Corporate Infighting Cripples Federal Cybersecurity Efforts." Interactive Weekly 8 No 32 (20 August 2001): 18-21.

Borchgrave, Atnaud de, Frank J. Cilluffo, Sharon L. Cardash and Michele M. Ledgerwood. "Cyber Threats and Information Security, Meeting the 21st Century Challenge." Washington, D.C.: Center for Strategic and International Studies, December 2000.

Brock, Jr., Jack L.. "Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination." Washington, DC: United States General Accounting Office, July 2000.

Bush, George W. "Executive Order 13228." Washington, D.C.: The White House, 8 October 2001.

_____. "Executive Order 13231." Washington, D.C.: The White House, 16 October 2001.

Carter, Ashton, John Deutch and Philip Zelikow. "Catastrophic Terrorism, Tackling the New Danger." Foreign Affairs. 77 (November/December 1998).

Clinton, William J. "Executive Order 13010." Washington, D.C.: The White House, 15 July 1996.

_____. "Executive Order 13025." Washington, D.C.: The White House, 13 November 1996.

_____. "Executive Order 13130." Washington, D.C.: The White House, 14 July 1999.

_____. "President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century." Washington, D.C.: The White House, 7 January 2000. Available from <http//www.epic.org/security/CIP/WH_pr_1_7_00.html>. Internet. Accessed 14 October 2001.

_____. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December 2000.

_____. National Plan for Information Systems Protection Version 1.0 – An Invitation to a Dialogue. Washington, D.C.: The White House, December 2000.

_____. Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities. Washington, DC: The White House, January 2001.

Denning, Dorothy. "Cyberterrorism." Testimony before the Special Oversight Panel on Terrorism, 23 May 2000. Available from <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>. Internet. Accessed 13 October 2001.

Dick, Ron. "Welcome message from the Director of the National Infrastructure Protection Center." Available from <http://www.npic.gov/about/about.htm>. Internet. Accessed 13 October 2001.

Flournoy, Michele A. eds. QDR 2001, Strategy-Driven Choices for American Security. Washington D.C.: National Defense University Press, 2001.

Government Electronics and Information Technology Association (GEIA). "Information Assurance and Critical Infrastructure Protection – 'A Federal Perspective'." Arlington: Government Electronics and Information Technology Association, 2001.

Hammond, Matthew Carlton. "The Posse Comitatus Act: A Principle in Need of Renewal." Washington University Law Quarterly 75 No 2 (Summer 1997): 953-967.

Joint Chiefs of Staff. Joint Vision 2020. Washington D.C.: Joint Chiefs of Staff, June 2000.

_____. Joint Doctrine for Information Operations, Joint Pub 3-13. Washington D.C.: Joint Chiefs of Staff, 9 October 1998.

Kelly, Terrence. " An Organizational Framework for Homeland Defense." Parameters 21 (Autumn 2001): 105-116.

Lathrop, Charles and Mackenzie M. Eaglen. "The Commission on National Security/21st Century: A Hart-Rudman Commission Primer." National Security Watch. Arlington: Association of the United States Army, 6 April 2001. 1-6

MacMillan, Robert. "Washington Prepares Cyber-Security Plan." 9 May 2001. Available from <http://www.washtech.com/news/netarch/9674-1.html>. Internet. Accessed 13 October 2001.

McCullagh, DeClan and Ben Polen. "Fighting Evil Hackers With Bucks." 11 October 2001. Available from <http://www.wired.com/news/politics/0,1283,47479,00.html>. Internet. Accessed 13 October 2001.

Montgomery, Mark C. "Cyber Threats: Developing a National Security Strategy for Defending Our Cyberspace." Harvard University: Center for Information Policy Research, July 2001.

O'Harrow Jr., Robert. "Key U.S. Computer Systems Called Vulnerable to Attack." 27 September 2001. Available from <http://www.washtech.com/news/regulation/12739-1.html>. Internet. Accessed 13 October 2001.

O'Neil, Michael J. and James X. Dempsey. "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry." 10 February 2000. Available from <http://www.cdt.org/security/fidnet/oneildempseymemo.html>. Internet. Accessed 29 January 2002.

Perine, Keith. "Senators, Privacy Advocates Spar Over FIDNet Plan." The Industry Standard, 1 February 2000. Available from <http://www.thestandard.com/article/0,1902,9327,00.html>. Internet. Accessed 29 January 2002.

Peterson, Molly, M. "Public-private Partnership Called Key to Cybersecurity." Government Executive Magazine 12 March 2002. Available from <http://www.govexec.com/dailyfed/0302/031202td2.htm>; Internet. Accessed 13 March 2002.

Rumsfeld, Donald H. "Quadrennial Defense Review Report." Washington D.C.: Secretary of Defense, 30 September 2001.

Tritak, John S. "Critical Infrastructure Protection: Who's in Charge?" Statement to the Senate Committee on Governmental Affairs, 4 October 2001. Available from <http://www.ciao.gov/News/SenGovAffTritakTmony100401.html>. Internet. Accessed 13 October 2001.

U. S. President's Commission on Critical Infrastructure Protection, Critical Foundations – Protecting America's Infrastructures. October 1997. Available from <http://www.terrorism.com/homeland/PCCIPreport.pdf>. Internet. Accessed 20 January 2002.

U.S. Congress, House, Committee on the Judiciary, The Constitution of the United States of America, as Amended. 100th Congress, 1st session, 1987, H Doc 100-94.

U.S. Congress, USA PATRIOT ACT. 107th Congress, 1st session, 2001, H.R. 3162.

U.S. Federal Aviation Administration. "A Brief History of the Federal Aviation Administration and its Predecessor Agencies." Available from <http://www.faa.gov/apa/history/briefhistory.htm>. Internet. Accessed 25 February 2002.

U.S. Office of the Press Secretary, Protecting America's Critical Infrastructure: PDD 63. Washington, DC: The White House, 22 May 1998. Available from <http://www.ciao.gov/CIAO_Document_Library/WhiteHouseFactSheet_PDD63.html>. Internet. Accessed 13 October 2001.

Vaida, Bara. "White House Resurrects Plan to Track Computer Break-ins." Government Executive Magazine 26 November 2001. Available from <http://www.govexec.com/dailyfed/1101/112601td1.htm>; Internet. Accessed 29 January 2002.

Wakeman, Nick. "IT Infrastructure Is Key to Homeland Defense." 21 September 2001. Available from <http://www.washtech.com/news/govtit/12654-1.html>. Internet. Accessed 13 October 2001.

Weiss, Aaron. "When Terror Strikes, Who Should Respond?" Parameters 21 (Autumn 2001): 117-133.

White Paper, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." May 1998. Available from <http://www.ciao.gov/CIAO_Document_Library/paper598.htm>. Internet. Accessed 13 October 2001.

Willemssen, Joel C. "Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer Based Attacks." Washington, DC: United States General Accounting Office, September 2001.

_____. "Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities." Washington, DC: United States General Accounting Office, September 2001.

Williams, Krissah. "U.S. Seeks To Build Secure Online Network." 11 October 2001. Available from <http://www.washtech.com/news/govtit/13066-1.html>. Internet. Accessed 13 October 2001.