USAWC STRATEGY RESEARCH PROJECT

DEPARTMENT OF HOMELAND SECURITY POLICY FOR DEFENSE OF CYBERSPACE

by

Lieutenant Colonel Timothy M. O'Hara
United States Army

Colonel H. Gordon Thigpen III
Project Advisor

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

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
07-04-2003		xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE
Department of Homeland Security Policy for Defense of Cyberspace
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
O'Hara, Timothy M. ; Author

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as Report (SAR)	32	Rife, Dave RifeD@awc.carlisle.army.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

ABSTRACT

AUTHOR: Lieutenant Colonel Timothy M. O'Hara

TITLE: Department of Homeland Security Policy for Defense of Cyberspace

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 32 CLASSIFICATION: Unclassified

The phenomenal growth of personal computers combined with various means to network them has created a "cyberspace" that has revolutionized everything we do. Effects of the rapid expansion of cyberspace over the past ten years has been seen in just about every facet of American society to include, but not limited to education, commercial enterprises, private organizations, public utilities, government services, law enforcement and national defense. A closer look at commercial enterprises includes web browsing, chat rooms, e-mail, e-commerce, overhauls of business practices and organizations, telecommunication operations, and management of power grids and distribution centers. These are all directly linked to and rely on the availability of cyberspace. Although the United States may be at the forefront of this Internet explosion, the rest of the world is also fully connected and an integrated member of cyberspace. Consistent with American values, cyberspace is a medium that allows a free and open exchange of ideas and information while allowing wide accessibility. The same openness and availability we value as a great strength of cyberspace is also one of its great weaknesses and makes us vulnerable to attack by a wide variety of potential enemies. The defense of our networks is currently a wide and varied tapestry of security implementations and protocols at all levels of private, commercial, and government services or agencies. The creation of the Department of Homeland Security could potentially provide a new platform from which a nationwide cyberspace defensive strategy could be coordinated and implemented. This paper will review the current cyberspace defense policies of the United States and will evaluate the Department of Homeland Security's (DHS) current plan, highlighting the changes it will propose to current policy. It will make recommendations pertaining to the DHS plan, designed to further strengthen its role as protector of this nations cyberspace.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

DEPARTMENT OF HOMELAND SECURITY POLICY FOR DEFENSE OF CYBERSPACE

The phenomenal growth of personal computers combined with various means to network them has created a “cyberspace” that has revolutionized everything we do. Effects of the rapid expansion of cyberspace over the past ten years has been seen in just about every facet of American society to include, but not limited to education, commercial enterprises, private organizations, public utilities, government services, law enforcement and national defense. A closer look at commercial enterprises includes: web browsing, chat rooms, e-mail, e-commerce, overhauls of business practices and organizations, telecommunication operations, and management of power grids and distribution centers. These are all directly linked to and rely on the availability of cyberspace. Although the United States may be at the forefront of this Internet explosion, the rest of the world is also fully connected and an integrated member of cyberspace. Consistent with American values, cyberspace is a medium that allows a free and open exchange of ideas and information while allowing wide accessibility. The same openness and availability we value as a great strength of cyberspace is also one of its great weaknesses and makes us vulnerable to attack by a wide variety of potential enemies. The defense of our networks is currently a wide and varied tapestry of security implementations and protocols at all levels of private, commercial, and government services or agencies. The creation of the Department of Homeland Security could potentially provide a new platform from which a nationwide cyberspace defensive strategy could be coordinated and implemented. This paper will review the current cyberspace defense policies of the United States and will evaluate the Department of Homeland Security’s (DHS) current plan, highlighting the changes it will propose to current policy. This paper will make recommendations pertaining to the DHS plan, designed to further strengthen its role as protector of this nations cyberspace.

GROWING CYBER THREAT

The same properties of openness and accessibility that make cyberspace so attractive also make it vulnerable to attack and exploitation. In the early 1980’s the attackers were often called “hackers” and would more likely than not be high school/college students trying to prove to themselves that they could “break-in” to a system. These break-ins rarely caused any significant damage and were more for bragging rights among the hacker community than for destructive effects of their actions. Then as cyberspace began to expand and become more interconnected, the 1990s saw the arrival of a different type of “hacker” focused on a more intrusive type of behavior. These new “cyber terrorists” would often spread viruses, destroy data, or cause some form of disruption of services. Many nations have invested in offensive

and defensive cyberspace capabilities focused on defending their cyberspace interests. Since 1995, we have seen the development of a much more dangerous and advanced group of hackers, cyber terrorists, and state sponsored cyber warriors. Their tools, talents and capabilities have increased at a frightening pace. Today, anyone with Internet access can download sophisticated hacking tools from various hacker web sites with instructions how to use them. State and private sponsored probing of hundreds of our networks and systems occur everyday. Countries around the globe have developed cyber defenses that not only look to protect their space but also are able to exploit a potential enemy when needed. The statistics of reported attacks as seen below (Figure 1) are staggering. Over 80,000 incidences were reported in 2002, an 8000 percent increase over a ten-year period. Even more disturbing is that the Director; CERT®[1] Centers stated that he estimated as many as eighty percent of incidents

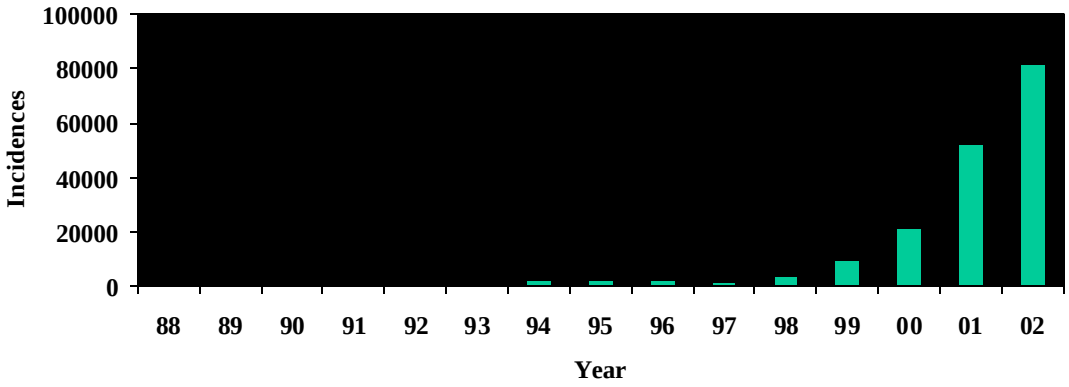


FIGURE 1 NUMBER OF INCIDENTS

go unreported for two reasons: (1) because the organization was simply not aware of the attack or (2) the organization was reluctant to report. In 2000 it was estimated that cyber crime had cost the global economy 1.6 trillion dollars.[2] Testimony of risks compiled by the United States General Accounting Office (GAO) before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives dated 19 November 2002 provided some of the following real world examples:

- "Just last week, news reports indicated that a British computer administrator was indicted on charges that he broke into 92 U.S. computer networks in 14 states belonging to the Pentagon, private companies, and the National Aeronautics and Space Administration during the past year, causing some $900,000 in damage to

computers. It also reported that, according to a Justice Department official, these attacks were one of the biggest hacks ever against the U.S. Military. This official also said that the attacker used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks looking for ones that might suffer from flaws in Microsoft Corporation's Windows NT operating systems software."[3]

- "The FBI's National Infrastructure Protection Center (NIPC) reported that on October 21, 2002, all of the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive "distributed denial of service" attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages. However, according to the media reports, a longer, more extensive attack could have seriously damaged worldwide electronic communications."[4]
- "In September 2002, NIPC issued a warning of cyber attacks against the International Monetary Fund and World Bank meetings to be held during the week of September 23.[5] The warning stated that, in addition to physical protestors, cyber groups might view the meetings as a platform to display their hacking talent or to propagate a specific message. Cyber protestors, referred to as "hacktivists," can engage in Web page defacements, denial-of-service attacks, and misinformation campaigns, among other attacks."[6]
- "In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[7] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. Consistent with this threat, NIPC also released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorist."[8]

- "In August 2001, we reported to this subcommittee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations.[9] Then in September 2001, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus that allowed it to spread widely in a shot amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage."[10]

Since 11 September 2001, it has become clear that terrorists' organizations such as al-Qaeda have effectively used cyberspace to attack the United States in a number of ways. Three examples include the use of encrypted email for direct communications, using web pages for promoting ideology and information campaigns, and developing methods of direct attack on networks or systems connected to the Internet. Evidence from Afghanistan would indicate al-Qaeda have their eyes on various critical infrastructures such as automated water treatment facilities that use computers to manage and regulate the water supplies. Given the ability to hack into the water treatment facility's management program, al-Qaeda could contaminate our drinking water without setting foot in the United States. Since the 1980s, the U.S. Government's efforts in the area of cyberspace security have not kept pace with the threat. Efforts between executive and legislative arms of government have historically not been well coordinated or synchronized.

CURRENT U.S. POLICY

Since the Computer Security Act of 1987, the U.S. Government has attempted to address the growing concern of cyberspace security. Technological advancements, particularly in the vast explosion of the Internet, have complicated the government's ability to keep up with effective information assurance and security policies. Many of these shortcomings came to a head in 1995 and 1996 prompting President Clinton to order a comprehensive review of the nation's critical infrastructure and vulnerabilities. This President's Commission on Critical Infrastructure Protection (PCCIP) reported in October 1997 on the widespread and growing capability to exploit US infrastructures, especially through information networks.[11] In May 1998, based on many of the PCCIP findings, the White House issued Presidential Decision Directive (PDD) 63[12]. This directive called for a range of activities to improve the nation's ability to detect and respond to cyber attacks, improve federal agency security programs, and establish a

partnership between the government and private sector. Since then, the Bush administration and the U.S. Congress have continued to address these security issues through various legislation, executive orders, and strategies.

CYBERSPACE LEGISLATION

Below are the primary legislative actions pertaining to use of cyberspace since 1986. It is not an all-exhaustive list, but is intended to provide an understanding to the complicated environment of cyber security. It highlights the fact that there are no overarching statutes on the use of cyberspace. Cyberspace legislation has been gradually pieced together over the years and could best be described as reactionary. Each piece of legislation stands on its own, providing a piece of the information assurance puzzle, but are not interrelated so as to form a cyberspace mosaic providing overall security. The following laws when combined with Presidential Directives, Executive Orders and National Security Strategy form the cyber security policy of the United States.

- Computer Fraud and Abuse Act 1986 – Prohibits unauthorized access to computer systems.
- Electronics Communications Privacy Act of 1986 – Prohibits interception of private email without a court order.
- Computer Security Act of 1987 – Designated the National Institute of Standards and Technology (NIST) as the lead government agency for computer security standards.
- Paperwork Reduction Act of 1995 – Ordered government agency to start digitizing or downloading its information to computer databases so that it could be easily accessible via the Internet and not require a paper copy.
- Clinger-Cohen Act of 1996 – Formerly known as the Federal Acquisition Reform Act of 1996 (FARA) and the Information Technology Management Reform Act of 1996 (ITMRA). FARA allowed DOD to streamline its acquisition process and thereby significantly shorten the time required to acquire information technologies. ITMRA further advanced the changes made by FASA.
- GIRSA Government Information Security Reform Act (November 2000) – Was a two-year mandate by Congress to all levels of government to develop and implement cyber security plans. This mandate has not been achieved.

- Cyber Security Research and Development Act of 2002 -- Allocates over 900 million dollars in scholarships, grants and research centers at American colleges and universities towards cyber security research.

The most recent legislation to pass Congress was the Cyber Security Research and Development Act. It allocates 903 million dollars in support of private institutions' research and development of cyber security technologies and professionals. This money will be used to promote higher education and research for the development of cyberspace experts capable of dealing with current day threats and challenges. This legislation is consistent with current cyberspace policy.

PRESIDENTIAL DECISION DIRECTIVE 63 (PDD-63)

In 1998, President Clinton issued PDD 63 as a strategy for government and private institutions to develop a cooperative spirit in the effort to protect the physical and cyber-based well-being of America's most critical infrastructures. It established Critical Infrastructure Protection (CIP) as a national objective with an initial capability to be in place by the close of 2000 and a more robust capability by 2003. PDD-63 designated and established the following organizations in order to provide a central coordination of this effort. It includes:[13]

- "Critical Infrastructure Assurance Office (CIAO), [14] an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies."
- "National Infrastructure Protection Center (NIPC)[15], an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response."
- "National Infrastructure Assurance Council (NIAC)[16], an office to enhance the partnership of the public and private sectors in protecting our critical infrastructures"
- Information Sharing and Analysis Centers (ISAC)[17], are privately owed organizations, voluntarily created in order to participate in PDD-63.

PDD-63 identified eight private infrastructures and five special functions along with their associated lead agencies (Table 1). For each of these infrastructures and special functions, PDD-63 assigned lead agency responsibility within the federal government, for example,

Information and Communications Sector was assigned to the U.S. Department of Commerce, while the Intelligence Function was assigned to the Central Intelligence Agency (CIA). Each of these government agencies is responsible for developing a working relationship with those private institutions aligned to their sector or special function. PDD-63 was created to protect critical infrastructures across the country. Its strategy was to build a partnership between government and the private sector in achieving an acceptable level of security. Specific to cyberspace, PDD-63's creation of the NIPC (hosted by the FBI) was an important first step in providing a crisis response capability as it provides the nation a place to turn to in the event of attack. NIPC has worked closely with the FBI to aggressively and effectively go after hackers and cyber terrorist here in the U.S. The ISACs also provide cyberspace an excellent forum to share defensive techniques and technologies as they arrive on the scene. The challenge for the Department of Commerce is that as the responsible agent, of "information and

INFRASTRUCTURE SECTORS	**LEAD AGENCY**
Information and Communications	Commerce
Banking and Finance	Treasury
Water Supply	EPA
Aviation, Highway, Mass Transit, Pipelines, Rail, Waterborne Commerce	Transportation
Emergency Law Enforcement	Justice/FBI
Emergency Fire Services, Continuity of Government	FEMA
Electric Power, Oil and Gas Production and Storage	Energy
Public Health Services	HHS
SPECIAL FUNCTION	**LEAD AGENCY**
Law Enforcement / Internal Security	Justice/FBI
Intelligence	CIA
Foreign Affairs	State
National Defense	DOD
Research and Development	OSTP

TABLE 1. PDD-63 SECTORS AND LEAD AGENCIES

communications", it is expected to coordinate specific cyberspace issues across all eight sectors and five special function areas. PDD-63 recognized the need to protect cyberspace, however, it was rather vague and non-specific on who or what needed to be done about it.

EXECUTIVE ORDER 13231

In October 2001, by Executive Order 13231,[18] President Bush expanded CIAO's role with the establishment of The President's Critical Infrastructure Protection Board (PCIPB). On 20 September 2002, the PCIPB issued a cyber security plan.[19] Its strategy builds on current policies while placing the responsibility of the nation's cyber defenses on all owners and users of cyberspace. From the home user to the Federal Government, each individual and organization has a responsibility to secure its own cyberspace. This will be accomplished through awareness and information, technology and tools, training and education, roles and partnerships, federal leadership, and coordination and crisis management. The means will be through private and governmental funding primarily focused on the development of highly skilled cyber security personnel. In support of this strategy, the President signed the Cyber Security Research and Development ACT into law;[20] authorizing $903 million over five years for creating cyber security research centers, undergraduate program grants, and fellowships through the National Science Foundation (NSF). Noticeably, the Department of Homeland Security is not directly mentioned in Executive Order 13231 or in the cyber security plan. The cyber security plan describes the objectives but fails to recommend or describe solutions. The cyber security plan of the PCIPB has been incorporated in the new *National Strategy to Secure Cyberspace*.

NATIONAL STRATEGY TO SECURE CYBERSPACE

The purpose of the *National Strategy to Secure Cyberspace* is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.[21] Its strategic objectives are to:

- Prevent cyber attacks against America's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur

This strategy recognizes that the security of cyberspace will require a coordinated effort from both private and public sectors of our society. It states that the private sector is generally

better structured and equipped to deal with cyber threats than the federal government. It describes an environment where government will only step in to protect its own cyber infrastructure and those public and commercial assets required for the continuity of government and essential services. The intent of this strategy is to limit the direct federal involvement with the private sector when pertaining to cyberspace. It lays out cyber security responsibilities for the newly formed Department of Homeland Security. This strategy can be best described as defensive in nature. With little control over commercial Internet service providers, the ability for the federal government to protect the public cyberspace is significantly reduced or nonexistent. The vast majority of federal actions in the face of cyber attacks will be after the incident occurs, trying to ascertain the damage assessment and the culprit responsible.

DEPARTMENT OF DEFENSE

Historically the U.S. has often turned to its military leadership and technical expertise in order to exploit emerging technologies and capabilities. An example of this is in the field of engineering. In the early 1800s up through the Civil War, West Point was one of America's finest engineering schools. Serving while on active duty or later as civilians, West Point engineers designed and built much of the country's roads, canals, and utilities.[22] These efforts not only supported the military's need for potential supply routes, it greatly enhanced the economic development of the country. As part of the early railroad expansion, West Point graduates applied their military training to the development of a new corporate model while working for the Baltimore and Ohio Railroad Company.[23]

Military influence on both defense and commercial development was again seen when on 29 June 1956, President Eisenhower signed the Federal Aid-Highway Act of 1956, which authorized the interstate highway system (later formally named the Dwight D. Eisenhower System of Interstate and Defense Highways). This system of roads and bridges not only supports strategic military needs of the nation but also directly supports the economic health of businesses across the country. Within the Department of Transportation, the Federal Highway Administration (FHA) was created to manage this network of roads. The majority of funding for the interstate highway system continues to come from Federal and State user fees on the price of gasoline. FHA ensures high standards are met for the interstate highway system. Access to all interstates is strictly controlled through the use of exit and entrance ramps. No intersections or traffic signals are allowed. All traffic and railroad crossings are separated through the construction of more than 55,000 bridges. Interstates are divided and have at least four wide traffic lanes (two in each direction) and adequate shoulders. Curves are engineered for safe

negotiation at high speed, while grades are moderated, eliminating blind hills. Rest areas are conveniently spaced.

Recognizing the long history that the U.S. Military has had in the development of key and essential infrastructures across this nation, DOD has created its own Interservice Internet Highway System called MILNET (Military Network). It is a tightly regulated and controlled sub network of the global Internet, providing its users a much safer and secure environment to operate from, yet the flexibility of allowing multiple connections to the Internet.

The centerpiece to the DOD implementation of a cyber security plan and its command and control of MILNET is the Joint Task Force – Computer Network Operations (JTF-CNO), located within the U.S. Strategic Command. Its mission is to direct the defense of DOD computer systems and networks, coordinate and, when directed, conduct computer network attacks in support of combatant commanders and national objectives. JTF-CNO is comprised of two specific yet complimentary mission areas: Computer Network Defense (CND) and Computer Network Attack (CNA). The National Cyberspace Strategy focuses solely on CND, while CNA is a tightly controlled offensive DOD capability.

The JTF-CNO service components are the Army's Land Information Warfare Activity (LIWA), the Air Force Forces-Computer Network Operations (AFFOR-CNO), Navy Component Task Force-Computer Network Defense (NCTF-CND), Marine Forces-Integrated Network Operations (MARGOR-INO), and Defense Information Systems Agency's DOD Computer Emergency Response Team (DOD CERT). JTF-CNO sets the policies for each of the services to implement. Day-to-day operations are fully integrated with JTF-CNO and DISA, to insure real time coordination and synchronization with all the services and agencies within DOD.

Since aggressively addressing the major concern of cyber security in 1998, DOD has struggled to implement an effective cyber security plan that significantly reduces the risk of attack. DOD has been a leader within the U.S. in developing the infrastructure, standard operating procedures, and protocols designed to improve its cyber security. The vast size of DOD and its numerous agencies and organizations make this task a daunting one. Understanding the significant risks and numerous vulnerabilities within cyberspace is to recognize how implementation of even the most robust and comprehensive security plan as witnessed within DOD is a challenge on a grand scale.

Daily intrusions still occur across DOD. All it takes is one network administrator's password to be compromised to allow a potential attacker access to that administrator's entire network. This intrusion might lead to further access to neighboring networks as well based on the trust relationship between domains. It has taken DOD five years of concerted effort to

significantly improve their cyber security posture. Yet there is still work to be done. Today, DOD has built layers of defense across the services focused primarily on network access points that allow a 24 Hour watch of all critical network operations. Use of security routers, intrusion detection systems (IDS), and certification of system programs, as defensive measures greatly restrict an outside agent from hacking his way into the DOD infrastructure. These technologies help the system administrators' monitor all outside activity thereby gaining a certain amount of situational awareness that alerts them to possible intrusions or attacks. The greatest challenge for DOD and all users of cyberspace is that "you are only as secure as your weakest link". If one network server misses a security patch or software upgrade and a sophisticated hacker gains access, a tremendous amount of damage can be done. Technologies such as IDSs or asset configuration control software gives a network operation center the ability to recognize the vulnerability before it occurs and great insight to the potential damage if the intrusion is successful. In spite of all these challenges, DOD has taken a lead role in providing a rather robust and layered defensive approach toward the protection of its networks. Intrusions and attacks still occur, and some are successful, but the amount of damage done, and speed to which the network can respond continues to improve.

EFFECTIVENESS OF CURRENT CYBER SECURITY POLICY

A recent GAO report on the effectiveness of current cyber security policy found that it has not been fully implemented[24]. It describes unwillingness across all the twenty-two federal agencies to provide manpower and resources to the NIPC or within their own structures. The NIPC was recognized as effective in reacting to and providing damage control after attacks have occurred. The NIPC's close association with the FBI has allowed it to develop a culture that is more focused on criminal investigations, not on preventing the crime from occurring. This association also inhibits the ability of the NIPC to influence and work with the private sector due in part to the public's natural fear of governmental intervention. GAO recognized that current policy is almost impossible to enforce and thereby holds various organizations accountable. As seen in Figure 2, PDD 63 lacks a simplified command and control structure necessary to bring about synergy and responsiveness across all federal agencies. Executive Order 13231 places much of the burden of cyber security back on the individual user or private organization. The National Strategy to Secure Cyberspace reiterates the current policy of public and private cooperation with no clear mandate or direction. It promotes the increased development of cyber security schools, training and experts, but prefers that the federal government sees to its own infrastructure protection while working with private industry to develop the standards and

protocols to bring about cyber security. Current cyberspace defense policy as implemented will not prevent the next attack or intrusion.

Changes to the current policy must be made to improve the country's cyberspace defense posture. Great strides have been made in the area of education and awareness. There is an understanding across the nation of the need for a robust and effective defensive strategy. The federal government must be able to protect the critical infrastructure and to take appropriate measures to stop an attack before it occurs. The creation of a new Department of Homeland Security (DHS), in the aftermath of 11 September 2001, will directly effect changes to be made in current policy. With its mission to "secure cyberspace" of our nation's critical infrastructure, let us review DHS's proposed organization. (Figure 2. Department of Homeland Security)

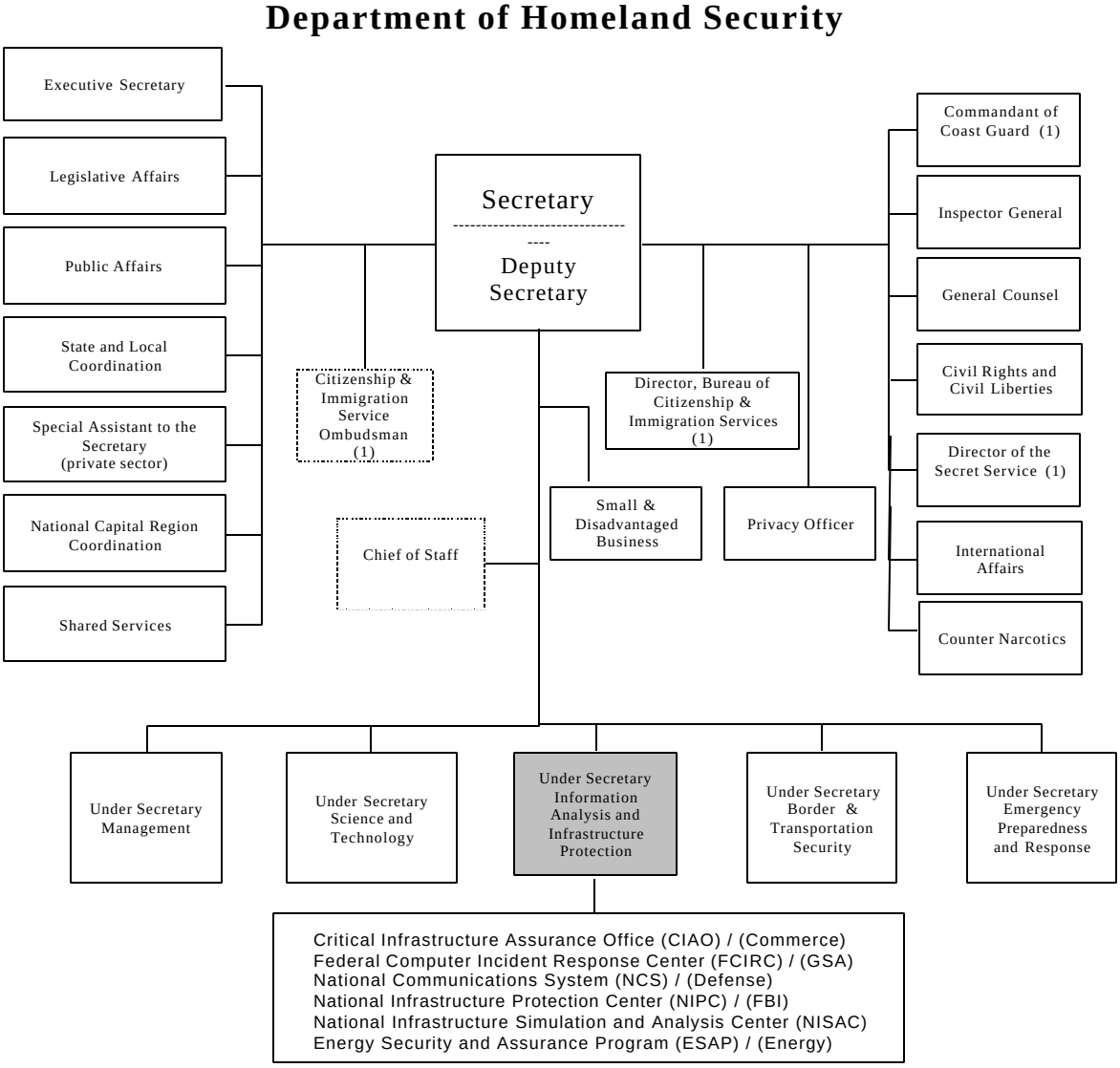
The best opportunity for the United States to develop a comprehensive and effective Cyberspace Defense policy is to place this responsibility on the shoulders of the Department of Homeland Security (DHS). As currently planned, DHS will be organized into Five Major Directorates headed by Under Secretaries: Management, Science and Technology, Information Analysis and Infrastructure Protection Directorate, Border and Transportation Security, and Emergency Preparedness and Response (See Figure 3 – DHS Organization Chart).[25]

The Information Analysis and Infrastructure Protection (IAIP) Office will be responsible for cyberspace. It will have transferred to it the following organizations (losing agencies in parentheses):

- Critical Infrastructure Assurance Office (CIAO) / (Commerce)
- Federal Computer Incident Response Center (FCIRC) / (GSA)
- National Communications System (NCS) / (Defense)
- National Infrastructure Protection Center (NIPC) / (FBI)
- National Infrastructure Simulation and Analysis Center (NISAC)
- Energy Security and Assurance Program (ESAP) / (Energy)

This is an impressive list of cross agency organizations to be brought under one roof within the IAIP office. The catalyst for this gathering of organizations was in response to one of the major initiatives stated in the *National Strategy for Homeland Security's,* which is to "Secure Cyberspace". [26] Additionally, in the executive summary of the *National Strategy to Secure Cyberspace*, DHS was assigned some specific roles and functions. These responsibilities include:[27]

- "Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States." (CIAO)



Note (1): Effective March 1st, 2003

FIGURE 2. DEPARTMENT OF HOMELAND SECURITY

- "Providing crisis management in response to attacks on critical information systems" (NPIC)
- "Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems." (FCIRC)
- "Coordinating with other agencies of the federal government to provide specific warning information and advice about appropriate protective measures and counter measures to state, local, and nongovernmental organizations including private sector, academia, and the public."
- "Performing the funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security." (NISAC)

The centralization and transfer of assets of those agencies that currently perform various functions could provide a tremendous amount of synergy in support of current national cyberspace policy. The creation of the Information Analysis and Infrastructure Protection (IAIP) Office will be able to address some of the criticism of numerous GAO reports on the effectiveness of PDD-63 and current U.S. policy. IAIP will provide a common platform to address major cyber issues from both public and private sectors of cyberspace. However, as envisioned, the effectiveness of IAIP in stopping an attack prior to occurring is undeniably suspect. Without some ability to control the access and use of the Internet, this implementation of cyberspace security will not have the ability to develop the necessary intelligence to prevent an attack. Using the DOD implementation of cyberspace defense as a model, in response to the cyberspace threat we live in today, recommended changes to the IAIP will now be addressed.

RECOMMENDATIONS

Cyberspace as it exists today is a virtual medium that is not restricted by lines on a map or national borders. Cyber-based activities are now imbedded in nearly all private and government organizations. Access points (e.g. exit ramps and entrance ramps) and connection paths are virtually unlimited and uncontrolled. There is both a physical and electronic capability that must be protected. Physical vulnerabilities are no longer the only concern as virtual attacks are now possible. One must worry not only about the physical security of a dam, but also that

same dam's remotely controlled and potentially vulnerable computer system. Current policy, combined with the expected transfers of agencies to DHS, is not sufficient to stop cyberspace attacks. At best, it will provide a capable consequence management capability, but will not be able to actively manage or affect daily cyberspace activities.

The current U.S. strategy for cyber security is based on a presumption that everyone who owns and operates a computer or a network of computers is responsible for ensuring they protect themselves against an attack. But in reality, when skilled and professional hackers, cyber terrorists, or state sponsored operators, are aggressively attempting to invade one's privacy, individual users are not typically educated or prepared for this challenge. Significant investments in both manpower and equipment combined with new organizations are necessary if both public and private cyberspace is to achieve an effective level of security. An organization that can provide a high degree of information assurance while severely limiting the risk of successful attacks must be created. DOD's creation of JTF-CNO and concurrent capabilities in each of the Services is a model program that should be emulated in regards to national cyberspace defense.

Implementing an effective cyberspace security plan will require additional infrastructure be built over which a command and control agency be added. As with the interstate highway system of the 1950's, a new National Cyberspace Highway System (NCHS) needs to be constructed. Operated by a proposed National Cyberspace Operations Center (NCOC), this system would be for both public and private use and would allow the government to greatly increase both the information assurance and security of electronic commerce and communications. The combination of protecting proprietary data while simultaneously ensuring that the cyberspace highway stays clear of accidents and keeps traffic flowing at optimum speeds would provide an environment that enhances both expansion and growth of commercial and government activities. Analogous to speed limits and safety requirements, each user of the NCHS would be expected to meet certain criteria before taking the "on ramp". Unlike the Federal Highway Administration, the management of NCHS would require additional authorities to ensure the safety of the network, much like the Federal Aviation Administration ensures safe air travel. Funding of the NCHS could be accomplished through matching funds and accelerated depreciation of current assets for both State and private organizations that decide to participate. The NCHS would be not be interested in proprietary or specific data flowing on the highway, but in providing a safe thoroughfare that electronic traffic could efficiently transit.

The proposed organization of the DHS, combined with the construction and management of the NCHS, would allow the U.S. to develop preventative measures that would

significantly reduce the threat of cyber attacks before they occur. DHS's recent combining of the CIAO, FCIRC, NIPC, and NIASC is a logical and necessary step and will bring a level of synergy that has been missing since the release of PDD-63. The new DHS will have the ability to correct PDD-63's shotgun approach of spreading responsibility for CIP across the entire government with limited focus and success. Bringing these critical agencies under one Secretary will greatly improve coordination and cooperation across private and government agencies and offer an opportunity to build a cyber highway system that can provide better business opportunities with better national security.

In response to the cyberspace challenges of today, and using DOD as a model, the following recommendations and modifications of DHS are proposed:

- Create the National Cyberspace Highway System (NCHS)
- Create a separate and distinct office of Cyberspace Protection Directorate within the DHS and IAIP that can coordinate and implement necessary protection and security protocols across government and public sectors.

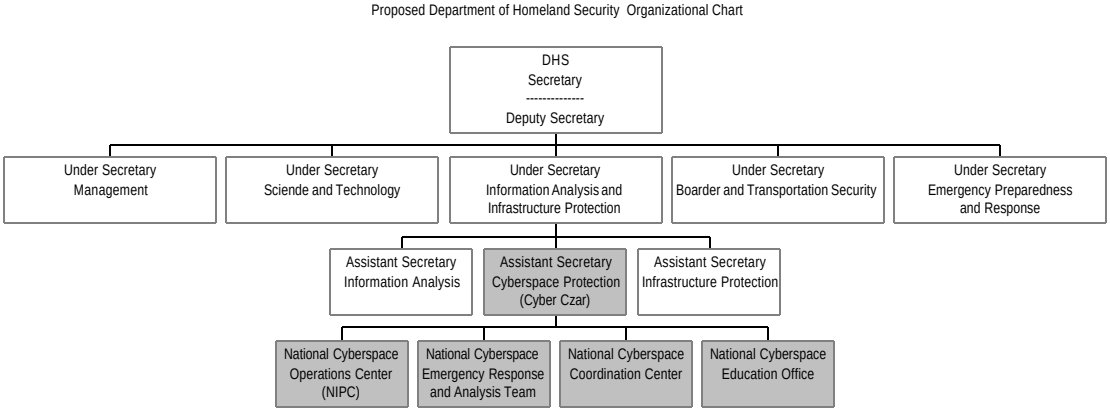


FIGURE 3. PROPOSED CHANGES TO DHS ORGANIZATION

- Designate the Director of the Cyberspace Protection Directorate as the "Cyberspace Czar" to act as the National Coordinator.
- Expand the NIPC and create a National Network Operations Center (NNOC) along the lines of JTF-CNO that manages the day-to-day operation of the NCHS. Also responsible to provide consequence management, vulnerability assessments and intrusion alerts.
- Create a National Cyberspace Emergency Response and Analysis Team
- Create a National Cyberspace Coordination Center
- Create a National Cyberspace Education Office

Creation of a Cyber Czar will provide the nation with a focal point for all cyberspace activities. It will provide both public and private sectors with a clear chain-of-command, enhancing both prevention and crisis management in the event of an attack. DOD's JTF-CNO's creation with a well defined chain-of-command, combined with the ability to direct network operations across the breadth of DOD and the MILNET, has created a well managed and relatively secure network. JTF-CNO is able to mitigate risk and quickly respond when a successful attack occurs. The CAIO would make up the bulk of this office.

The greatest weakness to the DHS plan is in the area of cyber attack prevention. Creation of a National Cyberspace Highway System (NCHS) combined with a National Cyberspace Operations Center (NCOC) with both CND and CNA and the National Cyberspace Emergency Response and Analysis Team (NCERAT) would be able to address prevention as well as crisis response. The mission of the NCOC would be to provide continuous technical control of the NCHS, and would be expected to work closely with the private sector by providing technical assistance as required. The NCERAT, modeled after the DOD-Computer Emergency Response Team DOD-CERT, would be collocated with NCOC and provide threat analysis based on data provided by various detection systems located at key points around the country. This data when properly analyzed can provide tremendous incite to the identity and capabilities of potential enemies. Based upon its analysis and various threats, the NCERAT would provide a National Information Assurance Vulnerability Alert (IAVA) database, assessable by both public and private organizations in support of their cyber security programs. The NCERAT would also provide highly skilled cyber experts able to deploy in times of crisis to repair or assess possible damage to key infrastructure in the event of a successful attack. Manning for this organization would come from the NIPC and FCIRC.

The National Cyberspace Coordinator would be responsible for developing the close working relationship between federal, state, local, and private organizations to cyberspace security concerns. This office would work closely with Information Sharing and Analysis Centers across the country to promote the sharing of new technologies and technical solutions across the nation. Basis for creation of this office would come from the National Infrastructure Simulation and Analysis Center.

The National Cyberspace Education Office would be responsible to developing educational material and classes, via the web, that will target individual users and promote safe and secure operating practices. The goal of this office would be to raise the level of national

awareness to potential cyberspace threats. The intent would be for these classes and educational services to be free and assessable to everyone.

The Department of Homeland Security, by its very nature would be extremely effective when working with all levels of federal, state, local, and private organizations. DHS combined with the creation of the NCHS is the perfect organization to provide the necessary leadership to make cyberspace defense a reality. As currently configured, DHS will fall short of its mission to secure cyberspace. The challenges the nation faces in protecting cyberspace against the individual hacker to sophisticated cells of state sponsored terrorists will continue to increase. Potential intruders can now assail the U.S. from anywhere in the world where Internet access exists. Information assurance on all forms of cyberspace and systems demands a security strategy that is both complex and comprehensive. Implementation of these recommendations would provide the U.S. a safe and secure cyberspace capable of protecting critical infrastructure while promoting business opportunities in a global economy.

WORD COUNT = 6,159

ENDNOTES

[1] CERT Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[2] As stated on 26 July 2000, by Michael Vatis, then Director of the NIPC within the FBI while testifying before the House Subcommittee on Government Management, Information, and Technology.

[3] U.S. General Accounting Office. Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-03-303T. (Washington, D.C.: 19 November 2002), 6.

[4] Ibid.

[5] National Infrastructure Protection Center, Assessment 02-002: Hacktivism in Connection with Protest Events of September 2002 (Washington, D.C.: September 23, 2002).

[6] U.S. General Accounting Office. Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-03-303T. (Washington, D.C.: 19 November 2002), 6.

[7] National Infrastructure Protection Center, Swarming Attacks: Infrastructure Attacks for Destruction and Disruption (Washington D.C. July 2002).

[8] U.S. General Accounting Office. Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-03-303T. (Washington, D.C.: 19 November 2002), 6.

[9] U.S. General Accounting Office, Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures; GAO-01-1073T (Washington D.C.: August 29, 2001).

[10] U.S. General Accounting Office. Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-03-303T. (Washington, D.C.: 19 November 2002), 7.

[11] Wentworth, Frances “Critical Infrastructure Protection: Establishing an Information Sharing and Analysis Center (ISAC) Can Be Like Developing an Organizational Security Policy”, 26 September 2000.

[12] Clinton, William J, U.S. Policy on Critical Infrastructure Protection. The Presidential Decision Directive - PDD 63. (Washington, D.C., The White House, May 1998).

[13] U.S. General Accounting Office. Critical Infrastructure Protection – Significant Challenges Need to Be Addressed. GAO-02-961T. (Washington, D.C.: 24 July 2002).

[14] Critical Infrastructure Assurance Office Web page, Available from <http://www.ciao.gov/publicaffairs/about.html>, Internet. Accessed 13 October 2002.

[15] National Infrastructure Protection Agency Web Page. Available from <http://www.nipc.gov/about/about.htm>, Internet, Accessed 13 October 2002.

[16] Executive Order 13231 replaces the National Infrastructure Assurance Council (NAIC) council with the National Infrastructure Advisory Council (NIAC).

[17] Information Sharing and Analysis Center Defined, Available from <https://www.it-isac.org/isacinfowhtppr.php>. Internet. Accessed 16 October 2002.

[18] George W Bush, Executive Order 13231 "Critical Infrastructure Protection in an Information Age". (Washington, D.C.: The White House, 18 October 2001). Available from <http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html>, Internet, Accessed 13 October 2002.

[19] The President's Critical Infrastructure Protection Board, "The National Strategy to Secure Cyberspace for Comment - Draft", (Washington, D.C.: The White House, September 2002). Available from <http://usinfo.state.gov/topical/global/ecom/02092002.htm>, Internet, Accessed 13 October 2002.

[20] U.S. Congress. House. Cyber Security Research and Development Act, 107th Cong., 2d sess,29 August 2001.

[21] The President's Critical Infrastructure Protection Board, "The National Strategy to Secure Cyberspace for Comment - Draft", (Washington, D.C.: The White House, September 2002). Available from <http://usinfo.state.gov/topical/global/ecom/02092002.htm>, Internet, Accessed 13 October 2002.

[22] Smithsonian National Museum of American History Behring Center Web Page, "West Point in the Making of America," available from http://www.americanhistory.si.edu/westpint/history_0.html>;Internet; accessed 23 March 2003.

[23] Ibid.

[24] U.S. General Accounting Office. Critical Infrastructure Protection – Significant Challenges Need to Be Addressed. GAO-02-961T. (Washington, D.C.: 24 July 2002).

[25] Department of Homeland Security <https://www.dhs.gov/dhspublic/display?theme=13>. Internet. Accessed 29 January 2003.

[26] George W. Bush, National Strategy for Homeland Security, Washington, D.C.: The White House, The President's Critical Infrastructure Protection Board, "The National Strategy to Secure Cyberspace for Comment - Draft", (Washington, D.C.: The White House, September 2002). Available from <http://usinfo.state.gov/topical/global/ecom/02092002.htm>, Internet, Accessed 13 October 2002. July 2002.

[27] Ibid.

BIBLIOGRAPHY

Burnett, Peter L. III. Information Operations Strategy Research Project. Carlisle Barracks: U.S. Army War College, 9 April 2002.

Bush, George W. "President Delivers State of the Union Address." 29 January 2002. Available from <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html>. Internet. Accessed 13 October 2002.

_____. The National Security Strategy of the United States of America. Washington, D.C.: The White House, September 2002.

_____. Executive Order 13231 "Critical Infrastructure Protection in an Information Age". Washington, D.C.: The White House, 18 October 2001.

_____. National Strategy for Homeland Security, Washington, D.C.: The White House, July 2002.

Clinton, William J. U.S. Policy on Critical Infrastructure Protection. The Presidential Decision Directive - PDD 63. Washington, D.C.: The White House, May 1998.

Infragard. "Welcome to Infragard." Available from <http://www.infragard.net>. Internet. Accessed 6 October 2002.

Information Sharing and Analysis Center Defined. Available from <https://www.it-isac.org/isacinfowhtppr.php>. Internet. Accessed 29 January 2003.

Myers, Richard B. National Military Strategy of the United States of America, Pre-Decisional Draft. Washington, D.C.: U.S. Department of Defense, 19 September 2002.

"National Infrastructure Protection Center (NIPC) - About NIPC - Critical Infrastructure." Available from <http://www.nipc.gov/about/about4.htm>. Internet. Accessed 13 Oct 2002

"National Infrastructure Protection Center (NIPC), Swarming Attacks: Infrastructure Attacks for Destruction and Disruption." Washington, D.C. July 2002.

Porter, Charlene. "White House Draws New Plan for Information Infrastructure Security". Available from <http://usembassy.state.gov/posts/ja1/wwwhse1716.html>.Internet Accessed 6 October 2002.

Smithsonian National Museum of American History Behring Center Web Page, "West Point in the Making of America," available from <http://www.americanhistory.si.edu/westpint/history_0.html>.;Internet. Accessed 23 March 2003.

The President's Critical Infrastructure Protection Board, "The National Strategy to Secure Cyberspace for Comment - Draft", Washington, D.C.: The White House, September 2002.

U.S. Congress, Senate, Commerce Subcommittee, Cybersecurity Legislation, 107th Cong., April 24, 2002 Available from <http://www.house.gov/science/press/107/107-205.htm> Internet. Accessed 13 October 2002.

U.S. Congress. House. Cyber Security Research and Development Act, 107th Cong., 2d sess, 29 August 2001.

U.S. Congress. House. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations "What Can be Done to Reduce the Threats Posed by Computer Viruses and Worms to the Workings of Government?" 107th Cong., 2d sess. 29 August 2001.

U.S. Congress. House. Joint Economic Committee Congress of the United States. Wired World: "Cyber Security and the U.S. Economy". 107th Cong., 2d Sess, 21 June 2001.

U.S. Department of Commerce, Critical Infrastructure Assurance Office Web Page, Available from <http://www.ciao.gov/publicaffairs/about.html>, Internet. Accessed 13 October 2002.

U.S. Department of Homeland Security, Web Page. Available from <http://www.dhs.gov> Internet. Accessed 29 January 2003.

U.S. General Accounting Office. Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures. GAO-01-1073T. Washington, D.C. 29 August 2001.

U.S. General Accounting Office. Critical Infrastructure protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C. 26 September 2001.

U.S. General Accounting Office. Critical Infrastructure protection: Significant Challenges Need to Be Addressed. GAO-02-961T. Washington, D.C. 24 July 2002.

U.S. General Accounting Office. Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-03-303T. Washington, D.C. 19 November 2002.

U.S. General Accounting Office. Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. GAO-02-231T. Washington, D.C. 9 November 2001.

"Using 21st Century Technology to Defend the Homeland." 20 January 2001. available from http://www.whitehouse.gov/homeland/21st-technology.html. Internet. Accessed 6 October 2002.

Wentworth, Frances. "Critical Infrastructure Protection: Establishing an Information Sharing and Analysis Center (ISAC) Can Be Like Developing an Organizational Security Policy." 26 September 2000. Available from <http://www.sans.org/infosecFAQ/infowar/CIP.htm>. Internet.

Walter, Frederick H. III. Protecting America's Critical Infrastructure Strategy Research Project. Carlisle Barracks: U.S. Army War College, 1 March 2002.