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.

THE EFFECTS OF PRESIDENTIAL DECISION DIRECTIVE 63 ON THE PUBLIC

BY

PAUL R. SMULIAN
National Security Agency

USAWC CLASS OF 2000

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

USAWC STRATEGY RESEARCH PROJECT

The Effects of Presidential Decision Directive 63 on the Public

By

Paul R. Smulian
National Security Agency

COL Ralph Ghent
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

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

ABSTRACT

AUTHOR: Paul R. Smulian

TITLE: The Effects of Presidential Decision Directive 63 on the Public

FORMAT: Strategy Research Project

DATE: 1 April 2000 PAGES: 27 CLASSIFICATION: Unclassified

Specific recommendations made in a report by The President's Commission on Critical Infrastructure resulted in Presidential Decision Directive 63 (PDD-63). PDD-63 complimented actions initiated under Presidential Decision Directive-39 (PDD-39) and specifically targeted the nation's cyber-infrastructure for protection. In December 1999, the Federal Government's plan entitled "Defending America's Cyberspace: National Plan for Information Systems Protection," was finalized and signed by the President. This report analyzes the Federal Government's plan and determines what effects the plan will have on the citizens of the United States.

TABLE OF CONTENTS

PREFACE

Infrastructure Protection covers a wide array of problems presented to the government and private industry of the United States. Worldwide accessibility to the Internet coupled with motive, opportunity, and cheap and accessible tools enable many types of attacks upon the networks, computers, databases, and control mechanisms that are attached to this worldwide network of networks. A relatively small group of citizens from the private and public sectors as well as the Military sector recognized the threat that was posed by this accessibility and set out to counter the threat efficiently and effectively. The result of their efforts was Presidential Decision Directive 63. This directive will forge the way for the future for infrastructure security of computer information systems and networks for the next century.

ACKNOWLEDGEMENTS

I would like to acknowledge those who have helped me along the way in the research and development of this project. First, Mr. Daniel Knauf who got me involved in infrastructure protection; Mr. Mike Jacobs who encouraged me to pursue this topic; Mr. John Tritak who provided unique insight to the problems and situations that arise from implementing plans. Several individuals from the Federal Bureau of Investigation's National Information Protection Center and the Bureau's legal department who shall remain unnamed here have also contributed to this effort. Many folks who work part time at the Critical Infrastructure Assurance Office have contributed their time and effort as well as their written products as part of the research effort for this paper. Finally, COL Ralph Ghent who provided guidance, consultation, and material when all seemed dismal.

THE EFFECTS OF PRESIDENTIAL DECISION DIRECTIVE 63 ON THE PUBLIC

In the beginning of time, man did not have to worry about something called infrastructure. Depending on the version of history you subscribe to, the greatest amount of infrastructure may have been a beautiful garden or a cold damp cave. Today, to keep us going, we do have to worry about things like water supplies, electrical grids, telecommunications networks, financial transactions, emergency fire services, continuity of federal government services, public health services, oil and gas production and storage facilities, national defense, and computer networks.

In 1996, President Clinton issued Executive Order 13013 that established the President's Commission on Critical Infrastructure Protection (PCCIP). This Commission studied issues concerning the protection of the nation's most critical infrastructures against enemy attack from both nation states and non-nation state aggressors. The Commission determined that protections exist for much of the nation's infrastructure as a result of Presidential Decision Directive 39 (PDD-39).[1] This Directive ensured that government and industry would partner to protect the most important facets of the nation's infrastructure. As a result of PDD-39, federal agencies and private sector providers took positive actions to secure the nation's utility infrastructure. But as technology progressed and the United States became increasingly reliant on Internet technology to control and manage infrastructures, business transactions, and communications, it was clear that initiatives resulting from PDD-39 would not provide adequate coverage for the new cyber-infrastructure.

Specific recommendations made in a report by The Presidents Commission on Critical Infrastructure[2] resulted in Presidential Decision Directive 63 (PDD-63). PDD-63 complimented actions initiated under PDD-39 and specifically targeted the nation's cyber-infrastructure for protection. PDD-63 called for each infrastructure sector to develop plans that would address cyber-protection. In December 1999,[3] the Federal Government's plan was finalized and signed by the President. Entitled "Defending America's Cyberspace: National Plan for Information Systems Protection," the plan outlines specific initiatives for various sectors of the United States Government including the Environmental Protection Agency, Transportation Department, Justice Department/Federal Bureau of Investigation (FBI), Federal Emergency Management

Agency (FEMA), Health and Human Services Department (HHS), Energy Department, Central Intelligence Agency (CIA), the State Department, the Commerce Department, the Treasury Department, the National Security Agency, the Department of Defense, and the Executive Branch.[4] This report analyzes the Federal Government's plan and determines what effects the plan will have on the citizens of the United States.

PRESIDENTIAL DECISION DIRECTIVE SIXTY-THREE

THE NATIONAL PLAN

The Critical Infrastructure Assurance Office (CIAO) was established as a result of Presidential Decision Directive 63. The CIAO's first task was to prepare a plan for the protection of critical information systems within the federal government. The plan was written by various parts of the federal government, assembled by the CIAO, and then staffed throughout key government agencies and departments for comments. The plan has many different parts and outlines ten programs which, when implemented, will provide for continued operation of the nation's critical information systems. The ten programs are organized around three broad objectives. These objectives and their associated programs are:[5]

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

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

- ***Objective: Detect and Respond***: We must take those actions required to identify and assess an attack in a timely way, to contain the attack, to quickly recover from it, and to reconstitute affected systems.

    - Program 2: Detect Attacks and Unauthorized Intrusions

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

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

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

➢ ***Objective: Build Strong Foundations***: We must take steps as a nation to create and nourish the people, organizations, laws, and traditions which will make us better able to Prepare and Prevent, Detect and Respond to attacks on our critical information networks.

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

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

- Program 8: Reach out to Make Americans Aware of the Need for Improved Cyber-Security

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

The last program in the plan is not associated with a specific objective.

- Program 10:[6] 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

ANALYSIS

This section provides a brief overview of each program and identifies those parts of the plan that will affect the public. It also looks at each program for positive and negative effects on the public.

Program 1 looks primarily at existing assets and shared interdependencies and addresses vulnerabilities. This program will produce many coordination actions and in-depth studies that address the security infrastructure of today's automated and networked systems. Most of this program targets internal governmental operations and will not directly affect the public. Secondary effects will occur. Such effects include Government systems becoming more secure and less vulnerable to attack. This will provide added privacy for personal records that exist in Government systems. The implementation of Federal Public Key Infrastructure (PKI) and electronic signatures on federal electronic mail will also affect the public. This new process will encourage private citizens to obtain credentials that will certify their identity to federal networks. An example of this already exists within the Internal Revenue Service (IRS). At tax time, the IRS sends out a personalized identification number (PIN) that is associated with your name and social security number that allows individuals to electronically file their federal income tax returns.

Program 2 is more active than program 1 in that it implements several key initiatives. First it establishes the National Security Incident Response Center (NSIRC), a collection of analysis and response centers which link detection systems in the Air Force, Navy, Army, and DOD Agencies. This program also includes the installation of detection monitors on critical DoD systems. Additionally, the Joint Task Force-Computer Network Defense (JTF-CND) will be established as a hub for intrusion detection. Other, less intrusive activities occur in this program that will help secure federal computer networks. Since this program deals mostly with securing federal systems and establishing mechanisms to promulgate information between federal entities, there is not a direct impact on the public. A secondary affect of this program will be an increase in computer security related positions both within the federal government and with contracting firms that support the government.

Program 3 addresses law enforcement issues. Included in this program is an added focus toward enforcement and detection of cyber-threats and vulnerabilities. Educational workshops are also introduced in this program as a way to educate enforcement and collection specialists on new techniques for information collection and analysis. On the surface, this program does not appear to affect the public. But it is this program that becomes one of the major concerns of privacy advocates. While the plan specifically addresses privacy issues (see program 10) the collection and analysis described here may be *perceived* as infringing on the conversations, electronic mail, and usage patterns of individuals.

Program 4 introduces the notion of Information Sharing and Analysis Centers (ISAC). These ISACs would share information among corporations and state and local governments and could receive warning information from the National Infrastructure Protection Center about threats, vulnerabilities and relevant incidents. Again this program seems innocuous; however corporations are concerned by liability issues stemming from the identification of vulnerabilities on their systems associated with consumer loss. Additionally, although the reporting process is designed to promote anonymity, several commercial firms are concerned about their proprietary information leaking to competitors through the ISAC.[7]

Program 5 directs the review of department and agency contingency plans to ensure that information warfare attacks are addressed. This program also directs the Federal Emergency Management Agency (FEMA) to modernize its emergency communications systems. This program does not directly affect the public.

Program 6 establishes research requirements and priorities needed to implement the plan and addresses the funding and creation of a system that ensures our information security technology stays abreast of changes in the overall threat to information systems. In an effort to accomplish this, program 6 directs that conferences on major research and development (R&D) priorities be held with industry, academic, and government experts. These conferences will enable the public to participate in setting priorities and will encourage private industry support for research and development efforts.

Program 7 tackles the long-term problem of highly qualified information security personnel. Government employers are experiencing a severe shortage of qualified personnel in the information specialty areas. Regardless of the reasons for the shortage, this portion of the plan describes an outreach program to universities and other educational institutions that would establish partnerships in education between these organizations and the government. This outreach effort includes funding for scholarships in exchange for government service, funding for the preparation of instructors to establish and teach an information assurance curriculum, and funding for infrastructure costs to these institutions for building such a curriculum.[8] This has a definite impact upon the public. The opportunities that may be created for educational and employment prospects are encouraging.

Program 8 provides for an information awareness campaign to be conducted to educate the American public about the threats to our cyber-infrastructure. This includes the creation of a Cyber-citizens program for school children, creation of a public-private "Partnership for Critical Infrastructure Security," and mandatory cyber-security awareness briefings to all federal government personnel with access to sensitive information systems.[9] Again, this will impact the public in several ways; by raising overall public awareness, by reaching out and touching children in their schools, and by having a series of public service commercials appear during highly rated television shows.

Program 9 recognizes that specific legislation may be needed to regulate new technologies and deal with this new threat. While no determination has been made regarding specific legislation, a reexamination of privacy laws has been initiated to ensure that current legislation is sufficient to allow implementation of this plan. The potential for this program to impact the public is great as Congress changes and adapts laws to prepare the nation for possible attempts to subvert the computer and network infrastructures that control so many of the nation's vital systems.

Program 10 speaks to the issue of privacy for citizens, protection of civil liberties, and protection of proprietary information of companies. This program calls for an annual review of the plan by the National Infrastructure Assurance Council to ensure that these rights and liberties are not violated.[10] The impact on the public from this program should be minimal unless this program fails.

INDUSTRY PARTICIPATION

Infrastructure protection cannot be accomplished without the full cooperation of commercial industry. This section examines the role of commercial industry in the protection efforts.

Program 4 introduces the notion of Information Sharing Analysis Centers. These centers will be administered and supported by industry participants. An ISAC will be set-up for each sector and will interface with the National Infrastructure Protection Center to communicate vulnerabilities throughout the infrastructure community. Each ISAC participant will receive warnings and notifications about viruses, threats, and vulnerabilities that may affect their systems. Each ISAC participant will help fund the overall organization. Other tasks that the ISAC could perform are coordination of Research and Development efforts unique to the industry, examination of industry-wide vulnerabilities and dependencies, and development of employee education and awareness programs about information security/assurance and other employee training programs. To date, two ISACs have been established: The Banking and Finance Sector ISAC, and the New Mexico Critical Infrastructure Assurance Council.

The Banking and Finance sector ISAC was established on 1 October 1999 and is designed to facilitate sharing of information in the financial services industry. Membership is open to all members of recognized financial services organizations. Currently, twelve organizations representing both private and public interests have signed letters of intent confirming their interest to participate in the center. The center, which is managed by a private contractor, is fully funded by participating organizations.

The New Mexico Critical Infrastructure Assurance Council is a cooperative, private and public sector enterprise founded initially to further the exchange of information among the business community, industry, educational institutions, the Federal Bureau of Investigation (FBI), New Mexico State government, and other Federal, state, and local agencies. This exchange of information ensures the protection of the critical infrastructure in New Mexico. As the first and only all-volunteer statewide organization in the U.S., it serves as a prototype for similar organizations. Currently this organization has recruited thirty-six organizations, both public and private. It operates using a working group format to address each sector of the infrastructure (utilities, banking and finance, transportation, emergency management, emergency and government services, Information Sharing and Analysis Center, and management operations).

In Ohio, the FBI established a prototype communications network called InfraGard for the ISACs. InfraGard is a cooperative effort between individual companies in private industry and the FBI to share information with each other and the government as it pertains to computer espionage and sabotage. As of December 1999, at least fifty companies have joined the inaugural InfraGard chapters in Ohio and Indiana.

Program 6, as well as Program 4, addresses research and development efforts both in the government and within industry. The government's Office of Science and Technology Policy (OSTP) will schedule and administer various conferences with industry and academia to establish major research and development priorities and to eliminate redundancy and maximizing funding. These conferences are being held annually. The first one was held in September 1999.

Program 7 is primarily surveys the government to determine the number of people needed, and the required skills necessary, to implement the information security/assurance tasks. This program also implements new programs, like pay incentive programs for information security/assurance technicians, which will become available to government employers to provide skilled personnel to fill government vacancies resulting in a pool of skilled technicians that will be available to both government and industry. This program provides specific funds for post secondary educational institutions to set up and conduct information assurance specific courses. This program also provides scholarships in exchange for government service.

Program 10 strives to ensure that any information that is shared through the ISAC structure or directly with the NIPC is treated as proprietary and private information and that this information is kept private in accordance with the existing laws and policies of the U.S.

FEDERAL BUDGET ISSUES

This section examines the federal budget to determine the feasibility of implementing the federal plan.

The President's fiscal year 2000 budget request included $2.849 billion for critical infrastructure protection, computer security, and domestic preparedness against weapon of mass destruction attacks. The budget also proposes $7.162 billion for conventional counter-terrorism security programs. From these requests, $1.464 billion has been identified to support critical infrastructure and computer security. This represents a 40% increase in the past two budget years since the President established the Critical Infrastructure Protection Commission. While much of the budget will be spent on administering the programs, here are some of the major highlights of the budget line items:

- Critical infrastructure applied research: $500 million
- Intrusion and detection systems: In addition to providing ongoing Department of Defense funding, $2 million will be spent to design and evaluate a similar system for other federal agencies.
- Information Sharing and Analysis Centers: $8 million.
- Cyber Corps: $16.9 million
- Development of Federal Intrusion Detection Network (FIDNET): $8.4 million.
- Treasury Department's Public Key Infrastructure projects: $7 million

While the President did not receive all of the funding he requested in the Fiscal Year 2000 budget, a supplemental budget request has been prepared which asks for an additional $39 million to fund many of the efforts described above.[11]

MILITARY POSTURE

The issue of Infrastructure Protection would not be complete without taking a brief look at the military to see what their approach is to this issue.

The Department of Defense is scrambling to ensure that critical infrastructures are protected. To this end, many studies have been commissioned to determine exactly how the department should approach the task. One such study, "The Reserve Component Employment Study 2005,"[12] which was initiated in April 1998 at the request of Secretary of Defense Cohen, concluded that the Reserve forces are well suited to homeland defense missions. The study calls for the creation of a new reserve cyber-defense unit consisting of reservists with information technology skills who could perform their duties, when activated, from dispersed locations rather than as a single consolidated unit. To accomplish their mission of protecting various critical infrastructure nodes, the soldiers in the unit would communicate from existing reserve centers and other Department of Defense facilities across the country that have access to the Secret Internet Protocol Routing Network (SIPRNET).

The Department of Defense has taken other actions, such as establishing the National Incident Response Center, the National Information Assurance Program (in partnership with the National Institute of Standards and Technology), the designation of Joint Forces Command being responsible for the mission of Homeland Defense, and the assignment of the Info war mission to Space Command. These efforts, closely coordinated, will go a long way to protecting the Defense critical infrastructure.

THE GOOD NEWS

There are many positive aspects of the National Plan. The largest benefit of the plan, that will have the most direct impact on the general public, is the implementation of Program 7 which provides for scholarships for students who wish to pursue a major in information security/assurance. This program will help financially challenged students afford the high cost of post secondary education as well as place them into a paid position upon completion of their education.

Other positive outcomes will result from implementation of the plan. Businesses and Industry will be able to provide better security for the data that resides on their systems by joining the Information Sharing and Analysis Centers for their respective business sector. These systems generally hold very personal information about their customers, clients, suppliers, and partners as well as proprietary information about product development. The more secure systems will help deter hackers from gaining access to these systems and stealing (and subsequently profiting from) data that resides on these systems. This results in savings to commercial entities that can be passed onto the consumer.

Finally, U.S. residents should not have to worry about vital services that could be affected by information attacks, whether they are nation-state sponsored, random hacker, or terrorist attacks. The mechanisms being set-up to facilitate sharing of vulnerability and warning information will make these systems more secure and therefore more difficult to penetrate without authorization.

SERIOUS CONCERNS

Along with any new plan come serious concerns that must be addressed. Many private and public organizations had access to draft versions of the National Plan and have voiced concerns over violation of privacy rights that are ensured under various laws and legislation.[13] This concern is addressed in Program 10 of the plan that deals specifically with the issue of privacy. Nonetheless, groups from outside and even within the government are concerned. Several high-ranking Government officials have indicated that a thorough review of privacy laws is being made along with a review of the Freedom of Information Act to address privacy concerns. The Freedom of Information Act is being reviewed specifically to avoid the issue of proprietary information being released as a result of a FOIA request. Officials do not believe that the FOIA will need to be changed but perhaps interpreted to allow for an exception under the law for information stored on ISAC or NIPC databases residing on the Federal Intrusion Detection Network (FIDNET). Such interpretation can be analogous to that used to protect vital Government information from being released to FOIA requesters. However, if the Executive Branch decides that such sensitive information would not be allowed on the FIDNET (even if law allows for this) than the policy will be enforced.

Several commercial firms and their attorneys have voiced concern over antitrust violations and civil liability issues. The ISAC pact calls for known vulnerabilities to be reported to the ISAC by a commercial firm for their sector and subsequently this vulnerability is passed to the NIPC. The primary concern is that, as a result of a known but unfixed vulnerability, someone whose personal data is stored on the system may suffer a violation of privacy or a real monetary loss. Many attorneys contend that this is a libelous offense that could open up the firm to civil liability suits from the public if a company knew that they had system vulnerabilities.[14] Several government attorneys are reviewing this concern and investigating the possibility of legislation that would limit the liability of companies reporting to ISACs. This would be difficult legislation to draft due to the endless number of possibilities that could occur as a result of limited liability coverage.

Several smaller firms are concerned with the cost of joining an ISAC. While larger firms can afford an annual fee of up to $15,000.00, many small firms cannot. While the fee structure for ISACs is not set in stone, creative ways to include smaller organizations need to be considered.

The Cyber Corps initiatives described under Program 7 may suffer from slow beginnings. Current recruitment policies start information technology specialists at the GS-5-7 grade. This means recruits earns approximately $20,000 - $32000 per year. Commercial firms pay much more for qualified college graduates. The Federal Government is already conducting a study of pay issues for information specialists and will address these issues in the year 2000. In addition, working for the government may not be enticing for college graduates. The attraction of the newest of the high technology systems that many commercial firms offer may dissuade many of these professionals from joining the government roll. There is some concern that Industry may "buy back" the Government scholarship obligation of graduates. As the shortage of industry professionals continues, commercial industry will find new ways to tap this critical personnel market.

Finally, concerns have been raised over where, exactly, each organization fits. The Paperwork Reduction Act of 1995 gave security oversight to the Office of Management and Budget (OMB) while the Computer Security Act of 1987 gave authority to the National Institute of Standards. Finally, in 1998, Presidential Decision Directive sixty-three created several new groups and required government agencies to secure their cyber infrastructures. All of this confusion leads one to wonder who is in charge.

CONCLUSION

Presidential Decision Directive sixty-three and the National Plan for Information Systems Protection have addressed ever growing concerns of both Government and Industry by setting out to identify and share vulnerability and security information. As a result of quick notification and quick repair of identified weaknesses, business and industry will be better protected from potential catastrophic failures or unauthorized access and/or use of critical systems. The National Plan calls for the implementation of many approaches to provide information security/assurance and to ensure that individual rights and privileges are not violated. Only time and technology will determine whether these efforts will be successful.

It has been proven time and time again that it is easier and cheaper for hackers and terrorists to prepare a successful offense against a known defender than for the guardians of our infrastructure to prepare a strong defense against an unknown attacker with unknown methods. With intrusion detection systems in place, policy and laws to support infrastructure assaults, and doctrine to lead the way for technologists, the security of the nation's cyber-infrastructure is better off than ever before. In the end, it comes down to people doing their jobs to counter the possibility of intrusions from unknown attackers who may have discovered new and unforeseen ways to penetrate our systems.

EPILOGUE

According to John Tritak, Chief of the Critical Infrastructure Assurance Office, "Protecting the nation's critical infrastructures may very well be the first national security problem that the country does not know how to solve."[15] The Government has begun the process of protection; it has organized and written the national plan and it has begun implementing the plan. Now it is Industry's turn; industry must develop sector specific plans to counter the threat to our Nation's critical infrastructure. A good step occurred on December 8, 1999 when a meeting was held between Government and Industry leaders in New York City, NT, to inaugurate the campaign to involve industry in this monumental effort. While, the outgrowth of this meeting has up to this time been sketchy at best, officials at the Critical

Infrastructure Assurance Office are optimistic that this call to action will be answered swiftly. One can only hope.

5030 Words.

ENDNOTE

[1] Presidential Decision Directive 39 (PDD-39) relates to the Federal Response Plan for domestic terrorist incidents and was signed 21 June 1995.

[2] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures", October 1997.

[3] The plan was given to the President for final signature in early December with an expected signature date before the end of the year. In fact, the plan may not be signed until January 2000.

[4] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures", October 1997.

[5] Critical Infrastructure Assurance Office, "National Plan For Information Systems Protection version 1.0 An Invitation to Dialog," 1999.

[6] Program 10 is not associated with any specific objective.

[7] John Tritack, Chief of the Critical Infrastructure Assurance Office, interview by author, 16 November 1999; conducted in the Office of the Chief, Critical Infrastructure Assurance Office.

[8] Shirley Molia, Labor Department, working at the Critical Infrastructure Assurance Office, telephone interview by author, 17 December 99.

[9] Ken Huffer, Critical Infrastructure Assurance Office, telephone interview by author, 7 December 1999.

[10] Everyone interviewed for this project echoed these sentiments.

[11] Office of Management and Budget, Budget Amendment (DRAFT), 21 September 1999.

[12] Anthony M Valletta, "Study Calls For Reserve Virtual IT Warfare Unit", Federal Computer Week, 26 July 1999, page 6.

[13] Many of the articles written, which decry these privacy issues, have been written by authors who have not seen the National Plan. The National Plan speaks to the heart of this very issue in Program 10.

[14] Tritack

[15] Tritack

BIBLIOGRAPHY

Baer, Gary. Treasury Department, telephone interview by author, 7 December 1999.

Chabinsky, Steven. Federal Bureau of Investigation, telephone interview by author, 23 December 1999.

Critical Infrastructure Assurance Office, National Plan For Information Systems Protection version 1.0 An Invitation to Dialog, 1999.

Defense Information and Electronics, "Report FBI To Expand InfraGard Cyber Security Info Sharing Effort Across U.S.," available from <http://www.fbi.gov/nipc/doc2.htm>, Internet, accessed 1 December 1999.

Fact Sheet "Protecting America's Critical Infrastructures: PDD 63," available from <http://www.fas.org/irp/offdocs/pdd-63.htm>, Internet, accessed 7 December 1999.

Federal American Scientists Intelligence Resource Program, "Presidential Decision Directives [PDD] Clinton Administration 1993 – 2000," available from <http://www.fas.org/irp/offdocs/pdd/index.html>, Internet, accessed 7 December 1999.

Frank, Diane. "Clinton Seeks $39M for Security," Federal Computer Week, 27 September 1999, page 6.

Frank, Diane. "Feds, Industry Join Forces on Info Security;" Federal Computer Week; 9 December 1999, available from <http://www.fcw.com/pubs/fcw/1999/1206/web-security-12-09-99.htm>, Internet, accessed 13 December 1999.

Frank, Diane. "GAO: IT Security Law Needed," Federal Computer Week, 18 October 1999, available from <http://www.fcw.com/pubs/fcw/1999/1018/fcw-pollaw-10-18-99.html>, Internet, accessed 21 October 1999.

Gaffney, Edward. Defense Investigative Service working at the Critical Infrastructure Assurance Office, telephone interview by author, 17 December 99.

Huffer, Ken. Critical Infrastructure Assurance Office, telephone interview by author, 7 December 1999.

Maynard, Terry, Chief, Analysis & Warning Section, National Infrastructure Protection Center, Implementing PDD-63: NIPC Progress and Plans; 19 November 1998, available from <http://www.fbi.gov/nipc/Impdd-63.htm>, Internet, accessed 1 December 1999.

Molia, Shirley, Labor Department, working at the Critical Infrastructure Assurance Office, telephone interview by author, 17 December 99.

Office of Management and Budget, Budget Amendment (DRAFT), 21 September 1999.

President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, October 1997.

The Clinton Administration, “The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,” May 22, 1998, available from <http://www.fas.org/irp/offdocs/paper598.htm>, Internet; accessed 7 December 1999.

The White House Office Of The Press Secretary Fact Sheet, Funding For Domestic Preparedness and critical Infrastructure Protection, available from <http://www.fbi.gov/nipc/fact2.htm>, Internet, accessed 1 December 1999.

The White House, Presidential Decision Directive/NSC-63 Subject: “Critical Infrastructure Protection”, 22 May 1998.

Tritack, John. Chief of the Critical Infrastructure Assurance Office, interview by author, 16 November 1999, conducted in the Office of the Chief, Critical Infrastructure Assurance Office.

Valletta, Anthony M. “Study Calls For Reserve Virtual IT Warfare Unit,” Federal Computer Week, July 26, 1999, page 6.

Vitas, Michael. NIPC Cyber Threat Assessment October 1999; available from <http://www.fbi.gov/pressrm/congress/nipc10-6.htm>; Internet; accessed 1 December 1999.