Assessing United States Information Assurance Policy

Response to Computer-Based Threats to National Security

by

John Frederick Stickman

A Dissertation Presented to the
FACULTY OF THE SCHOOL OF POLICY, PLANNING,
AND DEVELOPMENT
UNIVERSITY OF SOUTHERN CALIFORNIA
In Partial Fulfillment of the
Requirements for the Degree
DOCTOR OF PUBLIC ADMINISTRATION

May 2001

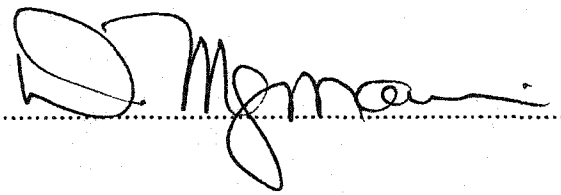
UNIVERSITY OF SOUTHERN CALIFORNIA
SCHOOL OF POLICY, PLANNING, AND DEVELOPMENT
UNIVERSITY PARK
LOS ANGELES, CALIFORNIA 90089

This dissertation, written by

John Frederick Stickman

under the direction of his Dissertation Committee, and approved by all its members, has been presented to and accepted by the Faculty of the School of Policy, Planning, and Development, in partial fulfillment of requirements for the degree of

DOCTOR OF PUBLIC ADMINISTRATION



Dean

Date 3-28-01

DISSERTATION COMMITTEE

Chester A. Newland

Chairperson

DEDICATION

This work is dedicated to my family: to my dear wife, Tina, who good naturedly put up with my years of procrastination and false-starts, never wavering in her support or her love for me; and, finally, to my loving children Johnny, Matthew, Katie, Joey, and Brittany, lights of my life and reason for my being; to my mother, Dr. Barbara R. Brown, who is the source of my intellectual passions; and to my father, Jack F. Stickman, who encouraged me during my years of intellectual "wanderings" and life's "interruptions" to get on with it and finish the project--my thanks to you all.

ACKNOWLEDGEMENTS

I wish to express my profound thanks to the staff and faculty at the Sacramento Center of the University of Southern California's School of Policy, Planning, and Development for their help in making this dream a reality. I especially wish to acknowledge my long-suffering Dissertation Committee for their patience, their guidance and for encouragement they afforded me during this very long and difficult journey.

To my fourth and final Committee Chair, Dr. Chester Newland, I thank you for your inspirational scholarliness, your gentile toughness, and for setting me a high standard to try to emulate. I certainly never would have completed this work without your help and Dutch Uncle proddings. To my friend and mentor, Dr. John Kirlin, my first dissertation chair, thanks for scholarly guidance, process support, and infinite patience in putting up with my many years of procrastinating over this project. I also express my profound thanks and appreciation to my friend and advisor, Dr. Jeffrey Chapman, my second dissertation chair, for his years of invaluable friendship, advice, and very, very patient perseverance on my behalf. Finally, thanks to Dr. Ross Clayton, who stepped in at the 11th hour as my third committee chair and who was instrumental in helping me sort through the chaff and to focus on the finish line. Without his invaluable and patient

guidance, I could never have finished this project. I wish I had been smart enough to seek his advice years ago.

I also wish to thank my employer, TRW, Inc., for the many years of encouragement and financial support in helping me to attain this goal. This was only possible through the personal attention afforded me over the years by Mr. Pat O'Malley, Senior Engineer, TRW; Dr. Robert Goldstein, Deputy Program Manager, SBIRS PDRR; Mr. Jim Apple, Director, TRW's Systems Development Operations; Mr. Douglas Pell, Deputy Director, TRW's Systems Development Operations; Col. Daniel B. Hutchison (USAF, Ret), Deputy Program Manager, SBIRS PDRR, TRW; Lt Gen Patrick P. Caruana, (USAF, Ret), Program Manager and TRW Vice President, SBIRS Low PDRR; Mr. Jack R. Distaso, Vice President and Deputy General Manager, Systems & Integration Technologies Group; Dr. Kurt W. Simon, Vice President and General Manager, TRW Data Technologies Division; BGen Earl S. "Van" Van Inwegen (USAF, Ret.), Director, TRW Air Force C4 Systems Organization; Mr. Joesph Martin, Ground Systems LOB Manger, Air Force C4 Systems; Mr. Steven Patay, Director, TRW Information Systems and Integrated Solutions Organization; Mr. Terry Savage, Director, TRW CALS/EDI Program Office; and Mr. Harry Luettchau, Systems Manager, TRW Manufacturing Division. Without their help and encouragement over the years, I would never have finally finished this project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY OF KEY TERMS

The Information Age and the Information Assurance subject area has spawned a variety of specialized terms, an understanding of which is essential to the reading of this study. The following is a glossary of those terms as they are defined and used in this dissertation.

Access Control -- physical and software system controls, such as passwords and encryption devices, and administrative controls, such as compartmentalization, segregation, and security screening intended to enhance the confidentiality, integrity, and availability of information by identifying and authenticating data and users.

Asymmetric-key Cryptography -- also known as public-key cryptography, a data protection scheme based upon a 1970s mathematical discovery that pairs of numbers exist, such that data encrypted with one member of a pair can only be decrypted by the other member of the pair, and by no other means. Anyone holding the first number, or public key, may encrypt data, but only the holder of the second number, the private key, can decrypt it. Asymmetric encryption is much slower than symmetric-key encryption and is therefore impractical for use in encrypting large amounts of data.

Authentication -- method of confirming the identity of a sender or receiver of electronic messages through the use of on-line digital technologies (e.g., signatures, addresses, automatic acknowledgements).

Backdoor -- relating to computer software engineering, a backdoor is a mechanism through which access to a computer or network system can be obtained by by-passing access securities through the use of a secret code embedded within the computer, usually by the software engineer who wrote the original program.

BIT -- industry accepted contraction of the words "binary digit." A digital bit is either a "1" or "0," representing an "on" or "off" electrical pulse. All digital information is represented as some combination of 1s and 0s. The term BIT was coined in 1946 by John Tukey, one of the nation's premier statisticians, while conducting research at ATT's Bell Laboratories. Twelve years later, Tukey coined the term "software" to describe the programs on which electronic calculators ran, first using it in a 1958 article he wrote for *American Mathematical Monthly.*

Critical Asset -- an asset that supports the national security, national economic security, and/or critical public health and safety activities.

Critical Infrastructures -- a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce a continuos flow of essential goods and services. Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP), tasking it with assessing vulnerabilities and threats to eight named critical infrastructures: transportation; oil and gas production and storage; water supply; emergency services; government

services; banking and finance; electrical power; and, telecommunications, including information and communications.

Critical Infrastructure Protection (CIP) -- policy-making and implementation associated with protecting and defending United States' critical infrastructures from physical and cyber attack.

Cryptography -- the science of transforming data through the application of mathematical algorithms making the data interpretable only by authorized persons having access to the cryptographic algorithm's mathematical key.

Defense Information Infrastructure (DII) -- domain comprising the collection of interconnected networks and information services that support the United States Department of Defense and defense community.

Domestic Terrorism -- terrorism originating in or targeting people or property within the United States.

Firewall -- an access control mechanism that acts as a barrier between two or more segments of a networked Information Technology (IT) architecture.

Global Information Infrastructure (GII) -- domain comprising the collection of interconnected networks and information services that supports global electronic commerce and the world-wide public/private electronic information exchange.

Information Age (IA) -- Third Age of Humankind beginning in 1955 with the invention of the microprocessor; the revolution in real-time computational capability facilitated by the invention of the microprocessor, catalyzing a fundamental paradigm shift in the basic infrastructure underpinnings of the global society.

Information Technology (IT) -- essential microprocessor based, information processing capabilities facilitating the Information Age.

Information Processing Technology -- the application of rapidly accelerating trends in microprocessor computational capabilities to permit the processing, collating, and real-time analysis of vast quantities of input (sensor) data.

Infrastructure Assurance (IA) -- a continuous process improvement in five general areas, the goal of which is to ensure uninterrupted access and use of the nation's critical information infrastructure. These areas are: policy formulation; prevention and mitigation; operational warning; incident management; and, consequence management.

Integrity -- the state of or process for guaranteeing that electronic data and messages have not been modified since their origin.

International Terrorism -- terrorism involving citizens or the territory of more than one country.

Intrusion Detection -- the process for analyzing networks or information systems to identify signs or indications of unauthorized access, attacks, or attempted attacks from outside the system boundaries.

Intrusion Detection System (IDS) -- software based capability used to monitor and analyze user and system activity, assess the integrity of critical systems and data files, identify activity patterns indicative of an unauthorized intrusion, perform statistical analyses to detect abnormal behavior, and alert system management to behavior which violates system security policy.

National Information Infrastructure (NII) -- domain comprising the collection of interconnected networks and information services that supports United States electronic commerce and the United States' public/private electronic information exchange.

Nonrepudiation -- computer network system accountability service that prevents the originator of a message from denying authorship at a later date.

Precision Guided Weapons (PGWs) -- incorporation of enabling electronics and guidance into conventional weapons to enhance their accuracy and lethality by factors of magnitude over equivalent conventional weapons. The Revolution in Military Affairs (RMA) associated with PGWs involves both their technical evolution as well as the means to produce PGWs cost effectively to facilitate their mass application in warfare.

Public Key Encryption (PKE) -- also called asymmetric-key encryption. Use of unique pairs of numbers such that data encrypted by one number can only be de-encrypted through the use of the second, unique number. The number made known to the public is called the public key; the number kept secret is known as the private key. The numbers used are large enough to make it extremely difficult to determine the second number by knowing the first. This allows the owner of a key pair to distribute the public key widely so long as the private key is kept secret. The most widely employed of the asymmetric encryption algorithms, the RSA algorithm was named for the three individuals (Rivest, Shamir, and Adelman) who discovered it:

Terrorism -- the premeditated, politically motivated violence perpetrated against predominantly noncombatant targets by networked, government-sponsored or subnational groups, non-governmental organizations (NGOs), clandestine agents or individuals, usually intended to generate political leverage or influence an audience.

Terrorist Group -- an organized group, consisting of more than one hierarchically ordered, significant subgroup, which practices terrorism to achieve the group's political goals.

Threat -- any circumstance or event that has the potential for harming a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment.

Vulnerability Assessment -- an examination of the ability of a system or application to withstand assault through the identification of weaknesses that could be exploited and the analysis of the effectiveness of additional security measures in protecting information resources from attack.

ABSTRACT

ASSESSING UNITED STATES INFORMATION ASSURANCE POLICY RESPONSE TO COMPUTER-BASED THREATS TO NATIONAL SECURITY

The Information Age profoundly affects United States military planning and national security administration. Information Operations employed during 1991's Gulf War demonstrated the asymmetric advantages of the informationally enabled over the informationally inferior. The absence of a coherent Information Assurance policy leaves United States critical information infrastructures vulnerable to similar information warfare attack.

To analyze United States' Information Assurance policy, this dissertation draws upon decision-making, organizational process, rational choice, and language-based social construction literature in developing the Policy as an Incremental Evolutionary Spiral (PIES) conceptual framework. PIES maps policy making as interdependent, incremental steps evolving through four stages (Goals/Objectives Analysis, Functional/ Requirements Analyses, Alternatives Analyses/Selection, and Validation/ Execution) within seven lifecycle phases (Conceptualization, Promotion, Initialization, Implementation, Sustainment, Exit/Termination, and Post Analysis).

Six, off-setting decisional vectors (problems, politics, participants, process, language/cognition, and rational choice) exert dynamic tension on

the model's decision cycles. These vectors are drawn from decision models by Allison (Rational Actor, Organizational Process, and Governmental Politics), March, Cohen, and Olsen (Garbage Can), Kingdon (Streams and Widows), Kirlin (Language-based Social Construction), and Raiffe and Kenny (Value-based Rational Choice).

This research employs a case study/participant-observer methodology and the PIES framework to analyze Clinton Administration policy. The results suggest that Information Assurance policy makers exhibit a predictable decision-making pathology: in the presence of technical uncertainty and causal risk, the decision makers' behavior reinforces the policy status quo through organizational, procedural, and statutory means. Policy gate keepers "buy" essential time for subject-matter specialists to coalesce, study policy-specific phenomena, and offer recommendations to the decision maker.

High-risk, high-technology national security policy is evolved by a select few. The professional bureaucracy, policy entrepreneurs, and key administrative appointees play minor roles in this process. Extraordinary reliance is instead vested in elite subject-matter experts from industry.

In the absence of focusing events, technical uncertainty and risk create opportunities for policy decision deferrals, rationalized as "bad decision" cost avoidances. Policy stagnation, or paralysis, results. Chief Executives overcome this policy inertia through direct policy interventions. Additional research is warranted to study this phenomenon.

CHAPTER ONE

INTRODUCTION, PROBLEM STATEMENT, AND CHAPTER PREVIEWS

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

The Information Age presages a true revolution in societal and military affairs, as the global society wrestles with what Alvin Toffler coined the "Third Wave" of fundamental change to human civilization.[1] The Information Age has profoundly affected United States' military planning and national security administration. The 1991 Gulf War, the first Information Age conflict, demonstrated the asymmetric advantages of an informationally enabled military over an informationally inferior one. The rapid and near total defeat of a modern, well-equipped and numerically superior Iraqi military by a numerically inferior, but informationally enabled coalition force, led by the United States, serves as striking testimony to the power of Information Technology applied to the modern battlespace.[2]

The extraordinary strategic advantage demonstrated by the United States during the Gulf War was made possible through the use of Information Technology. However, the euphoria accompanying the stunning victory in the Gulf War was tempered by a growing recognition that the United States lacks a coherent Information Assurance policy to protect its own Information Technology-based, critical national infrastructures. Such an absence leaves

the United States' information infrastructure vulnerable to Strategic Information Warfare (SIW) attack and the consequent disruption of essential societal services on a national or even global scale.

In the United States, the expansive growth and integration of interoperable computer-controlled information and communications systems form the foundation of the nation's Information Age-based economic vitality and quality of life. This information and communication systems infrastructure, comprised of the Public Telecommunications Network (PTN), the Internet, and millions of interconnected computers in private, commercial, academic, and government service, creates a virtual "electronic backbone," upon which all essential information and control services within the United States depend, i.e., transportation, energy production and storage, water, emergency services, government services, banking and finance, electrical power, and telecommunications.

This unique set of interconnected infrastructures creates an entirely new dimension of strategic vulnerability and an Information Age challenge to the national security of the United States. As the President's Commission on Critical Infrastructure Protection stated in its 13 October 1997 report to President William J. Clinton:

> The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. The interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.[3]

The evolution of an effective Information Assurance policy is wholly dependent on the policy-making process of the United States Federal Government. The pathology of decision making within the administrative organs of the Federal Government is key to understanding and assessing the adequacy of national security policy-making behavior, catalyzed by Information Technology (IT) and the advent of Strategic Information Warfare (SIW).

Building upon the richness of Decision Theory, Organizational Theory, Administrative Behavior, Language-based Social Construction, Systems Engineering, and Rational Choice Theory, and in concert with the researcher's experience as a participant–observer within national security administration, this study introduces the Policy as an Incremental Evolutionary Spiral (PIES) model as a conceptual framework for the analysis and evolution of Information Assurance policy.

PROBLEM STATEMENT

This research was undertaken in recognition that the on-going Information Revolution and a growing dependence on vulnerable elements of the National Information Infrastructure (NII) are profoundly affecting the national security interests of the United States. The pervasive evolution and adoption of information technologies in most aspects of society present an entirely new type of national vulnerability and policy-making complexity to those charged with "providing for the common defense."

In the very near future, it is highly probable that the United States' defense establishment and the nation's critical infrastructure--its energy systems, telecommunications systems, financial systems, transportation systems, water and sewage treatment systems, banking and securities systems, emergency medical services--will come under a well-orchestrated and sophisticated, strategic computer-based "cyber attack" from sources with the political will and technical acumen to mount such an assault.

When this strategic attack comes, it will not be an isolated incident, nor an effort by hackers to gain notoriety through proof of their technical skills; it will instead be a carefully crafted and ruthlessly executed cyber offensive, designed to test the technical and political mettle of a future Administration.

The perpetrator of such an attack might well be a traditional nation-state or geo-political entity, but it could equally as well be one of a proliferating number of Non-Governmental Organizations (NGOs) or electronically-networked terrorist groups. The attack could also come from a growing number of disenfranchised individuals bound by a shared political affiliation, a networked electronic connection, and the intent to act in a malicious or destructive manner against the interests of the United States.

To defend against such cyber-attacks, the United States is in need of an effective, long-term Information Assurance (IA) policy, the foundation of which must include the defense of United States' critical infrastructures,

accomplished within a framework of an expanding Defense Information Infrastructure (DII), National Information Infrastructure (NII) and Global Information Infrastructure (GII).[4] Such a policy requires a careful balancing between the imperatives of Information Assurance and critical infrastructure protection and the preservation of the civil liberties guaranteed by the 1st and 4th Amendments to the United States Constitution.

This dissertation draws from the extensive decision-making and policy-choice literature to develop a framework for national security policy evaluation and evolution. In so doing, this dissertation seeks to answer the question, "How can the national security interests of the United States of America be served in an era of increasing national dependence on electronic information exchange and infrastructure?" In addressing that core issue, this dissertation posits five underlying questions:

- How has the Information Revolution affected the framework within which national security policy is developed and then evolves?
- How do policy and decision-makers frame or theorize about high-risk, technologically complex issues involving the development of national security policy?
- What effects do emerging and complex evolutionary shifts in society have on the framework of governance and the administrative institutions associated with it?

- Within the high-risk, high-technology national security policy arena, who exercises the greatest influence and leverage among policy makers and why?
- Are existing decision-making frameworks successful in determining and then addressing high-risk, complex questions of national security policy?

Using a case study/participant-observer methodology, this dissertation decomposes, then maps the evolution of United States Information Technology/Information Assurance policy during the eight years of the Clinton Administration. A policy-evaluation framework is developed through this analysis. From the results of the mapping into this policy-evaluation framework, this dissertation analyzes the case study results and applies those findings to selected research questions and associated hypotheses. Finally, the dissertation offers a summary and set of conclusions regarding the Government's Information Assurance policy, along with an assessment of the efficacy of the policy-evaluation framework developed for this study as a tool for policy analysis and decision making.

UNIT OF ANALYSIS

National Security Administration in the Information Age is the unit of analysis central to this study. It was chosen for the following five reasons:

- First, it presents an all-pervasive policy question of immediate national proportion, due to a universal employment of Information Technology within the national mainstream and critical information infrastructure;

- Second, it mandates a new policy, the weight of which is only now being felt by decision makers and national security policy makers;
- Third, Information Technology has catalyzed a significant and fundamental revolution in military affairs (RMA), altering not only the weapons of war, but the entire command and control infrastructure, war-fighting strategies, doctrine, and training of the nation's military establishment;
- Fourth, it encompasses a broad range of Information Technology issues, which, though in their infancy, have fundamentally altered the basic structural foundations of the United States and the global community; and the change dynamic is accelerating; and,
- Fifth, the nature and scope of the national security challenge presented by strategic information warfare (SIW) has significantly altered the form, charters, functions, and infrastructures of traditional institutions of government, creating much less hierarchical, more horizontal decision making and policy evolution mechanisms and organizations.

Within the unit of analysis, three case study elements were selected for detailed study. The first, Federal Information Technology Policy, examined the evolution of telecommunications technology policy during the eight years of the Clinton Administration, from 1992 through 2000. This policy evolution helped catalyze the formation of the nation's existing critical information infrastructure. It was this critical information infrastructure

foundation that facilitated the explosive growth of first the Internet and then electronic commerce in the United States between 1992 and 2000.

The second, Federal Encryption/Export Policy, examined the evolution of government policy for the control of electronic data and computer system encryption technologies and products during the Clinton Administration. Until September 1999, control of encryption technologies and products, especially their export, served as the de facto government mechanism for assuring unfettered national security and law enforcement access to electronically exchanged information. But it left unprotected the vast majority of electronic data systems the nation relies on to sustain its critical information infrastructure. In serving the need for national security and law enforcement information access, government policies placed at risk a more global imperative for secure information access and assurance.

The third, Critical Infrastructure Protection Policy, examined the government's awareness of and responsiveness to growing vulnerabilities created through the evolution of the Federal Government's encryption and telecommunications policies during the Clinton Administration years.

Taken together, these three subunits of analyses created the "whole cloth" with which the researcher evaluated the adequacy of existing decision-making theory and models for analyzing the mechanisms of national security decisions and policy making within the United States Federal Government.

MODEL ABSTRACT: A FRAMEWORK FOR ANALYZING DECISIONS WITHIN A LIFECYCLE POLICY CONSTRUCT

To analyze United States Information Assurance policy, this dissertation draws from decision-making, administrative behavior, organizational process, rational choice, system engineering and language-based social construction theory and models to develop the Policy as an Incremental Evolutionary Spiral (PIES) conceptual framework. The PIES framework is illustrated in Figure 1-1. A detailed description of its evolution, its theoretical heritage, and its application is presented in Chapter Two.

PIES models the elements of policy making as interdependent, incremental decisions evolving through four stages:

- Goals/Objectives Analysis
- Functional/Requirements Analyses
- Alternatives Analyses/Selection
- Validation/Execution

These four stages exist within seven, discrete lifecycle phases:

- Conceptualization
- Promotion
- Initialization
- Implementation
- Sustainment
- Exit/Termination

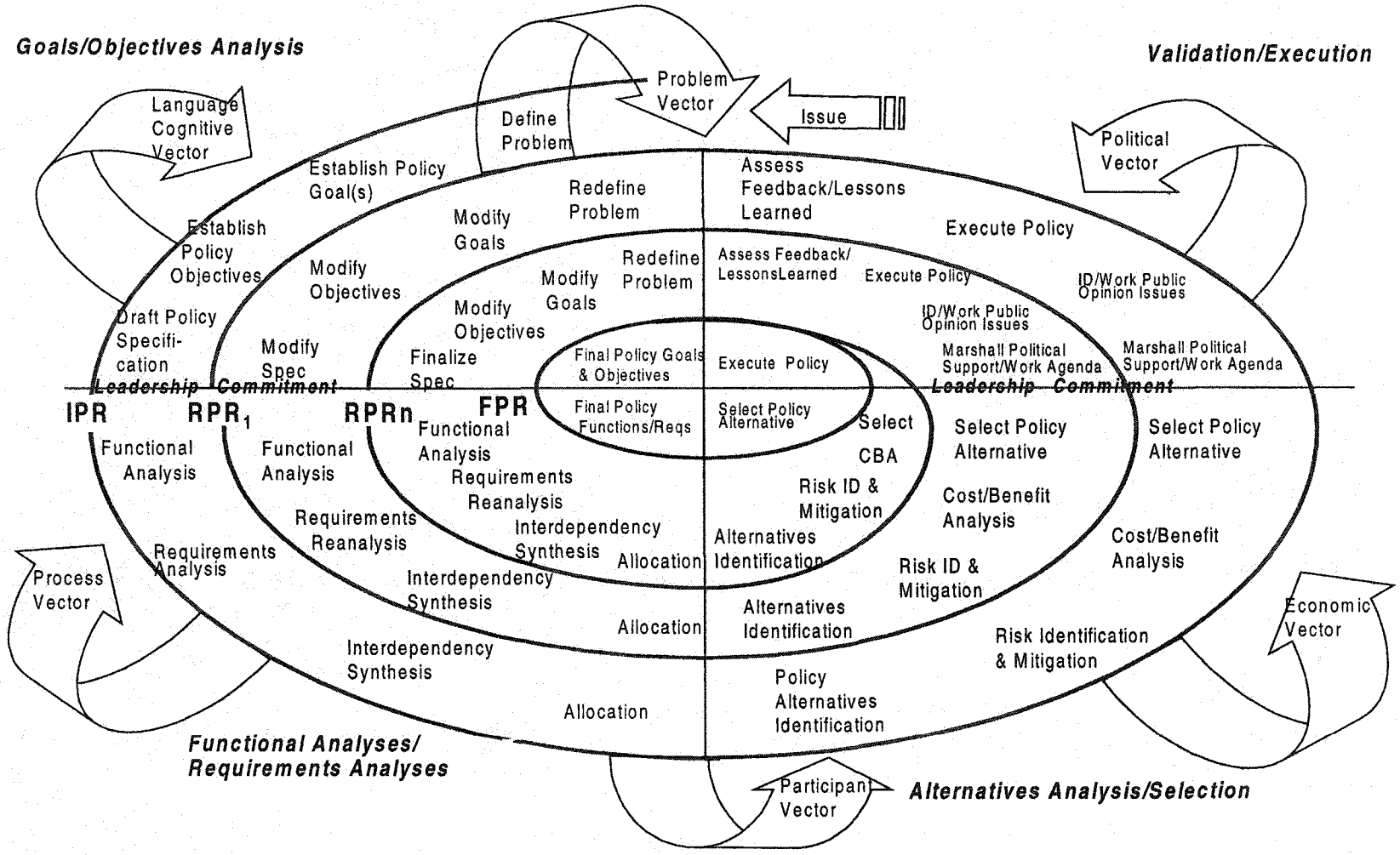


Figure 1-1: Policy as an Incremental Evolutionary Spiral (PIES) Model

- Post Analysis

Six, off-setting influence vectors exert dynamic tension on the model's decision cycles. These vectors are drawn from decision models by Allison (Rational Actor, Organizational Process, and Governmental Politics), March, Cohen, and Olsen (Garbage Can), Kingdon (Streams and Widows), Kirlin (Language-based Social Construction), Keeney and Raiffa (Rational Choice). These vectors are:

- Problems
- Politics
- Participants
- Process
- Language/Cognition
- Rational Choice

METHODOLOGY AND SOURCES OF INFORMATION

A combined case study/participant-observer method was utilized in satisfying the data collection needs of this study. Miller identifies both the case study and the participant-observer methods in his list of principal methods and techniques for social science research.[5] Yin stipulates that the case study method is an appropriate approach for the study of a contemporary subject when issues of "how" and "why" are being investigated and when the researcher lacks control over either events or phenomena.[6]

O'Sullivan and Rassel identify four criteria that must be met in determining the appropriateness of the case study method for studying social science phenomena. Those criteria are:

- The case must be contemporary, i.e., of current relevance;
- The investigator must have first-person access to the case histories and the key participants involved;
- Sources of research material must be varied. These may include interviews, direct observations, participant-observer observations, archival data, and physical artifacts;
- Source information should be cross-corroborative, i.e.; one source or information type should be supported by other sources/types of information.[7]

The Information Assurance case studied in this dissertation is contemporary, with a currency spanning less than a decade (1992-2000), and relevance is derived from contemporary national security policy and fundamental critical information infrastructure issues. As a participant at the national level in the evolution of Information Assurance national security policy, the author enjoyed direct and on-line access to the relevant case histories and first person access to many of the subject case's critical decision makers. These are documented throughout the study and compiled as source materials within the dissertation's reference section.

The sources of the research material used in this study were varied. They included interviews, direct observations, both structured and unstructured participant-observer data collections, archival data, and physical

artifacts (e.g., computer and network "sniffer" outputs, showing attempted intrusions into restricted data enclaves). The source information used was cross-corroborative.

This case was selected for study due to both its relevance and the author's personal, professional exposure to the subject matter. Kingdon, in describing the research method used to gather material for his work, purposefully limited his field of research to two focus areas (health and transportation) in which he had sufficient, personal knowledge to be conversant in the subject matter with the interviewed subject matter experts. As Kingdon relates:

> I chose to concentrate on two federal policy areas, health and transportation. I studied more than one policy domain to insure that generalizations and policy processes would not be due to the idiosyncrasies of one case or policy area, and to open up new avenues for theory building by observing contrasts. I decided not to examine more than two areas because the researcher needs to be somewhat conversant with the substantive issues involved in the area under study.[8]

For the purposes of this study, three interdependent policy areas were studied: Information Technology policy (Chapter 5), Encryption policy (Chapter 6), and Infrastructure Protection policy (Chapter 7). The author chose these three crosscutting policy areas for study because, in their integrated state, they form the functional underpinnings of Information Assurance policy.

The author's Information Assurance professional background was particularly useful in conducting this study. During the period of study, the

researcher participated in a variety of Information Assurance studies and in related project leadership roles for TRW. This afforded the author first person access to a number of company executives and industry leaders, serving or having previously served in key government positions or on Presidential Commissions and Committees cited in this study.

In addition, the author collected information and gained access to key national policy decision makers, military, government, and industry leaders through membership and participation in a variety of national advisory committees, studies, and professional associations, including:

- Aerospace Industries Association (AIA)
- National Security Industrial Association (NSIA)
- Computer-Aided Logistics Support (CALS) Industry Working Group (ISG)
  - MIL-HNDBK-59B
  - CALS Integrated Technical Interchange Service (CITIS)
- National Security Industrial Association (NSIA)
- National Defense Industrial Association (NDIA)
  - 1998 NDIA Space Summer Study for the United States Space Command
  - 1999 NDIA Information Assurance-Defense Summer Study for the United States Space Command
- American National Standards Institute (ANSI) X.12 Electronic Data Interchange (EDI) Working Group
- National Space Industrial Association (NSIA)

Key individuals interviewed are identified in Table 1-1. The basic interview form used in collecting data during these interviews is found in Figure 1-2.

Table 1-1: Key Government/Industry Sources Accessed for this Study

Source:	Title/Organization:	Contact Period:
James H. Apple	Director, Systems Development Operations, Integrated Information Technologies Division, TRW.	Interview/series of emails and private discussions, June 1998-April 2000
Lt Gen Patrick P. Caruana	Lieutenant General, USAF (Ret); former Vice Commander, USAF Space Command; Vice President and Program Manager, Space Based Infrared Low Systems, TRW.	Interview/series of emails and private discussions, Aug 1999-April 2000
Guy Copeland	Computer Sciences Corporation (CSC); Working Session Chair, Industry Executive Subcommittee (IES), NSTAC; Member, 1999 NDIA Summer Study on Information Assurance--Defense.	Interview and series of committee meetings as participant-observer, NDIA Summer Study, July-Oct 1999.
Gen Howell M. Estes III	General, USAF (Ret); former Commander in Chief, United States Space Command.	Interview, 14th Annual National Space Symposium, Broadmoor Hotel, Colorado Springs, CO, 8 April 1998; series of emails and discussions, Aug 1998-Feb 2000.
Daniel Goldin	Administrator, NASA; former Vice President and General Manager, Space and Technologies Division, TRW.	Briefing/follow-up interview, 15th Annual National Space Symposium, Broadmoor, Colorado Springs, CO, 8 April 1999.
Hon. Keith Hall	Assistant Secretary of the Air Force and Director, National Reconnaissance Office (NRO).	Briefing and follow-up interview, 14th Annual National Space Symposium, Broadmoor, Colorado Springs, CO, 8 April 1998.

Table 1-1: Key Government/Industry Sources Accessed for this Study (cont)

Source:	Title/Organization:	Contact Period:
Dr. Richard L. Haver	Former Deputy Director, Office of Naval Intelligence; Vice President and Director, Intelligence Programs, TRW Systems.	Briefing and private discussion, TRW Space Park, Building R2/1094, 17 Aug 1999.
Dr. Jeffrey Hunker	Senior Director, Critical Infrastructure Assurance, National Security Council.	Briefing and follow-up interview, Unisys Corporate Offices, Washington, D.C., 27 Oct 1999.
Col Daniel B. Hutchison	Colonel, USAF (Ret); former Deputy Director, Office of Special Projects, USAF; Deputy Program Manager, Technical, Space Based Infrared Low Systems, TRW.	Interview and series of private emails and discussions, Feb 1998-April 2000.
GEN Robert T. Marsh	General, USA (Ret); Chairman, President's Commission on Critical Infrastructure Protection (PCCIP).	Briefing/follow-up interview, Air Force Industries Association Symposium, Beverly Hilton Hotel, Beverly Hills, CA, 14 Nov 1997.
Col Robert Mihara	Colonel, USAF (Ret); former Deputy Director, Office of Special Projects, USAF; Deputy Program Manager, Operations, Space Based Infrared Low Systems, TRW.	Interview, series of private emails/ discussions, March 1999-April 2000.
Hon. Arthur L. Money	Under Secretary of Defense for Acquisition and Technology.	Briefing and follow-up interview, Air Force 50th Anniversary Expo, Las Vegas, NV, 24 April 1997.
Gen Richard Myers	General, USAF; Commander in Chief, United States Space Command.	Briefing and follow-up interview, 15th Annual National Space Symposium, Broadmoor, Colorado Springs, CO, 8 April 1999.

Table 1-1: Key Government/Industry Sources Accessed for this Study (cont)

Source:	Title/Organization:	Contact Period:
Dr. James E. Oberg	Consultant, USAF Space Command; author, *Space Power Theory.*	Interview, 14th Annual National Space Symposium, Broadmoor, Colorado Springs, CO, 8 April 1998.
Gen Bernard Randolph	General, USAF (Ret); former Commander in Chief, USAF Systems Command; Vice President, Space & Electronics, TRW.	Interviews, series of private discussions, Feb 1993-April 2000.
Gen Michael E. Ryan	General, Chief of Staff, USAF.	Briefing and follow-up interview, Air Force Industries Association Ball, Beverly Hilton, 14 Nov 1997.
ADM William O. Studeman	Admiral, USN (Ret); former Chief of Naval Intelligence; former Deputy Director, CIA; Vice President and General Manager, TRW Systems.	Interview, series of private emails/ discussions, Feb 1997-April 2000.
Dr. Alvin Toffler	Futurist, Toffler and Associates; author, *The Third Wave; War and Antiwar.*	Interview, 14th Annual National Space Symposium, Broadmoor Hotel, Colorado Springs, CO, 7 April 1998.
Brig Gen Earl S. Van Inwegen	Brigadier General, USAF (Ret), Former Director, TENCAP, USAF; Director, Air Force C4I Programs, TRW.	Interview, series of private emails/ discussions, Feb 1996-June 1998.
Dr. Daniel Wiener	Vice President, Unisys; Chair, Information Infrastructures Group (IIG), Industry Executive Subcommittee (IES), NSTAC; Chair, 1999 NDIA Summer Study on IA-Defense.	Interview/discussions as participant-observer, NDIA Summer Study, July-Oct 1999.
Richard T. Witton, Jr.	Vice President and General Manager, Integrated Information Technologies Division, TRW.	Series of interviews/emails, Feb 1997-April 2000.

Figure 1-2: Information Assurance Interview Form

Information Assurance Interview Form

Date:

Place of Interview:

Name of Subject:

Title:

Organization:

1. **What is the role the United States Government must play in "providing for the common defense" with regards to Information Assurance?**

2. **What is your/your organization's role in shaping United States Information Assurance policy?**

3. **What do you perceive as the greatest threat(s) to United States Information Assurance?**

4. **What do you perceive as the greatest vulnerabilities in United States critical information infrastructure?**

5. **How would you approach the creation of a government/private sector partnership for addressing Information Assurance challenges?**

6. **What aspects of Information Assurance policy would you like to see adopted by the United States Government?**

In addition to data collected through direct participation and first- and second-party interviews conducted for this study, a wealth of contemporary source material was extensively utilized during the research period. Original documents collected and utilized for the study include Presidential Commission and Committee reports, proposed bills, statutes, Congressional hearing records, General Accounting Office reports, Administrative agency reports, industry association studies, position papers, and briefing materials presented at national symposia. This material is presented in chronological order in Chapters Five through Seven.

A rich collection of both archival literature and recent studies were also helpful in compiling the necessary data for this study. Contemporary literature accessed included books, professional organization and association publications and journals, conference proceedings and anthologies, and doctoral dissertations. Additionally, major newspapers, national newsmagazines, transcripts of televised hearings and special topic programs, press releases, and videotapes were indispensable in the completion of this dissertation.

The Internet/World Wide Web (www) proved an invaluable source of real-time Information Assurance data. It was extensively accessed for both contemporary and archival information, ranging from data extracted from the White House homepage to information found on computer "underground" bulletin boards frequented by hackers. Table 1-2 provides a list of key websites accessed during the execution of the research phase of this study.

Table 1-2: Key Websites Accessed in the Performance of this Study

Universal Address Locator:	Description of Website:	Sponsor:
www.whitehouse.gov	Collection of current administration policy papers, press releases, information, publications, Presidential Decision Directives (PDDs) and Executive Orders (EOs). Also provides electronic access to the papers and records of the previous two administrations (Bush and Clinton).	The White House
www.house.gov	On-line electronic record of current and archival information concerning the United States House of Representatives, its members, legislation, time-phased progress of bills, Public Laws, speeches, and related data. The House search engine, THOMAS, named after President Thomas Jefferson, is an excellent tool.	United States House of Representatives
www.senate.gov	On-line electronic record of current and archival information concerning the United States Senate, its members, sponsored legislation, time-phased progress of bills, Public Laws, speeches, and related data. Currently, there is no Senate equivalent to THOMAS.	United States Senate
www.nsff.org	The website of NSA's Information Assurance Technical Framework Form (IATFF), a sponsored forum for the exchange of Information Assurance technical ideas, concepts, threats, and defenses.	National Security Agency (NSA)
www.defcon.org	DefCon is a computer underground event for hackers, held in Las Vegas Nevada. 2001 will be the ninth consecutive year for the annual event.	DefCon is a non-profit, private-sector organization.

Table 1-2: Key Websites Accessed in the Performance of this Study (cont)

Universal Address Locator:	Description of Website:	Sponsor:
www.techweb.com	Information Technology network, publishing current IT news, events, technologies, discoveries, issues, and reports. Offers search engine linkage to other websites.	CMP, a private sector web-based information source.
www.psycom.net/iwar.1.html	Created by Dr. Ivan Goldberg, this website offers a wealth of current studies, white papers, articles, position papers, and technical treatise to the general public.	Institute for the Advanced Study of Information Warfare
www.fas.org/irp/wwwinfo.html	Founded in 1945, FAS is the oldest organization dedicated to ending the worldwide arms race, achieving nuclear disarmament, and avoiding the use of nuclear weapons. The FAS website is a clearinghouse for its research.	Federation of American Scientists (FAS), a publicly funded foundation.
www.andrews.af.mil/89cg/89cs/scbi/infowar/html	USAF website, providing guide to Information Warfare, terrorism on the Internet, Cyber War concepts, and theories about Information Warfare (IW)	USAF, Andrews AFB
www.defenselink.mil	DefenseLink is the official website for the Department of Defense and Internet entry port for linking to and finding information about the United States military, it organization and assets, and its policies.	Department of Defense (DOD)
www.janes.com	Jane's is a global defense, geopolitical, transportation, and law enforcement information service. Jane's on-line service provides real-time news and technical reference information including on Information Warfare, Information Assurance, and Information Technology matters.	Jane's, Ltd.
www.dodccrp.org	Website of DOD's C4ISR Cooperative Research Program (CCRP),. Focus on improving command and control state-of-the-art; enhancing DOD's understanding of the national security implications of the Information Age.	Office of the Assistant Secretary of Defense, DOD

The application of rational choice models and Operations Research tools and techniques was a focus of study early in the course of the research design phase of this project, as one of several avenues of inquiry explored into Information Assurance policy analysis. Although exercised extensively in the early phases of the project, this methodology was abandoned after eighteen months when its results were found to be lacking in conclusiveness. Lack of success in deriving a successful approach for employing Operations Research techniques and tools to define a mathematically precise construct for modeling Information Assurance policy issues, was a primary determinate in the selection of the *case study/participant-observer* research methodology used. Appendix A provides an overview of algorithmic approaches and rational choice implications considered in the framing of this study during the research design phase.

ORGANIZATION OF THE STUDY and CHAPTER PREVIEWS

Chapter One, Introduction, establishes the research problem, unit of analysis, methodology, and conceptual framework used in this study. As summarized in this chapter, the Information Assurance national security policy issue is the unit of analysis for this dissertation, with the case study/participant-observer method as the chosen research methodology. The Policy as an Incremental Evolutionary Spiral (PIES) model is the conceptual analysis framework developed for this study.

Chapter Two, Theory Bases and Model Construction, outlines a theoretical grounding of the study within the decision-making, organizational,

administrative behavior, rational choice, system engineering, and language as social construction theory bases. Rational analysis, as defined by Dr. Herbert Simon, forms the grounding and departure point for the theory review. The impact of organizational character, values, structure, ethics, and language in the exercise of judgment in making policy decisions is examined. Policy decisions, as a reflection of organizational character and as determined by organizational history, structure, functions, values and organizational dynamics are illustrated through the works of Selznick, Ramos, Schon, David Thompson, Dennis Thompson, and Woodhouse, among others. Utility maximization in the decision process is examined through the writings of Keeney and Raiffa, Green and Shapiro, Scharpf, Shepsle and Bonchek. The models of Lindblom (policy as a set of incremental decisions) Stone (policy as a "construction" of elements), Kirlin (policy as language-dependent social constructions), March, Cohen, and Olsen ("garbage can" model) and Kingdon ("streams" and focusing events) are detailed and then combined with the structured analysis approach of System Theory and systems engineering to formulate the PIES Model, which is used in the case study analysis presented in Chapter Eight.

Chapter Three, Research Questions and Propositions, identifies the research questions and underlying propositions examined during the course of this study. Five research questions and seventeen supporting propositions are formulated for consideration in this chapter.

Chapter Four, Background--Waves of Change and the Information Age Challenge to National Security, provides a historical foundation for the

Information Assurance policy issues, providing "anchor points" from which to frame the case study analyzed in detail in Chapters Five through Seven. Chapter Four discusses the Three Ages of humankind and the specific manner by which this most recent Age, the Information Age, has fundamentally changed the fabric of society. It examines the impact that Information Technology and its applications through microprocessors, computers, and the Internet have had on both the public and private sectors. It discusses the Revolution in Military Affairs (RMA), facilitated through the application of Information Technology in military planning and battlespace execution, and how the technologies of the Information Age have created unique, new challenges and critical infrastructure vulnerabilities for United States' national security administration in the 21st Century.

Chapter Five, Information Technology Policy and Legislative Initiatives During the Clinton Administration (1993-2000), discusses the evolution of United States Federal Information Technology policy during the Clinton Administration. Clinton Administration policy decisions and legislative action by Congress taken in support of critical information infrastructure, electronic commerce and the Internet, and Information Technology are examined.

Chapter Six, Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), investigates the role played by Federal encryption policies and encryption export statutes in shaping the role of Information Technology in American society. The focus on encryption policy as

the major component of Information Assurance during the Clinton Administration is also examined.

Chapter Seven, Critical Infrastructure Protection Policy and Legislative Initiatives During the Clinton Administration (1993-2000), examines the role played by United States' critical information infrastructure as the foundation of the electronic society, focusing on efforts by Congress and the Clinton Administration to evolve an effective policy for safeguarding these national assets.

Chapter Eight, Analysis of Federal Information Assurance Policy (1993-2000) employs the Policy as an Incremental Evolutionary Spiral (PIES) model, developed in Chapter Three, to analyze each of the three case study policy elements presented in Chapters Five, Six, and Seven.

Chapter Nine, Findings, Conclusions, and Recommendations for Further Study, makes use of the background and case study data collected and presented in Chapters Four, Five, Six, and Seven, along with the Policy as an Incremental Evolutionary Spiral (SPIES) analysis results found in Chapter Eight, to address the research questions and supporting propositions introduced in Chapter Four. Chapter Nine also reflects on the purpose of the research and the unit of analysis as a preamble to a presentation of a set of policy and policy process conclusions suggested by the results of the research. Additionally, the applicability of the Policy as an Incremental Evolutionary Spiral (PIES) model as a decision- and policy-making framework and Public Administration research tool, is evaluated. Recommendations for additional research are offered in conclusion.

[1] Alvin and Heidi Toffler, *The Third Wave* (New York: William Morrow and Company, Inc., 1980), 22.

[2] James Adams, *The Next World War* (New York: Simon and Schuster, 1998), 35-51.

[3] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection,* 13 October 1997, ix.

[4] Richard N. Haass, "Paradigm Lost," *Foreign Affairs*, vol. 74, no. 1 (January/February 1995), 45.

[5] Delbert C. Miller, *Handbook of Research Design and Social Measurement,* 4th ed. (White Plains, New York: Longman, Inc., 1983), 72.

[6] Robert K. Yin, *Case Study Research: Design Methods,* 2d ed., Applied Social Research Methods Series, Vol. 5 (Thousand Oaks, CA: Sage Publications, 1994), 3-10.

[7] Elizabethann O'Sullivan and Gary R. Rassel, *Research Methods for Public Administrators* (New York: Longman, 1989), 30-34, in Ruth Gillie Krueger, *Analyzing American Social Policy: A Study of the Development of the Child Support Provisions of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996*, a Dissertation presented to the Faculty of the School of Public Administration, University of Southern California, December 1998, 56-57.

[8] John W. Kingdon, *Agendas, Alternatives, and Public Policies*, 2d ed. (New York: HarperCollins College Publishers, 1995), 231.

CHAPTER TWO

THEORY BASE AND PROBLEM ANALYSIS FRAMEWORK

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

Chapter Two chronicles the theory bases under which this study was conducted and upon which it is grounded. The chapter is organized into two sections. The first section details the rich theoretical foundations used to anchor the study. Then drawing upon this rich heritage, the second section is devoted to explaining the workings of the Policy as an Incremental Evolutionary Spiral (PIES) model, developed for use in this study as an analytical tool for modeling United States' Information Assurance policy evolved during the Clinton Administration.

BACKGROUND--SETTING THE STAGE

Central to the theoretical and operational bases for understanding how policy evolves is the issue of how government organizations function as social institutions and how individual decision makers operate within those organizational constructs. At the core of organizational existence lies the issue of choice. Change management, decision making, organizational effectiveness, organizational values, and institutional ethics all revolve around the issue of choice. How decisions are made, how choice is exercised, is core to the study of organizations and the behavior of individual

and group decision making within organizational boundaries. Managing change--making choices within a given system of values--is the central theme of organizational existence.

Opportunities for change arise through the convergence in time of three fundamental conditions. First, a problem must exist, requiring the exercise of choice to achieve an end state different than that state which currently exists. Second, one or more decisionable options must be available to modify or change the existing end state condition. Third, a group or individual must assume and exercise authority to invoke a change to the end state condition. Cleland and King stated that a group or individual assumes the decision maker role when there is dissatisfaction with the existing end state or with the prospect of a future end state, and when that individual or group possesses the desire or formal authority to initiate an action to alter the existing state.[1]

The goal of change to the existing end state, and the objectives associated with achieving that goal, provide the policy framework and criteria from which rational choices, i.e., decisions, can be made. To promote these end-state goals, the decision maker seeks or develops attainable, alternative actions for consideration. These available alternatives, bounded by quantifiable measures of risk associated with each choice, constitute the heart of any decision problem. To resolve the choice issue, the decision maker must exercise rational choice in selecting the best, possible solution from among the available, competing alternatives.[2]

RATIONALITY IN THE DECISION-MAKING PROCESS

The exercise of rational choice, i.e., decision making, exists as the binding thread through organizational and behavioral theory. Simon felt that the rationality of decisions--that is, their appropriateness for the accomplishment of specified goals--is the central concern of administrative theory. In fact, Simon went so far as to declare that decision making is the essence of management and administration.[3]

A core problem and challenge for all political societies is the proper distribution and structuring of decision-making power.[4] The goal for society is to derive the maximum aggregate utility from the exercise of decision-making power by the individuals and institutions exercising that power. Power may be vested in the elected representatives of a constitutional democracy, or closely held by a single individual under the mantel of monarchy or dictatorship. The aegis under which decision-making power is exercised, the underlying mechanisms for its derivation within the body politic, and the administrative structures for its implementation are determinants of the degree of benefit the society derives from the exercise of that power.

In the United States, the Federal Government is accorded decision-making power conferred on it by the United States Constitution. The Federal Government assumes constitutionally legitimate authority in the exercise of its decisions-making powers. The government's authority is exercised

through institutions and organizations, whose individuals are delegated decision-making authority under constitutionally prescribed conditions and limits.[5]

Origins: Classic Model and Bureaucratic Model

The premise that legitimate power is the point of origin for the development of the specific organizational structures of government and public administration, is the nexus for both the Classical Model (Luther Gulick) and the Bureaucratic Model (Max Weber) of organization. Both models stress efficiency, top-down hierarchical, authority structures, and a rational decision-making process through which higher-ranking officials draw upon the knowledge and expertise of the subordinate levels to make their decisions, while lower level decision makers are furnished the policy framework and criteria that assures conformity with policy direction set by higher authority.[6]

Despite attempts at structural integrity under the law, public sector decision making has historically been inexact at best. Nigro and Nigro characterized it as:

> A process and a result of cooperative group efforts in a public setting, affected by the shared responsibilities and interrelationships of all three branches of government, that takes place within the political process, which is affected and affects the actions of private sector groups, which also provide service to the public.[7]

Private sector decision making is differentiated from public sector decision

making in several important aspects, the principal of which is public decision making takes place within the political process, although it would be naïve to suggest that private sector organizations are internally apolitical.

Rationality: Classic Roots and Foundations

Nobel Laureate, Dr. Herbert Simon, opinioned that the decision-making process consists of three basic components: intelligence, design, and choice. By intelligence, Simon referred to the essential information gathering activities by which the environment is examined and decision points are approached; by design, Simon referred to a course of action tailored by specified goals and objectives; by choice, Simon referred to the rational selection of that course of action which promises to achieve the closest to the desired result.

Simon was concerned that the rational method at arriving at decisions did not, perhaps could not, reflect enough of the real world condition to make decision making empirically rational. Simon suggested that actual decision-making behavior falls short in at least three key ways. First, although rationality requires a complete knowledge and anticipation of the consequences that follow on each choice, rarely is knowledge of consequences anything but fragmentary. Second, the hands-on experience and expertise necessary to make the decision in the present is usually wanting. In such cases, imagination must supplement the lack of personal experience by the decision maker in attaching value to decisional choices,

despite the fact that values can only be imperfectly anticipated. Third, although rationality requires a choice among all possible alternatives, in actuality, only a very few of these possible alternatives ever becomes decisional in any given situation.[8]

Bounded rationality and satisficing behavior provided Simon the bridge between the requirements of rational decision "theory" and the decision "realities" of an imperfect world environment. Simon's "escape mechanisms" allow individuals and organizations to exist, make decisions, and survive without having the capability to operate in a purely rational manner. This concept is based on the premise that decision makers are overwhelmed and cognitively grid locked if forced to contemplate the full range of choices and consequences available through rational decision making. Therefore, the organizational decision maker operates in a much narrower, confined stream of reference, allowing decisions to be made without due consideration for all possible alternatives or their effects.

This cognitive scheme effectively places "boundaries" on the rational environment. The result of this boundedly rational decision making is a "satisficing" choice, as opposed to the rational choice model's maximization imperative. Satisficing allows the decision maker to select a choice without making the comprehensive and requisite cause/effect computations required by the rational approach. The decision maker simply makes a selection from among a set of alternatives that is "good enough," but not necessarily the value maximizing or "perfect" solution.[9]

If the administrative organization is viewed as a decision-making system, one of its fundamental goals is to ensure that individual decision making might be co-opted to more closely approximate the rationality of the system. Simon argued this can only be accomplished where individuals make choices that are guided by the interests of the organization. In its ideal type, the organization functions as an integrated decision-making system, defined to include:

> Attention directing or intelligence processes that determine the occasion of decisions, processes for discovering and designing possible courses of action, and processes for evaluating and choosing among them.[10]

In an uncertain world, the decision maker is continually challenged to strike an appropriate balance between organizational and environmental uncertainties, while exercising an imperfect judgement in making decisions upon which rest organizational and individual preferences for the consequence or outcome of the decisions made. These outcomes have intrinsic worth, with satisfactory results valued at or above an established threshold of acceptability, i.e., what could be called a stable state. Therefore, the focus of rational choice on the analysis of empirical uncertainty in decision making can be balanced through the exercise of value-based choice, which exits as the opposite equality expression in a balanced decision-making equation.

ORGANIZATIONAL VALUES, CHARACTER AND STRUCTURE AS DETERMINATES OF ORGANIZATIONAL DECISION MAKING

Organizational Character and Decision Making

Individual and organizational values are strongly influenced by organizational character. Organizational character is central to the understanding of critical decision making in organizations. Like Simon, Selznick offered that organizations exist to make rational choices and that the decisions made by organizations, or by individuals in the name of organizations they serve, are determined by four definable organizational components: organizational history (experience), character-structure, function, and organizational dynamics.[11] These attributes, Selznick argued, create an organizational identity or personality, which defines, to a predictable degree, what an organization and what individual decision makers within the organization can, or will do, in a given circumstance.

Selznick asserted that individual values and decision-making constructs are shaped by the institutional values and decision-making frameworks of the organization. Simon contended that this ideal type view, though preferred, requires a proactive effort and a high degree of maintenance on the part of the organization to affect. Nonetheless, both Simon and Selznick argued that organizational character is key to understanding how individuals and organizations make the value judgements that underlie policy decisions.

Organizational character influences, however imperfectly, the decision makers' individual value set, i.e., that which has intrinsic worth, and utility functions, i.e., usefulness preference, exercised when making decisions.

Organizational Value and Decision Making

Keeney and Raiffa suggested that the focus of decisions must be based upon individual and group values. Their premise is that the focus of classic decision making is so overwhelmingly objective as to relegate subjective preference, or value-based analysis, to an afterthought. This has the undesirable effect of skewing the decision-making analysis toward the empirical, requiring that subjective values be systematically inserted into the decision process. Decisional alternatives should be considered only after a careful assessment of core values and an articulation of specific objectives and utilities associated with each value. Keeney and Raiffa's decision-making framework focused on the assessment and qualification of subjective values and their systematic inclusion in the decision-making continuum.[12]

By first establishing a values-objectives framework, decision alternatives can be assayed against those values-objectives, then ranked according to their expected utilities. The assigned rankings ensure that the more preferred the outcome, the higher the rank ordering of the preference. Utilities are similarly scaled in a way that justifies the maximization of the expected decision-making returns, i.e., highest preference and "biggest bang for the buck" ranked first.[13] Once objective and utility functions have been

analyzed to establish outcome preferences, courses of action or alternatives can be assessed within that value framework. Informed, value-based decisions can then be made.

Organizational Structure and Judgment in the Decision-Making Process

Dr. James D. Thompson tied the concept of organizational character, as identified by Selznick and Simon, with the concept of coalition behavior and judgment. Thompson argued that decision making in organizations involves two major dimensions: a specific set of organizational beliefs concerning cause/effect relationships; and, organizational preference regarding possible outcomes of decisions made.[14] Like Selznick, Thompson believed that organizational goals are set and decisions are made affecting those goals through structured coalition behavior between members of the organization. The organization's "character," to borrow a term from Selznick, hence the basis for its decision making, is a product of the interdependent groups making up the organization.[15]

Though it is generally true for every organization that the "buck stops somewhere," it is not always an individual, but rather a group of individuals who collectively share responsibility for making a choice among alternatives. Examples might be a corporate board of directors absent their chair, or a cabinet absent the chief executive officer. Often times, decisions have to be made where several individuals share in the responsibility for making the

decision. Such a characterization is referred to as a group decision problem.[16]

Thompson suggested that decision-making strategies can be introduced to maximize the goal satisfaction of the organization in given environmental circumstances. Thompson proposed that where there is certainty regarding cause and outcome preference, a computational strategy for decision making is most appropriately employed. This strategy deals in hard tangibles: certainty, logic, and fact. Where there is certainty as to preferred outcome, but the cause/effect relationship is unclear or uncertain, Thompson introduced the concept of judgement strategy. Organizational value is introduced as a player in the choice process.

In the reverse situation where the cause/effect relationship is well understood but there is no organizational unanimity concerning preferred choice, Thompson argued in favor of what he calls a compromise strategy for decision making. Organizational politics becomes the mechanism for achieving an organizational direction for choice. Finally, Thompson suggested that there will be times when the organization faces a decision for which there is no understanding of the cause/effect relationship for the problem at hand, and neither is there certainty concerning organizational preference. In such cases, Thompson stated, the organization must rely on inspiration to make its choice. Where inspiration is not forthcoming, the organization will, when possible, attempt to avoid the problem altogether. This is defined as a decision-avoidance strategy.[17]

When organizations face uncertainty in arriving at a group decision, Raiffa and Keeney suggested that the real challenge may be in first reaching a consensus, or "crucial metadecision" (i.e., decision about how to make a decision) on selecting the process-oriented strategy by which the group decision is to be made. The prescriptive solution requires first obtaining each individual's preferences of the available alternatives, then combining them in some reasonable manner to achieve the group's preferences. With this as a decision-making framework, the essence of the group's metadecision is how to equitably integrate each individual's preferences.[18]

Value Judgment and Institutional Ethics in the Decision Process

Thompson's, Keeney's, and Raiffa's orientation toward values and value judgment provides an appropriate linkage for the work of Alberto Guerreiro Ramos. Ramos contended that the dominant factor in modern man's existence is the conflict between formal rationality and substantive rationality and that in a society whose primary focus is markets, substantive rationality takes a back seat to formal rationality. As a result, society becomes valueless and stagnant. Decisions are based on expediency in satisfying the goals of the organizational markets.[19]

In expanding upon the work of Ramos, Dennis Thompson examined issues raised by Ramos in questioning the possibility of administrative ethics. Thompson contended that the most serious objections to administrative ethics arise from two common conceptions concerning the role of individuals

in organizations.[20] The first, the ethic of neutrality, portrays the ideal administrator as a completely reliable instrument of the goals of the organization, never interjecting personal values in the process of furthering the organization's goals. The second, the ethic of structure, stipulates that even if an administrator is permitted to exercise some scope of moral judgment in the exercise of his or her duties, he cannot be held morally responsible for the decisions and policies of the organization served. Moral judgment presupposes moral agency. Personal moral responsibility may only extend to those specific duties for which an individual can be held personally liable.[21]

Though organizational existence may create decision-making patterns of behavior that are predictable, Thompson argued that public figures are still accountable for their individual actions due to the broader range of ethical responsibility that public office carries with it. While Thompson may not have claimed to have a workable plan for institutionalizing administrative ethics in public sector decision making, he successfully argued the point that understanding how ethics might be employed in the exercise of choice may be an initial step in that direction.

Incrementalism: The Step-by-Step Approach to Decision Making

Lindblom is the originator of a most appropriate term to describe organizational decision making. Lindblom's term for this process is "the science of muddling through." Formally known as the incremental approach

to decision making, Lindblom postulated that decision makers first settle on a limited objective to be achieved as a result of a decision made, followed by the outlining of the few options that are immediately available to choose from (i.e., the low hanging fruit). The decision made attempts to coalesce into one, "the choice among values and the choice among instruments for reaching values."[22]

Lindblom held that the comparison of options and the making of decisions are limited by the decision maker's past experience. For this reason, the decision maker will adopt an incremental approach to the decision making by decomposing complex decisions into their constituent elements. Using marginal analysis techniques, the decision maker makes value-based judgments on manageable components of the decision space, adding knowledge and direction to each incremental step taken in the sequence of decisions made.

Lindblom posited that although the rational model approach to decision making is the correct or ideal approach, he also contended that it is unrealistic to expect decision makers to consider every possibility when faced with making a decision. Lindblom argued that the clear-cut organizational values that are presupposed in the rational model are rarely without some element of conflict in organizational life. Because of this, Lindblom suggested that an approach that allows decisions to be made between marginal value or objective issues is more consistent with the pluralistic nature of organizations than that suggested by the rational

approach. Lindblom further suggested that incremental decision making provides the administrator with a sort of built in check and balance against making errors in judgement that cannot be easily overcome.[23]

Stone labeled this linear, incremental approach to rational decision making as the production model, in which policy is created in a fairly orderly sequence of stages, as if on an assembly line. As Stone described it, many political scientists speak of "assembling the elements" of policy. An issue is placed on the agenda and a problem gets defined. The issue transits through the legislative and executive branches of government, where alternative solutions are proposed, analyzed, selected, and either rejected or embraced. If the policy-making process is "managerially sophisticated," a means is evolved for evaluating and revising the implemented solution as time and externalities provide a more experienced perspective to the original problem, or work to fundamentally change the problem-solution set altogether.[24]

Policy Formulation as a Cycle of Functional Phases

In contrast to the incrementalists' view, a second classical approach frames the decision-making continuum as a cycle of functional phases. First formalized by Lasswell, policy formulation is viewed as a series of discrete phases in a policy lifecycle. In Kirlin's view:

> The cycle approach encourages those who use it to view policy processes as repetitive and as ideally characterized by rational choice making. Policy choices can be novel, especially in instances where a particular choice is first encountered, but it is more commonly perceived to be a sequence of successive approximations when the policy cycle approach is adopted.[25]

Laswell identified seven distinct policy phases in his lifecycle policy model: intelligence, promotion, prescription, invention, application, termination, and appraisal.[26] In like manner, Brewer characterized six separate phases of the policy lifecycle: initiation and invention, estimation, selection, implementation, evaluation, and termination.[27] May and Wildavsky labeled their six, distinctive policy phases as agenda setting, issues analysis, service delivery systems, implementation, evaluation, and termination.[28] In all three constructs, individual steps in the policy process are viewed as repetitive and predictable.

Policy and Decision Making as Language-Based Social Construction

Kirlin, concerned that both incremental and cyclical constructs of the policy lifecycle presume too great a stability in the social, political, and economic continuums, argued that change in policy, as elsewhere in human society, is not a linear process but rather discontinuous, following the random ebb and flow normal to most human activity. Kirlin opinioned that decision makers are more apt to be occupied with choices that result in only marginal adjustments in the status quo than they are to be facing major decisions and change to the exiting policy framework.[29]

But decision makers also face irregular, but inevitable, periods of environmental discontinuity, occasioned by widespread political, social, or economic instability. It is during these occurrences, Kirlin maintained, that

major shifts in policy occur which are not easily explained by the incrementalists:

> Stable-state approaches to the study of policy formation do not provide either adequate understanding of the dynamics of the periods of major change in public policy making nor appreciation of the constraints that these episodic substantial shifts in public policies place upon the subsequent choices and actions.[30]

Kirlin offered that these major shifts in policy are the consequence of a process of social construction based in language. Periods of major change in policy choice are accompanied by changes in the dominant policy language and its precise use to define new policy concepts. It therefore holds that language is both a determinate as well as an indicator of major policy change and choice opportunities.

ORGANIZATIONAL PROCESS MODELS

Rational Actors, Organizational Process, and Government Politics

A useful approach to the study of organizational decision making is through the framework of a decision-making model. Allison used this framework approach in borrowing heavily from Simon and his rationality constructs to explain the critical decisions made during the Cuban Missile Crisis of October 1962. Allison found that the Rational Actor Model, which most analysts use to explain and predict behavior and which he labeled, the Classical Model, or Model I, proved insufficient in explaining the decision

processes in the case study. Accordingly, Allison proposed two, additional constructs, based upon political analyses, to explain the action of organizations and political actors not easily explained by either the Rational Actor Model or by its associated quantitative analyses. He proposed two additional models: the Organizational Process Model, or Model II, and the Governmental (Bureaucratic) Politics Model, or Model III.[31]

In Model II, the Organizational Process Model, what Model I described as deliberate choice and decision making, Model II defines as predictable outputs of large organizations functioning according to regular patterns of behavior.[32] The unit of analysis is organizational output and the focus of attention is the perceived strengths, standard operating procedures, and operational repertoires of the organization. From this framework, predictive behavior may be identified from decision-making trends that reflect established and fixed organizational values, procedures, and processes.[33]

Model III, the Governmental (Bureaucratic) Politics Model, focuses on the internal politics of large organizations and the internal negotiations and bargaining that take place between individuals and component organizations as they jockey for beneficial position, often at the expense of sister or even parent organizations. The unit of analysis is political resultant. Decisions are made within the confines of the political reality, not the rational one.[34]

The strength of Allison's tri-model approach is that he successfully entertains decision and policy analysis from a balance of analytical and

political processes. His is the middle ground between quantitative and qualitative analyses, taking both into account and employing organizational constructs to bound the analysis space.

Garbage Cans: Problems, Solutions, Participants, and Opportunities

March, Cohen, and Olsen offer a different organizational construct for decision making in the Garbage Can Model. The garbage can process, as March, Cohen, and Olsen described it, is one in which streams of problems, solutions, participants, and choice opportunities are all dumped into a metaphoric garbage can and allowed to mix together and "ferment." Elements move from one choice opportunity to another in such a way that the nature of the decision, the time it takes, and the problems it solves all depend on a relatively complicated meshing of the available problems and solutions and the environmental demands on the decision makers.[35]

In the garbage can, March, Cohen, and Olsen posited that rational decisions are arrived at in one of three distinct ways. The first is by oversight. If a choice is activated when problems are attached to other choices and if there is energy available to make the new choice quickly, it will be made without any attention to the existing problems and with minimum time and energy. The second method is by flight. In some cases, choices are associated with problems in an imperfect matching for some period of time, until a choice more attractive to the problems' solution comes along.

Problems "leave" the former choice and bond to the "new, improved" solution, thus making it possible to make the decision. The decision resolves no new problem; the "old" problems having now attached themselves to "new" choices. The third method is by resolution. Solution choices may resolve problems after some period of time simply by working on them, i.e., the problem and the choice of solution gradually grow together and become in synch over time, as a result of adjustments for both. The length of time may vary greatly, depending on the number of problems. This is the familiar case implicit in most discussions of choice within organizations.[36]

In the Garbage Can Model, decision making becomes more a matter of a chance alignment of all requisite decision elements, as it is a conscience, deliberate act of problem solving. As March, Cohen, and Olsen themselves stated:

> It is clear that the garbage can process does not do a particularly good job of resolving problems. But it does enable choices to be made and problems sometimes to be resolved even when the organization is plagued with goal ambiguity and conflict, with poorly understood problems that wander in and out of the system, with a variable environment, and with decision makers who may have other things on their minds. This is no mean achievement.[37]

The Evolved Garbage Can: Streams, Windows, and Focusing Events

Kingdon derived much of the logical framework of his decision-making modeling to the work of March, Cohen, and Olsen and their seminal "garbage can" theory. Kingdon postulated that policy emanates from the

convergence of at least three different streams of consciousness within the body politic: a Problems Stream (Garbage Can), the Politics Stream, and the Policy Steam.

Policy is enacted when these three streams converge on some Window of Opportunity, usually created by a Focusing Event. A focusing event is an occurrence of great emotional or symbolic meaning to public opinion and the decision-making process. Given the short life-span of an agenda item and the even shorter attention span of the decision makers, policy evolution through the political process requires a great "harmonic convergence" of streams through windows of opportunity in order for policy to be adopted.

For policy to evolve to the point it can be enacted at that moment in time when the streams and policy windows align is dependent upon the co-alignment and convergence of closely held ideas and desirements of the policy specialists and stake holders into an acceptable policy alternative. Kingdon spoke of communities of policy specialists, made up of researchers, congressional staffers, planners and evaluators, academicians, interest groups, and entrepreneurs. Kingdon wrote:

> Ideas float around in such communities. Specialists have their conceptions, their vague notions of future directions, and their more specific proposals. They try out their ideas on others by going to lunch, circulating papers, publishing articles, holding hearings, presenting testimony, and drafting and pushing legislative proposals. The process often does take years.[38]

In any particular policy arena, policy specialists may be found both inside and outside of government. Their common bond is a shared concern with one particular area of policy.

Kingdon observed that the policy community operates independent of even major political events, such as changes in administration, the results of congressional elections, or pressures exerted on elected officials by their constituents. While not immune to the influences of Kingdon's political stream, the policy community operates in an arena that is independent of the political one.

Some policy communities internally operate as tightly knit entities. Policy alternatives that evolve form such tightly knit policy communities tend to reflect a unified policy view, reflecting common outlooks, orientations, and even a specialized language (see Kirlin) common to the policy community. Policy alternatives that evolve from more diverse and fragmented policy communities tend to reflect a greater diversity of opinion, begetting the potential for policy instability.[39]

RATIONAL CHOICE THEORY

The collective works of Allison, March and Olsen, and Kingdon focus upon the exercise of judgement within the political process associated with decision making. There is another, analytic side of the decision-making continuum, which concerns itself with the empirical bases for making rational choices among competing decision-making choices. The literature identifies

theories associated with utility maximization in the structure of preferences, decision making under conditions of uncertainty, and more broadly, the centrality of individuals in the explanation of collective outcomes, as members of the rational choice theory base.[40]

Green and Shapiro identified rational choice theory with the task of explaining collective decision-making outcomes, by reference to the maximizing behavior of individuals within the decision-making group.[41] This "maximizing behavior" precept originated in the work of Mancur Olson and his theory of the logic of collective action. Olson's theory evolved from observations of the behavior of individuals coalescing into interest groups to pursue collective value objectives. While many members actively work to advance the interests of the collective, others refuse to support the active membership, even when those individuals greatly value the benefit that the group action elicits. Olson wrote that these individuals will "not voluntarily make any sacrifices to help their group attain its political objectives."[42]

Olson observed that the prevailing orthodoxy of political science offered no explanation for this paradox, so he created his own theory to explain what he termed this "free rider" behavior. Olson contended that free rider behavior is characterized by individual avoidance of participation in group action, secure in the knowledge that lack of individual participation will likely have no affect on the outcome of the resultant decision, but that the individual benefit of the group action will be accrued nonetheless.[43]

Rational choice literature has generally followed Olson; many of its core tenets arise from a grounding in the individual as the basic maximizing unit.[44]

Within rational choice theory, the decision-making constructs and models upon which the mechanics of policy choice rest are predicated upon linear rationality. Linear rationality asserts that policy decisions evolve from a series of interdependent, utility-maximizing choices, made by individual decision makers acting individually or within a group, all operating from a hierarchically-ordered, goal-maximizing value set within a stable economic and political system.[45] Because rational choice theorists assume that social outcomes are the by-products of choices made by Individuals, rational choice explanations are typically formulated by reference to individual intentions.[46]

Saz and Freejohn held that the most common philosophical interpretation of rational choice theory:

> conceives it as philosophical theory wedded to a reductionist program in the social sciences, where the behavior of a social aggregation is explained in terms of the mental state (i.e., the desires and beliefs) of its component individuals and their interactions.[47]

Elster argued that rational choice explanation is predicated on the decision maker's beliefs and choice desires, which must be both rationally held and internally consistent.

> Ideally, then, a rational choice explanation of an action would satisfy three sets of requirements. First, there are three optimality conditions. The action is the best way for the agent to satisfy his desire, given his belief; the belief is the best he could form, given the evidence; the amount of evidence collected is itself optimal, given his desire. Next, there is a set of

> consistency conditions. Both the belief and desire must be free of internal contradictions. The agent must not act on a desire that, in his opinion, is less weighty than other desires, which are reasons for not performing the action. Finally, there are a set of causal conditions. The action must not only be rationalized by the desire and the belief; it must also be caused by them and, moreover, caused in the 'right way' [it must have been intended by the agent to produce the effect it in fact produced]. Two similar casual conditions are imposed on the relation between belief and evidence.[48]

In the "real world," meeting Ester's relevant optimality, consistency, and intentional conditions for each policy consideration is challenging. Despite the bar being set high, the inherent difficulty of traversing the bar is insufficient reason to abandon quantitative analysis or the analytic process in favor of a pure reliance on the qualitative analyses of the political process.

The mathematically based, predictability models that form the basis of the Operations Research discipline, encompass many of the tools of rational choice. Linear and Integer Programming, Game Theory and Decision Theory, et. al., are predicated on the core assumption of value- and utility-maximizing decision making on the part of the decision maker. Rational actors make decisions based upon individual preferences, intended to maximize the chances of obtaining value-generating results against well-ordered sets of prioritized outcomes. Within this framework, the essence of decision really becomes a study on how to integrate individual preferences into a group consensus.[49]

Rational choice theorists answer uncertainty in the decision maker's judgement or beliefs through the advent of conditional probabilities. The

calculus of conditional probability is made possible through the application of Bayes's Equilibrium Theorem (and other equilibrium theorems). The construct allows the decision maker to factor in and measure the value of "hunches," i.e., non-quantifiable knowledge factors that exist in the subconscious, but which help bound the decision space and, therefore, learning.[50]

Equilibrium theorems offer the rational decision maker a way to explore how information affects choices. It allows the decision maker to evaluate how new information affects the selection of decision alternatives. Equilibrium theorems allow the decision maker to update his or her subjective probability distribution and thus determine if a decision or strategy should be revisited.[51]

To significantly reduce the high level of statistical uncertainty induced by randomness, equilibrium probability theorems used in predicting decision outcomes assume that decision makers are rational, i.e., choices will always be made that maximize the decision maker's value-driven utility function. But even in this best of cases and even through the application of the most mathematically- sophisticated, analytical modeling tools Operations Research offers, it remains impossible to perfectly, predictively model the outcome of a complex set of interactions involving even just two, randomly-selected, decision makers.

This is not to suggest that Operations Research, i.e, the analytic process, does not have its place in the decision-making continuum.

Decision making is shaped by the dependent variables of the total public environment, or system, that it affects. Too often in both public and private decision making, decisions are made based upon an expediency driven by the urgency of the crisis at hand. The formal, quantitative decision analysis is truncated, incorporating barely enough of the independent variability of the system whole to enable a qualitative conclusion to be reached, a policy to be established, and a solution to be implemented. While the alternative chosen may very well meet the needs of the immediate, it carries with it a certain political and policy-making risk, due to the previously discussed limits on human cognitive abilities.

Those limits make it impossible, with any degree of surety, to know that the complete set of decisional interdependencies have been taken into account in the expediency of making goal- and utility-maximizing decisions. Without a comprehensive framework from which these critical dependencies may be ascertained and managed over the policy lifecycle, decision making is necessarily fraught with risk.

SYSTEMS THEORY AND SYSTEMS ENGINEERING ANALYSIS

In the search for an "ideal type" framework for making objective assessments of complex, interdependent decision making associated with policy evolution, the idea of a "systems approach," which balances the qualitative judgement of the political process with the quantitative empiricism

of the analytical process, is worthy of consideration. Systems theory offers the potential for the construction of such a framework.

Since its advent nearly fifty years ago, systems theory has evolved from a purely engineering science discipline, into a much broader focus area, encompassing both technical and engineering fields, as well as the social sciences. First evolved and studied as control theory by electrical engineers and mathematicians, system theory is integral to the study and understanding of complex systems, e.g., biological, sociological, economic, psychological, political, administrative, et. al.. Since all systems exist as sets of individual components that work together to satisfy the objectives of the collective, Systems Theory is defined as that body of conceptual abstractions and modeling constructs that attempt to describe and/or predict the behavior of components interacting as systems.[52]

The methodology used in the study of systems is systems analysis. First appearing in *Webster's New Collegiate Dictionary* in 1956, systems analysis was defined as:

> The act, process, or profession of studying an activity (as a procedure, a business, or a physiological function) typically by mathematical means in order to define its goals or purposes and to discover operations for accomplishing them most efficiently.[53]

Webster's definition remains unchanged nearly fifty years later.

Systems engineering analysis--systems analysis, for short--is a scientific process, or methodology, which can best be described in terms of its salient, problem-related elements. The process involves a

systematic examination and comparison of those alternative actions that are related to the accomplishment of some desired outcome. These alternatives are sorted and ranked on the basis of their imputed costs and the benefits to be accrued with each of their implementations. Inherent to this cost-benefit analysis is the explicit consideration of risk and uncertainty for each alternative considered. Each alternative studied assumes the sum of all of the system components, their interdependencies, and the relationship of the system to its internal and external environments, i.e., inputs, outputs, controls, and mechanisms.[54]

In December 1994, the Electronic Industries Association (EIA) published systems engineering analysis standard, EIA/IS-632. EIA/IS-632 was endorsed upon its release as the industry benchmark by the American National Standards Institute (ANSI), Aerospace Industries Association (AIA), the Department of Defense (DoD), the National Security Industrial Association (NSIA), and the National Council on Systems Engineering (NCOSE).

EIA/IS-632 traces its roots to DoD Military Standard 499, Systems Engineering (MIL-STD-499). EIA/IS-632 evolved from the unpublished version of MIL-STD-499B. When it became evident in June 1994 that the government would not release MIL-STD-499B as a military standard (a "victim" of DoD's move to commercial standards), an industry working group was formed to undertake the task of

"demilitarizing" MIL-STD-499B and releasing it to government and industry alike as a unified standard.[55]

EIA/IS-632 organizes the systems engineering method into four integrated processes, each having inputs and outputs with the external environment and a set of internal processes that govern system mechanisms and controls, along with internal component inputs, outputs, and feedback between elements. Figure 2-1 illustrates the EIA-IS 632 system engineering process.

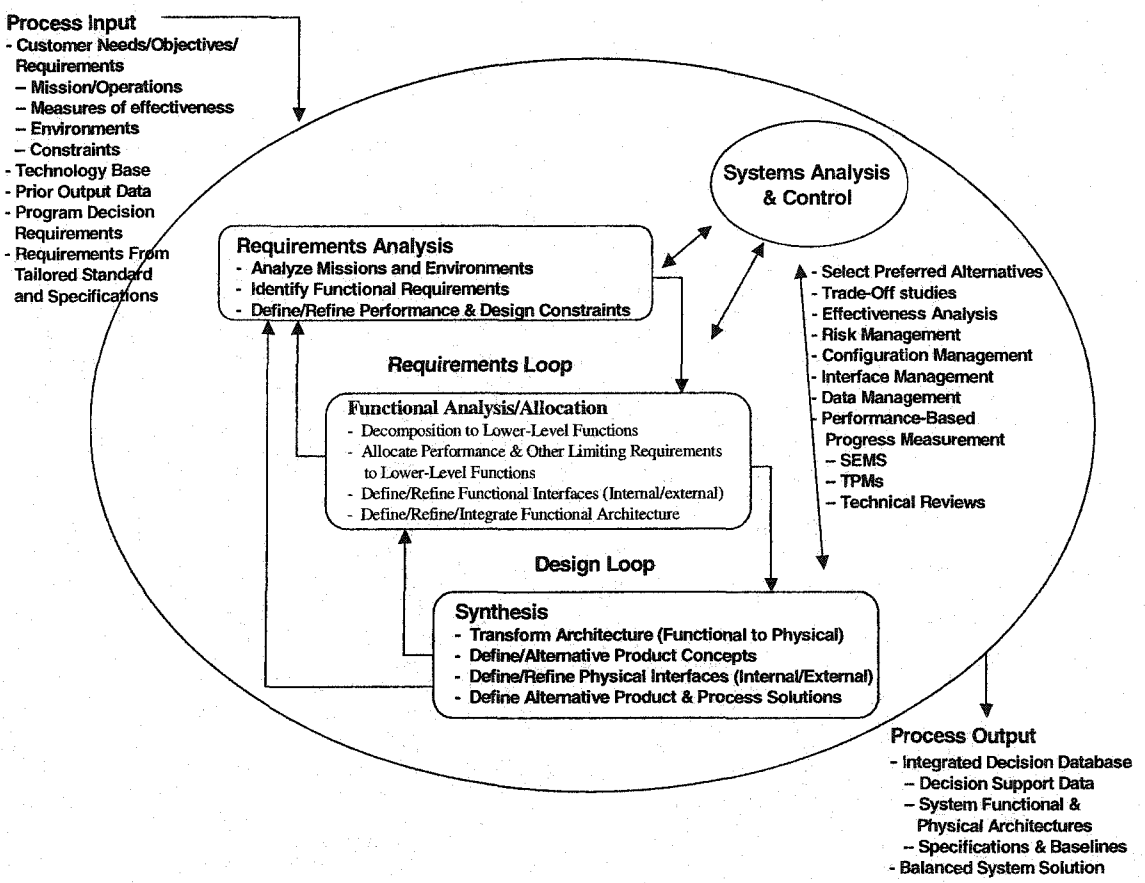


Figure 2-1: Systems Engineering Analysis Process (EIA/IS-632)[56]

The power of systems engineering analysis in decision making is that it proceeds logically within a structured context. The scientific process has the additional "virtue" of guaranteed logic and consistency, while generating results that are reproducible. The subjective, political process has no such guarantees. If one views the quantitative approach of the systems engineering process as a compliment to the qualitative and subjective political approach to decision making, nothing is lost and much may be gained by harnessing quantitative logic to the choice process.

As in most matters, acceptance of systems analysis as a decision-making tool is predicated on gaining an understanding of the language of systems engineering, i.e., the definition of its inherent terminology. Understanding is dependent on a shared interpretation of the definition of the language and cognitive constructs implicit in the system engineering methodology; what Kaplan described as a conception. Kaplan defined conception as how meaning is taken in a particular way:

> A conception "belongs" to a particular person (though, of course, others may have very similar conceptions), and it will differ, in general, from time to time. Associated with the use of a term is a concept, which may be said correspondingly to be a family of conceptions. [A] Concept may be [regarded] as impersonal and timeless, in contrast to its conceptions, since it is an abstract construction from the latter.[57]

The definition of the term systems analysis, therefore, depends on the user's frame of reference, or construction, in Kaplan's terms.

Accordingly, systems analysis is often used interchangeably in the political context with the term "policy analysis" or in the economic context with the term "cost-benefit analysis." Conceptually and for the purposes of this research, the systems analysis construction of Simon has been appropriated. According to Simon, "the power of systems analysis is in its ability to meet the essential criteria of comprehensiveness, technical sophistication, and pluralism in constructing a decision-making framework."[58]

Satisfaction of these three criteria does not ensure that correct decisions will always be made in a world of uncertainty and conflicting preferences. However, it does suggest that decisions made can be made defensible if there exists a clear audit trail from the decision to an underlying set of shared, value-based goals and objectives; if there is accountability between the set of assumptions supported and alternatives considered prior to the decision being made; if there has been a reasonable assessment of risk and due consideration for risk mitigation incorporated into the decision implementation; and if the policy issue achieves sufficient prominence on the political agenda and the requisite public support necessary for execution.

Potentially, the most significant contribution systems engineering analysis offers to the decision-making process is that it serves as a framework for Kirlin's language-based social construction, such that through this framework, systems analysis contributes to the due process demanded of our democratic institutions. Simon stated as much in writing about the

challenges associated with the anti-ballistic missile (ABM) and supersonic transport (SST) decisions of the mid-1970s:

> The struggles over the anti-ballistic missile and supersonic transport are to my mind what we might hope for in the way of informed discussion of highly technical and complex issues. This does not mean that the correct decisions were necessarily reached. I have no more infallible means for deciding that than did the disputants at the time of the debate. Honest and reasonable men could and did take either side of either question. But what distinguished these particular debates was that both sides were armed with sophisticated systems analyses based upon man-years of careful study supported by quantitative models. For this reason, it was possible for the layman, with a reasonable expenditure of time, to understand where the differences lay--which disagreements about what assumptions were responsible for the divergent conclusions reached. Moreover, for each of the decisions there was not a single analysis but several, prepared by protagonists who had different set of interests and different viewpoints.[59]

MODELS AND SIMULATIONS

The power of systems engineering analysis in decision making is that it proceeds logically within a structured context. Visibility and simplicity of understanding are core tenets of an effective decision-making framework. It is often useful to construct an abstract representation of the system and use that abstraction as a tool to empirically define, describe, and then analyze the cause and effect relationships and elemental interactions within the system. Such a model can be a very powerful analytical tool. But as Morrow admonished, "The single most important principle in modeling is simplify, simplify, simplify. Simpler models are easier for [the originator] to solve and for the reader to follow than complex models."[60]

System complexity is reflected in the number of elements that interact, the dimensions of their interactions, the elemental interdependencies, the inputs, outputs, controls, and mechanisms that define and differentiate those interactions. Gaining a complete, empirical understanding of the interdependencies exhibited by the individual components of a system allows insight into and predictability of the reaction of the system, as a whole, to both internal and external stimuli.

While the goal is simplicity, the model must also be capable of comprehensively grasping the entirety of the decision-making domain, including all its nuances and its time-phased interdependencies. It must exhibit an explanatory sophistication that ensures confidence in the decision-making process, but not such sophistication as to be indecipherable to an informed citizenry. It must be flexible in adjusting to the political vagaries of a pluralistic society. Finally, its frame of reference must be grounded in and reflective of the culture and, in the context of this dissertation, the Age, from which it originates.

Policy evolution, like any complex construct or system, is decomposable into its base elements through a rigorous requirements, functions, constraints, risks, and trade-off analyses. The literature is replete with arguments concerning the inadequacies associated with the application of quantitative analysis to the public policy decision-making realm. Many of these concerns center on the tendency for systems analysis and quantifiable

modeling, i.e., rational choice, to take on a life of their own, easily absorbing the complete resources of an organization in the effort to understand a problem. Since decisions are frequently made under extreme time pressures, critics point to systemic analyses as both too exacting and too time intensive to be of significant use in the real-time dynamic of most decision making.

Proponents of rational choice and system theory would argue that these criticisms ring hollow in light of the objective evidence and disappointing results of politically-based, decision making results manifest in many recent government policies, e.g., Iraq Policy; Somalia Policy; Kosavo Policy. In the absence of a structured, systemic analysis and resulting understanding of the interdependent relationships among decisional elements and variables, policy decisions made in the interest of expediency result in poorly framed, chaotically implemented policy.

Policy involving complex issues or which evolves over time may best be analyzed and structured within a decision model that has an inherent flexibility to accommodate the inevitable change and environmental variability over the life of the policy. The model must be structured to maintain the changing interdependency relationships of the policy elements over time, an absolutely essential component to the understanding of the complex cause-effect dynamics of policy making. The model, therefore, must exhibit both incremental and evolutionary attributes.

Complexity can be a variable that is managed successfully over time by decomposing complex decisions into structured increments. Lindblom's

incrementalism is a fair start, but fails to account for change caused by the March-Cohen-Olsen type garbage can interactions, or Kingdon's focusing events and streams fusions. Kingdon addressed the essential elements of policy change and the decision dynamic, but attributes real opportunities for change to focusing events outside the decision maker's control. Systems engineering analysis provides that essential structure for evolving decisions from among a set of achievable alternatives derived from a systemic requirements and functional analyses.

While each of the approaches discussed contribute to the understanding of the decision-making process, none of them is entirely whole. Each is lacking in some essential element(s). What is needed is a comprehensive, evolutionary construct, that allows the elements of randomness, change, and time to interact within the incremental latticework of the essential elements of policy decisions: requirements, functions, risk, cost, benefit, alternatives, agendas, execution, and lessons learned. Without an end-to-end threading, policy fails to maintain an essential consistency over time. More importantly, policy and decision makers may lose cognizance of those critical frames of reference and institutional histories that are the essential foundations of policy over an extended lifecycle.

THE POLICY AS AN INCREMENTAL EVOLUTIONARY SPIRAL (PIES) FRAMEWORK

The Policy as an Incremental Evolutionary Spiral (PIES) conceptual framework is offered as a potentially useful construction in fulfillment of the

need for an evolved, decision-making framework for policy and decision-making analysis. The model builds upon each of the decision-making constructs and models presented in this chapter. The macro-framework is an extension of the lifecycle models of Lasswell, Brewer, May and Wildavsky. It decomposes the policy process into seven lifecycle phases: Conceptualization, Promotion, Initialization, Implementation, Sustainment, Exit/Termination, and Post Analysis.

Within the macro-framework is an extrapolation from the system engineering construct found in EIA/IS-632, wherein the model decomposes each phase of the lifecycle into one of four increments (quadrants): goals/objectives analyses, functional/requirements analyses, alternatives analyses/selection, and validation/execution. Finally, within each phase, each increment of the evolving policy is integrated in a cyclical, or spiral, decision continuum, iterating as many times through the spiral as the decision maker deems necessary to ensure that the most informed decision possible is made.

PIES Lifecycle Phases

The first phase of the PIES policy lifecycle is the Conceptualization Phase. In this phase, the policy concept is developed, objectives established, alternatives studied, requirements and cost-benefit analyses made, risks and failure potential assessed and mitigated, and political and public opinion analyses undertaken. The Conceptualization Phase is followed by the

second phase, the Promotion Phase, during which the objective is securing the necessary political capital to promote the implementation of the policy proposed for execution.

The third phase of the policy lifecycle, the Initialization Phase, establishes the essential groundwork necessary for policy implementation. All decisional elements associated with requisite inter-party agreements (including treaties), resource allocations, execution planning, and contingency planning are finalized during this phase. The Initialization Phase represents the first of four execution phases within the policy lifecycle.

The fourth phase is the Implementation Phase. During this phase, the policy executables of the selected implementation alternative are put into play. The Implementation Phase represents the second of the four policy execution phases within the policy lifecycle; it is the phase wherein the actual policy initiatives are physically implemented.

The fifth phase is the Sustainment Phase. Following the Initialization and Implementation Phases, Sustainment is the third of the execution phases. Sustainment is designed to maintain the policy status quo, but will accommodate changes to the policy and its execution, as needed.

The sixth phase is the Exit/Termination Phase. This is the fourth and last of the execution phases and another critical phase, equivalent to the Initiation Phase in terms of risk. The exit strategy is conceived during the Conceptualization Phase, but modified, as necessary, with each successive stage and cycle of the policy process.

The final and seventh stage is the Post Analysis Phase. During this phase, the policy team assesses the successes and failures of the policy's lifecycle decision making, collecting "lessons learned" to better enable future executions of the process. Figure 2-2 illustrates the lifecycle phase framework of the PIES model.

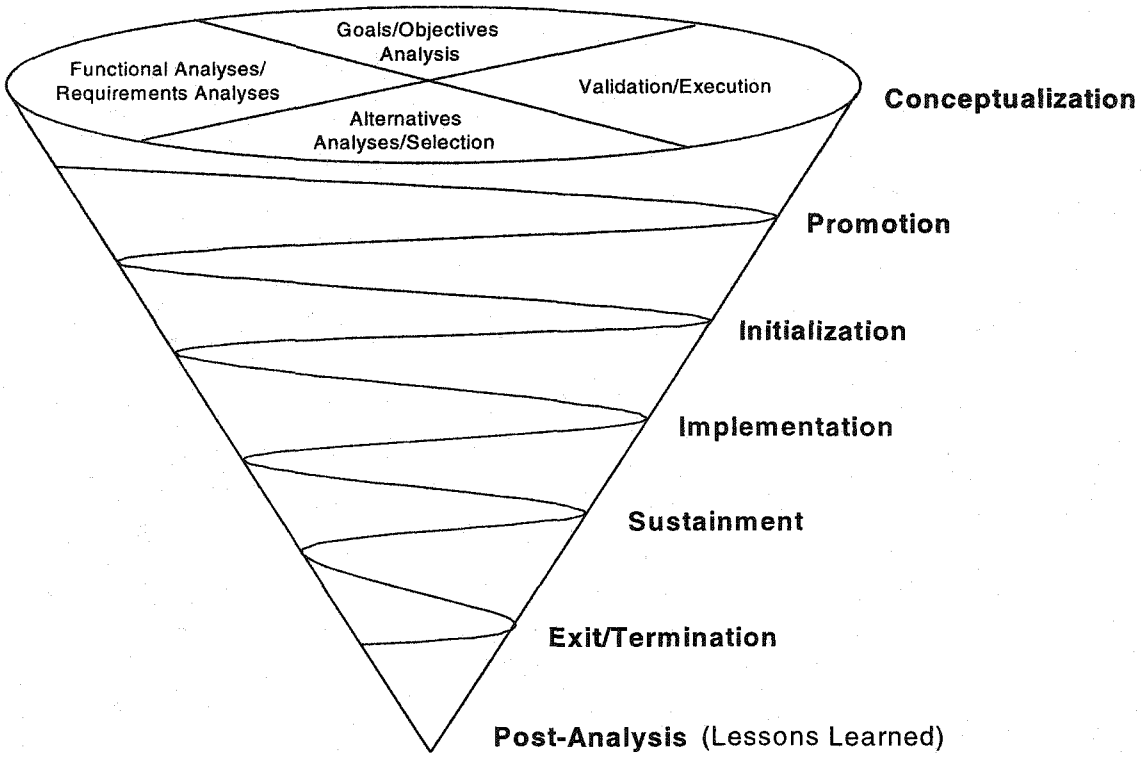


Figure 2-2: Policy as an Incremental Evolutionary Spiral (PIES)

PIES Decision Analyses Quadrants

Each lifecycle stage of the PIES model shares a common set of decision processes with each other stage. The cross-section of the model at any individual stage is divided into quadrants (see top, cross-section of

Figure 2-2). It is within these quadrants that policy evolves through a structured set of system-engineered processes.

Goals/Objectives Analysis

The first quadrant is Goals/Objectives Analysis. The objective of the activity within this quadrant is the establishment of policy objectives and goals, based upon a value-focused analysis. Value analysis is the appropriate starting point for policy evolution, as opposed to alternatives analysis. The key question to be answered is what does the decision maker hope to achieve with this policy? Value thinking is defined here as constraint-free thought. It is conceptualizing on what the organization, the society, or the individual hopes to achieve by implementing policy. Evolving a set of desirable alternatives is also constraint-free thinking. Selecting among alternatives is constrained thinking.[61]

The basic input to this decision quadrant is the identification of a decision problem. For the purposes of this dissertation, the decision problem is considered as follows: "How will the national security interests of the United States of America be preserved in a era of increasing national dependence on electronic information exchange and infrastructure?"

Within this quadrant, initial policy goals are established and an initial draft set of objectives, based upon the agreed-upon goals, is articulated and analyzed. Once the goals have been articulated, a draft analysis of the expected high-level benefits of the policy may be enunciated. With each

circuit of the model, goals, objectives, and benefits are modified based upon environmental changes and knowledge gained through exercising any of the other decisional elements in each of the four model quadrants, while factoring into this quadrant the resultant feedback. Eventually, the goals and the objectives of the policy are finalized.

Functional Analyses/Requirements Analyses

The second quadrant is Functional Analyses/Requirements Analyses. Though its notional inputs are derived from the Goals/Objectives Analyses output, feedback from the exercise of decisional elements in any of the four quadrants can drive activity within this quadrant.

Functional and requirements analyses exist in a symbiotic relationship. Requirements are objectives and design constraints that identify the boundaries for a particular solution set, i.e., in this case, a policy decision. Thus, requirements both identify needs as well as identify limits to solutions.

Requirements are manifested in functional architectures. Functional architectures are frameworks representing the synthesis of requirements into logically ordered forms. Requirements can be viewed as a "shopping list" of core capabilities that must be functionally satisfied in order to accomplish a goal. The functional analysis process serves to allocate requirements into discrete, executable functions.[62]

In the PIES model, requirements and functional analyses are iterative. In fact, PIES analyzes functions first and then applies the requirements

analyses to refine the application of alternative functional architectures. By establishing a functional need and framework first, requirements serve as capabilities functions must meet. In the inverse, requirements dictate function, potentially limiting the choice of available solutions.

Once a functional architecture is established, identified functional requirements are analyzed to ascertain the lower level functions required to accomplish the parent requirement. All specified usage modes are included in the analysis. Functional requirements are arranged such that lower level functional requirements are recognized and traceable to a higher level, or parent, requirement.

Completion of the functional allocation of all policy requirements catalyzes the synthesis of the logical, functional architecture into a physical, or executable architecture. Requirements analysis is employed to verify that physical alternatives can satisfy the policy needs manifested in the requirements set. The output from synthesis defines the policy "design." It forms the framework for the derivation of policy implementation alternatives

Alternatives Analysis/Selection

The third quadrant is Alternatives Analyses/Selection. Within this quadrant, solution alternatives, identified through the design output of the synthesis function in Quadrant Two, are analyzed. Decision alternatives are evolved from the value driven goals and objectives established for the policy in Quadrant One, Goals/Objectives Analyses, and the functions and the

requirements the policy must achieve in meeting the goals and objectives of that policy. As noted by E. E. Schattschneider," the definition of alternatives is the supreme instrument of power."[63]

Alternatives, therefore, are essential to the "health" of the policy evolutionary process. They are established through a careful analysis of the policy functions and the specific requirements those policy functions must satisfy. Resource analysis allocates resources to achieve the functions specified by the requirements analysis. Cost-benefit analysis, or CBA, compares the expected costs associated with a functional alternative with the benefit to be derived from its implementation. In this quadrant, the results from all the previous analyses--requirements analyses, functional analyses and allocation, resource allocations, and cost-benefit analyses--come together into a series of implementation options. This is a key step in the evolution of policy and is heavily influenced by the value engineering from Quadrants One and Two. From this activity will come the exercise of choice. Out of this quadrant, a policy alternative is selected, based upon the comprehensive trade-off analyses among the competing choices.

Trade-offs are an integral part of the decision-making process. Trade-offs are essential, deterministic models used in establishing value preferences, indifference relationships, and the maximizing behavior necessary to achieve individual and systemic goals. Rational actors, e.g., individuals, companies, governments, or nations, make decision choices

against an ordered set of preferences. Outcome preferences are ranked and ordered based upon the value-maximizing mind-set of the decision maker. Alternatives are compared and the preference relationships complete if, for any two alternatives, the decision maker has either a preference or an indifference between the set of alternatives.

Risk is the product of the probability or likelihood that a policy alternative will fail to achieve its expected utility or fail to meet its value-based objectives and the consequence of that failure.[64] The functions undertaken within this quadrant are designed to provide the tools necessary for the decision maker to assess the various risks associated with policy implementation. This area addresses the policy risks and the specific activities that must be accomplished to mitigate those risks. The risks are adequately mitigated when the results of an evaluation, analysis, or prototype reduce the risk impact to a level acceptable to the decision maker.

Decision making in this quadrant may be aided by the use of simulations and modeling of the policy decisions and the identification of metrics to collect, assess, and ultimately validate, the usefulness of the implemented policy. Risk assessment validates that known risks associated with the selected alternative are either manageable, or that the decision maker is cognizant of the risks and their costs prior to making any decisions.

The formal, quantifiable assessment of risk and strategies for mitigating assessed risk is crucial to the successful derivation and

implementation of policy. Risk assessment and management processes that are weakly structured, subjective, and/or ad hoc in nature are anathema to the successful promulgation of policy.

Finally, the impact of potential failure of a policy to affect a desired outcome must be assessed to provide the decision maker with a complete, world-view from which to make decisions. Failure analysis, coupled with exit planning, provides the decision maker with the requisite policy "escape mechanism" in the form of an exit criteria and strategy, should circumstances warrant.

Validation/Execution

Quadrant Four, Validation/Execution, encompasses the critical political analyses and agenda setting activities necessary to ensure that the policy to be implemented is both understood and supported by the Congress and the American people. Capture and maintenance of favorable public opinion is crucial to the sustainment of policy. Policy execution follows successful agenda setting, political bargaining, and public opinion capture.

One additional, critical step follows policy execution throughout each of the seven, lifecycle phases of the PIES model. That step involves a lessons learned analysis of the policy execution. Lessons learned are key to improving policy and its execution. As Neustatdt and May observed:

> Marginal improvement in performance is worth seeking. Indeed, we doubt that there is any other kind. Decisions come one at a time, and we would be satisfied, taking each on its own terms, to see a slight upturn in the average. This might produce much more improvement measured by results.[65]

Formal Policy Reviews

Each quadrant of the PIES model is separated by a formal decision review. These are labeled as Initial Policy Review (IPR), Revised Policy Review (RPR), and Final Policy Review (FPR). The IPR is scheduled and formally executed at the completion of each quarter turn of the spiral and before the next quadrant is entered. The RPRs are scheduled to occur with each subsequent complete spiral of the model, until a final FPR is executed at the conclusion of a lifecycle phase and prior to the policy execution. These interim reviews provide policy decision makers an opportunity to review evolving policy during key stages in its lifecycle. Figure 2-3 illustrates the four quadrants and the formal review cycles incorporated into the PIES model.

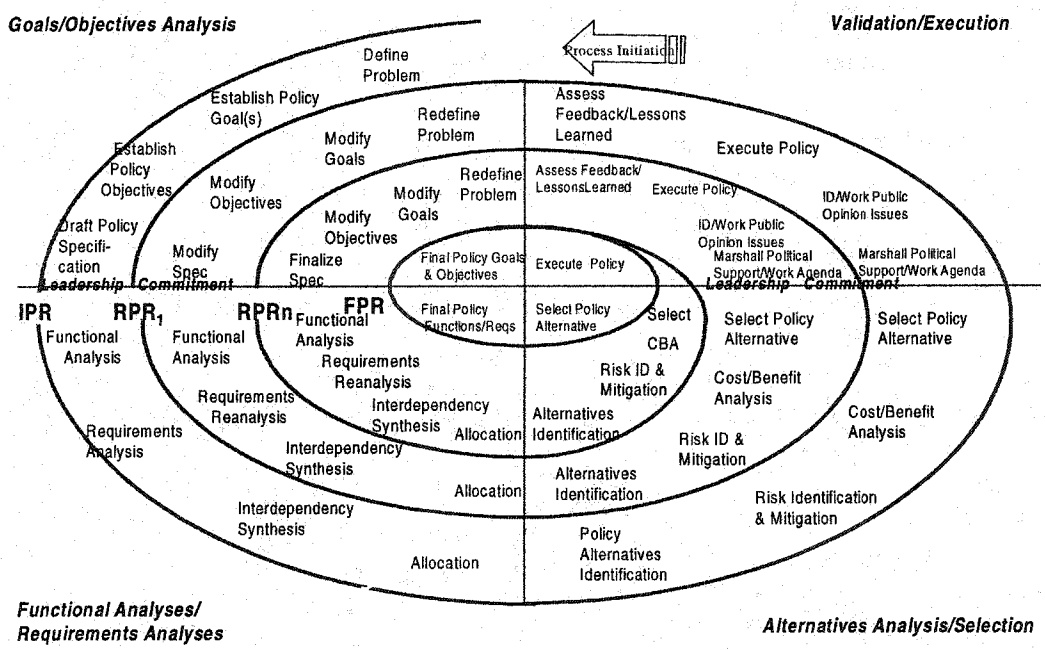


Figure 2-3: Four Policy Evolution Quadrants of the PIES Model

PIES Vectors

Many kinds of external forces serve to act upon the policy-development process, exerting influence on elements of the decision-making cycle. Kingdon spoke of a set of "streams" which run through the decision structure, exerting influence on the decision process. Kingdon identifies three such streams as problems, policies, and politics:

> Each of the streams has a life of its own, largely unrelated to the others. Thus people generate and debate solutions because they have some self-interest in doing so, not because the solutions are generated in response to a problem or in anticipation of a particular upcoming choice. Or participants drift in and out of decision making, carrying their pet problems and solutions with them, but not necessarily because their participation was dictated by the problem, solution, or choice at hand...At any rate, the logical structure of such a [organizational] model is the flow of fairly separate streams through the system, and outcomes heavily dependent on the couplings of the streams in the choices that must be made.[66]

Kingdon's construct described these streams as "flowing" through the decision space. In his model, "streams" is an apt metaphor. Webster defines stream as "a steady succession; a constantly renewed supply; an unbroken flow."[67] The connotation is that a stream is a force of nature. There is no discussion of "controlling" the stream, i.e., damming or channeling the force.

In the PIES construct, these externalities are defined not as streams, but as decisional vectors. *Webster* defines a vector as "a quantity [or element] that has magnitude and direction."[68] In the PIES context, therefore, vectors refer to specific influences, which exert measurable force in a specific direction on an element, quadrant, phase, or the totality of the policy

continuum's decision-making structure. Any decision-making construct, including PIES, would be an incomplete policy analysis framework if it failed to take into account the existence of these forces.

Arguably, an infinite number of decisional vectors might notionally exert some measure of influence on the policy process. PIES identifies six, major influence vectors: Problem Vector, Language Cognitive Vector, Process Vector, Participant Vector, Economic Vector, and Political Vector.

Problem Vector

The Problem Vector is borrowed from March, Cohen, and Olsen's garbage can model and later from Kingdon's streams model. Problems are issues raised for inquiry, consideration, or solution. A problem exists when a decision is required or an action is necessary to address a real or perceived inequity, or to surmount an environmental challenge to an existing status quo. For the purposes of the PIES model, the Problem Vector represents the set of decisionable issues and their influences exerting tension on the organizational system through the application of a specific force and direction on the decision continuum. The Problem Vector exerts its greatest influence on the decision continuum through its interaction with the Goals/Objectives Analyses quadrant of the PIES model.

Language Cognitive Vector

The Language Cognitive Vector accounts for the influence that language plays in the cognitive processes and decision making leading to the

evolution of policy. Major shifts in policy are the consequence of a process of social construction based in language. Periods of major change in policy choice are accompanied by changes in the dominant policy language and its precise use to define new policy concepts. It therefore holds that language is both a determinate as well as an indicator of policy change and choice.

Process Vector

The Process Vector identifies and measures influences arising from the dominant decision making process, or body, during each stage of the policy lifecycle. In particular, this vector weighs changes in the decision making process, institutions, and power bases and their affects on the direction policy evolves over time. Process change exerts an influence on the basic tenets of policy evolution, if not its actual direction.

Participant Vector

The Participant Vector accounts for the ever shifting set of decision makers, subject matter specialists, and other key players involved in the policy process. Participants come and go during the policy's lifecycle. Each exit spawns an attrition of some amount of individual and corporate history unique to the individual who participated in the evolution of policy. With each entrance of a new player comes a new set of preferences, experiences, and beliefs, all of which exert a different influence on the policy evolution. Substantial variation in participation serves as a metric for measuring the waxing or waning of the policy issue on the alter of political agenda.

Economic Vector

The Economic Vector measures the influence that the dominant economic forces have upon policy direction over time. In periods of relative economic stability, policy would tend to favor the economic status quo, reflecting minor or no change. However, in times of economic instability, policy evolution could be profoundly affected by economic influences and reflect that instability through significant change in policy.

Political Vector

The Political Vector accounts for the political forces which act upon the policy continuum. These forces are composed of such elements as interest group pressures, election results, Congressional partisanship, ideological differences within the body politic, or even, simply the "mood" of the country. All serve to influence the political agenda and thus the attention of key decision makers. As Kingdon wrote:

> These developments in the political stream have a powerful effect on agendas, as new agenda items become prominent and others are shelved until a more propitious time.[69]

The political vector measures the influence political forces and their constituents have on the lifecycle evolution of policy.

Figure 2-4 provides a cross-sectional view of the PIES model, combining the four quadrants and policy review/decision points with the six vectors described above.

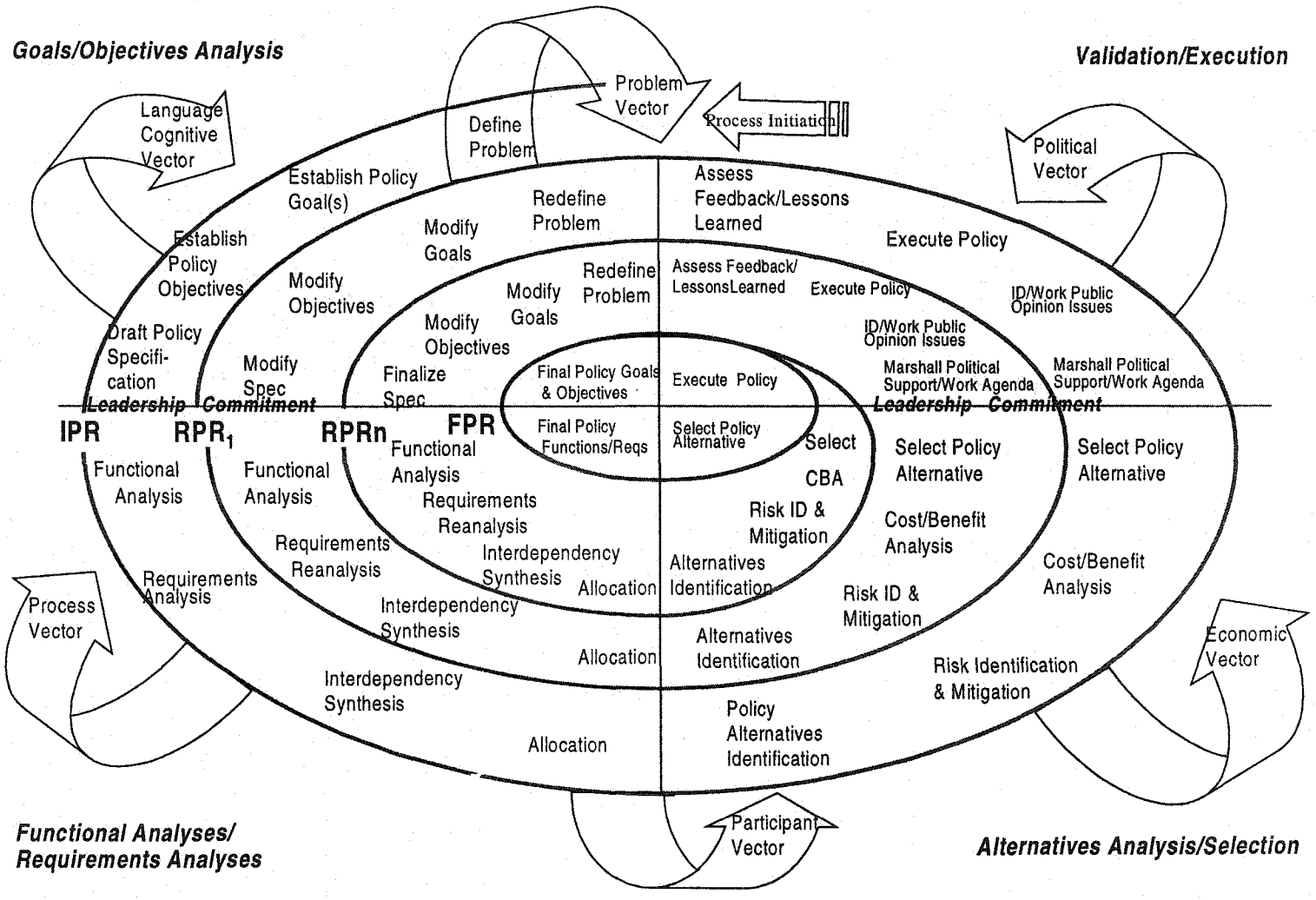


Figure 2-4: Cross-sectional View of the Policy as an Incremental Evolutionary Spiral Model

SUMMARY

The heart of organizational theory is the study of the decision-making process. In Simon's words, "that is administration."[70] Paradoxically, organizational decision making is, at best, a very inexact science. It is based on the character of the organization, the intrinsic values of its members, and the latitude to which the organization will promote value judgements.

The range of possibility is great: from Simon's bounded rationality to Kirlin's language-based social construction; from Allison's tri-model construct to March, Cohen, and Olsen "garbage can" and Kingdon's "streams and windows;" from Lindblom's incrementalism and Stone's production line to Laswell's and Brewer's cycles. From the analytic and empirical analysis identified with systems engineering, rational theory, and operations research to the political process identified with judgement, values, and ethics--it all points to a single premise: the central theme of organizational existence is decision making. The issue at the forefront of the study of formal organizations remains, can we learn to do it better?

In a democracy, the public expectation is that the government acts in the society's pluralistic "best" interest and that through decision-making authority afforded it through the ballot process, elected leaders exercise decision-making choice in a manner superior to that which the ordinary citizen is capable of exercising. The aura and mystique of the institutions of governance in Washington, D.C., and elsewhere have been tarnished by the realization that

elected decision makers often fail to exhibit the capacity for what might be termed, "world-class decision making." In fact, the electorate is often baffled by what appears to be a lack of even common sense in the decision-making processes practiced by their elected representatives.

But public policy that appears to violate the notion of "the public good" serves the purposes of some interest group. The exploitation of the pluralist nature of the United States' decision-making process to influence or achieve a desired policy outcome, even at the expense of the general population, is a legitimate exercise of political influence in the policy-making process. The appearance of "impropriety" may be exacerbated by the general public's lack of knowledge or interest in policy decisions that, on the surface, seem to impact a limited group of the population. The basic assumption is that what is invisible or transparent to the general electorate does not arouse their interest or political sanction.[71]

This assumption underscores a fundamental tenet of rational choice theory, which holds that rational action always involves efforts at utility maximization. This posits that an individual or a group of individuals, having a shared set of values and goals, when confronted with an array of options, will select the option that best serves, i.e., maximizes, the objectives of the decision maker(s). As Olson stated, an individual's actions are rational when the objectives sought are "pursued by means that are efficient and effective for achieving those objectives," given the decision maker's beliefs. [72] Simon echoed this when he stated, "in its broadest sense, to be efficient simply means to take

the shortest path, the cheapest means, toward the attainment of the desired goal."[73]

In policy development, this premise is ripe with what Katz and Kahn termed "undifferentiated logic," i.e., the assumption that all parties are assumed to operate within the same frame of rationality, creating a false homogeneous view of both individuals and their societies, motives, goals, and reason. The more removed or remote an individual or group of individuals are to the decision makers' experience set or frame of reference, the more "sameness" is attributed to that individual or group. This "comfort zone" of cognitive processes underlies many of the mistaken assumptions contributing to fundamentally flawed decision logic and policy making.[74]

This convolution of differentiated and undifferentiated logic bearing down upon the decision maker begs the question, "Is there a better way?" For the purposes of this dissertation, the Policy as an Incremental Evolutionary Spiral model is offered to that end. PIES is an enhanced framework for evolving and analyzing policy development. It avoids being bound by any single modeling heritage or decision-making school of thought by borrowing the best from ALL of the authors and theory bases discussed in this chapter, melding them into a simple, yet powerful, analysis tool. The proof, of course, is in an assessment through its application, found in Chapter Eight of this manuscript.

[1] David I. Cleland and William R. King, *Systems Analysis and Project Management*, 3d ed. (New Delhi: McGraw-Hill Book Company, 1983), 84.

[2] Ibid., 86.

[3] Herbert A. Simon, *Administrative Behavior* (New York: The Free Press, 1976), 240.

[4] James W. Fesler and Donald F. Kettle, *The Politics of the Administrative Process* (Chatham, New Jersey: Chatham House Publishers, Inc., 1991), 41.

[5] Charles E. Lindblom, *Politics and Markets* (New York: Basic Books, 1977), 17-32.

[6] Fesler, 45.

[7] Felix A. Nigro and Lloyd G Nigro, *Modern Public Administration* (New York: Harper and Row, Publishers, Inc., 1973), 18.

[8] Ibid., 241.

[9] Ibid., xxviii

[10] Herbert Simon, "Administrative Decision Making," *Public Administration Review* (March 1965), 35-36.

[11] Phillip Selznick, *Leadership in Administration* (Berkeley, CA: University of California Press, 1957), 38.

[12] Ralph L. Keeney, and Howard Raiffa, *Decisions with Multiple Objectives* (Cambridge, UK: Cambridge University Press, 1993), 4.

[13] Ibid., xvi-xvii.

[14] James D. Thompson, *Organizations in Action* (New York, NY: McGraw-Hill Books, 1967), 132.

[15] Ibid., 134.

[16] Keeney and Raiffa, 26.

[17] Thompson, 135.

[18] Keeney and Raiffa, 26.

[19] Alberto Guerreiro Ramos, *The New Science of Organizations* (Toronto, Canada: The University of Toronto Press, 1981), 25.

[20] Dennis F. Thompson, "The Possibility of Administrative Ethics," *Public Administration Review*, Vol. 45, No. 5 (September/October 1985), 555.

[21] Ibid., 559.

[22] Robert B. Denhardt, *Theories of Public Organizations* (Monterey, CA: Brooks/Cole Publishing Co., 1984), 81.

[23] Ibid., 82.

[24] Deborah Stone, *Policy Paradox* (New York: W.W. Norton and Company, Inc., 1997), 10.

[25] John J. Kirlin, "Policy Formulation," in *Making and Managing Policy*, ed. G. Ronald Gilbert (New York: Marcel Dekker, Inc., 1984), 13.

[26] H.D. Laswell, *A Pre-View of Policy Sciences* (New York: Elsevier, 1971) in John J. Kirlin, "Policy Formulation," in *Making and Managing Policy*, ed. G. Ronald Gilbert (New York: Marcel Dekker, Inc., 1984), 13.

[27] Gary Brewer, "The Scope of the Policy Sciences," (New Haven, CT: Mimeo course syllabus, 1978) in John J. Kirlin, "Policy Formulation," in *Making and Managing Policy*, ed. G. Ronald Gilbert (New York: Marcel Dekker, Inc., 1984), 13.

[28] J. May and Aaron Wildavsky, eds. "The Policy Cycle," *Sage Yearbooks in Politics and Public Policy,* Vol. 5 (Beverly Hills, CA: Sage Publishing, 1978) in John J. Kirlin, "Policy Formulation," in *Making and Managing Policy*, ed. G. Ronald Gilbert (New York: Marcel Dekker, Inc., 1984), 13.

[29] Kirlin, 13.

[30] Ibid., 14.

[31] Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston, MA: Little, Brown and Company, 1971), 5.

[32] Ibid., 6.

[33] Ibid., 6.

[34] Ibid., 6-7.

[35] James G. March and Johan P. Olsen, *Ambiguity and Choice in Organizations* (New York: Columbia University Press, 1982), 36.

[36] Ibid., 33.

[37] Ibid., 37

[38] Kingdon, 117.

[39] Ibid., 120.

[40] Donald P. Green and Ian Shapiro, *Pathologies of Rational Choice Theory* (New Haven, CT: Yale University Press, 1994), 13.

[41] Ibid., 16.

[42] Mancur Olson, *The Rise and Decline of Nations* (New Haven, CT: Yale University Press, 1982), 17-19.

[43] Ibid., 18.

[44] Green and Shapiro, 17.

[45] John J. Kirlin, "Policy Formulation," in *Making and Managing Policy: Formulation, Analysis, Evaluation*, ed. G. Ronald Gilbert (New York: Marcel Dekker, Inc., 1984), 13-14.

[46] Green and Shapiro, 20.

[47] Debra Satz and John Freejohn, *Rational Choice and Social Theory*, Manuscript, Stanford University cited in Donald P. Green and Ian Shapiro, *Pathologies of Rational Choice Theory* (New Haven, CT: Yale University Press, 1994), 20.

[48] Jon Elster, *In Rational Choice,* ed. Jon Elster (New York: New York University Press, 1986), 16.

[49] Ralph L. Keeney and Howard Raiffa, *Decisions with Multiple Objectives* (Cambridge, MA: Cambridge University Press, 1993) , 26.

[50] R. Duncan Luce and Howard Raiffa, *Games and Decisions,* 2d ed (New York: Dover Publications, 1989), 312-313.

[51] James D. Morrow, *Game Theory for Political Scientists* (Princeton, New Jersey: Princeton University Press, 1994), 166.

[52] Louis Padulo and Michael A. Arbib, *System Theory* (Washington, D.C., Hemisphere Publishing Corp., 1974), V.

[53] Merriam-Webster, definition of "systems analysis," Webster's New Collegiate Dictionary (Springfield, MA: Merriam-Webster, Inc, 1956), in David Cleland and William King, *Systems Analysis and Project Management*, 3d ed. (New Delhi, India: McGraw-Hill Book Company, 1983), 83.

[54] David Cleland and William King, *Systems Analysis and Project Management*, 3d ed. (New Delhi, India: McGraw-Hill Book Company, 1983), 87.

[55] Electronic Industries Association, *EIA/IS-632, Systems Engineering* (Washington, D.C.: EIA Engineering Publications Office, 1994), 5.

[56] Ibid., 8.

[57] Abraham Kaplan, *The Conduct of Inquiry* (New York, NY: Harper and Row Publishers, 1963), 49.

[58] Herbert A. Simon, *Administrative Behavior,* 3d ed. (New York: The Free Press, 1976), 306-307.

[59] Ibid., 306.

[60] Morrow, 312.

[61] Keeney, 6-28.

[62] EIA/IS-632, 9.

[63] E. E. Schattschneider, *A Semi-Sovereign People* (New York: Holt, Reinhart, and Winston, 1960), 68.

[64] Edmund C. Conrow and Patricia S. Shishido, "Implementing Risk Management on Software Intensive Projects," *IEEE Software*, vol. 14, no. 3 (May/June 1997), 84-85.

[65] Richard E Neustadt and Ernest R. May, *Thinking In Time* (New York: The Free Press, 1986), xvii.

[66] Kingdon, 85.

[67] Merriam-Webster, definition of "stream," Webster's Ninth New Collegiate Dictionary (Springfield, MA: Merriam-Webster, Inc, 1983), 1165.

[68] Ibid., definition of "vector,"1306.

[69] Kingdon, 145.

[70] Simon, 240.

[71] Murray Edelman, *The Symbolic Uses of Power* (Urbana, IL: University of Illinois Press, 1985), 36-37.

[72] Mancur Olson, Jr., *The Logic of Collective Action, 2d ed.* (Cambridge, MA: Harvard University Press, 1971), 65.

[73] Simon, 14.

[74] Daniel Katz and Robert L. Kahn, *The Social Psychology of Organizations.* 2nd ed. (New York: John Wiley and Sons, Inc., 1978), 506.

CHAPTER THREE

RESEARCH QUESTIONS AND PROPOSITIONS

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

This study uses the Policy as an Incremental Evolutionary Spiral (PIES) model, described in Chapter Two, to analyze the development of the Information Assurance component of United States national security policy during the Clinton Administration, from January 1993 through December 2000. Chapter Three presents a set of five research questions and a total of 17 supporting propositions used to frame the PIES analysis. Each research question is supported by two to five propositions.

RESEARCH QUESTION ONE: How has the Information Revolution affected the framework within which national security policy is evolved and implemented?

From the national security perspective, the impact of the Information Age on how this country develops its national security policy and wages war will increasingly depend on information and communication assurance. Former Deputy Under Secretary of Defense for Policy, Jan M. Lodal, stated in 1996:

> Information technology has the potential to revolutionize war. Nearly perfect battle-space awareness, real-time coordination of operations and just-in-time logistics are all made possible by

> the new information technology, and any one of these would constitute a revolution.[1]

Berkowitz, in discussing the role of information and information infrastructure would have on future conflicts involving the United States, said:

> What stands clear today is that information technology has reached critical mass. Information systems are so vital to the military and civilian society that they can be the main targets in war, and they can also serve as the main reasons for conducting offensive operations. In effect, SIW [Strategic Information War] is really the dark side of the Information Age. The vulnerability of the military and society to IW attack is a direct result of the spread of information technology. Conversely, SIW's potential as a weapon is a direct result of United States' prowess in information technology.[2]

This research question and its subordinate propositions probe the role that Information Technology and the Information Age revolution, as independent variables, have on the framework within which national security policy, as dependent variable, evolves and is implemented.

Proposition 1: The pervasiveness and technical complexities inherent in the dichotomy of Strategic Information Warfare (SIW) and Information Assurance (IA) have fundamentally altered the basic tenets upon which national security policy rests.

In the near future, adversaries of the United States, or of its domestic or foreign policies, will leverage Information Technology tools and techniques to hold at risk key United States' strategic assets, such as elements of the

nation's critical infrastructure (e.g., telecommunications, energy, banking, transportation, etc.). As Molander, et. al. stated in 1998:

> Both regional adversaries and peer competitors may find SIW tools and techniques useful in challenging the United States, its allies, and/or its interests. SIW weapons may find their highest utility in the near term in *"asymmetric" strategies* (Molander's highlighting) employed by regional adversaries. Such adversaries might seek to avoid directly challenging United States' conventional battlefield superiority through a more direct attack (or threat) involving some combination of nuclear, chemical, biological, highly advanced conventional, and SIW instruments.[3]

SIW tools and techniques pose a dual-edged challenge to United States' security interests. First, an attack on a critical national infrastructure vulnerable to massive disruption, which results in the widespread loss of public confidence in the ability of the government to protect these resources, would afford an adversary an asymmetric, strategic leverage over the United States and the exercise of its policies. Second, a similar threat directed against the United States military or elements of the critical national infrastructure that support the force projection capability of the uniformed military, could slow or even derail the application of United States military force to affect national policy.

Traditional "threat" identification, analyses, and defense response -- staples of Cold War defense planning--may no longer serve to affect national security policy in the Information Age. Rather, the analysis, identification, and mitigation activities associated with inherent "vulnerabilities" of the critical national information infrastructure may be the key, or focus of concern, for

United States national security policy makers. As Col. Alan Campen noted in 1997:

> Attempts to quantify the threat as a precursor to building a new national security sanctuary are exercises in futility. These efforts employ an approach to defense that vanished with the Cold War. Vulnerabilities, on the other hand, are the handiwork of the system designers, and the same talent that created them can repair them in the quickest and best manner.[4]

This proposition probes the degree to which Information Technology has altered the basic foundation of national security policy formulation and its application.

Proposition 2: Decision-making processes at all levels of national security implementation have been radically impacted by the Information Revolution.

Instantaneous access to a much wider universe of available information changes the fundamental decision-making focus of individuals and organizations. Cooper suggests that the most fundamental paradigm shift associated with the Information Revolution may be one of perspective.[5] National security policy and its implementation have evolved from an inside-out perspective, i.e., a "pre-Copernican" view, in which the United States assumes the central locus and, therefore, narrow focus of a previously introspective national security "universe."

But instantaneous access to and "near perfect awareness" of pertinent information, to borrow from Lodal,[6] permitting a fundamental expansion in the

depth and breadth of the decision maker's tactical and strategic frames of reference, demand a change in the decision-making perspective. This "panoramic view" of the decision space, difficult, if not impossible, to frame prior to the advent of Information Age technology, strongly lends itself to an inversion of the classic United States' perspective, shifting the world view from an inside-out framework to a much more outside-in construct.[7]

The Unites States, and its vested interests, assume a much different position from the outside-in field of regard. This proposition examines the conjecture that this fundamental shift in perspective drives a reactive change in the national security policy decision-making process, especially in those involving issues of high-risk, complex technologies.

Proposition 3: By virtue of its position in the world and its reliance on Information Technology, the United States is at risk from assault through asymmetric Information Technology means that could seriously impact the execution of foreign policy through the projection of military force.

While seeking to augment its considerable offensive military arsenal with Information Technology weapons, the United States finds itself uniquely vulnerable to the application of Strategic Information Warfare (SIW) by current and future adversaries. The Information Technology-intensive infrastructures of the United States create a singular vulnerability to SIW. That vulnerability may be exploited by parties seeking to gain asymmetric

leverage against the United States through the disruption of its ability to project military power through an SIW attack on the nation's critical information infrastructure. As Molander, et. al. noted in 1998:

> The United States leads the world in the development and application of Information Technology and has a complex society and economy that are critically dependent on information systems. It is geographically protected and has the world's most awesome conventional military capabilities. If the Unites States is to be defeated militarily in the near future, it will most likely be because an enemy successfully uses an "asymmetric" strategy to achieve some strategic end.[8]

Two specific classes of threat fall into the SIW category. The first are SIW threats that can be directed against the nation's economic infrastructure. The second are more direct SIW threats to United States' military infrastructure, or to the national information infrastructure that supports the military during periods of national mobilization and force projection.

The key to the SIW risk to the United States inherently lies in vulnerabilities that exist in the critical information infrastructures that underpin the essential foundations of the United States' electronic society: telecommunications, banking, emergency services, telecommunications, government services, electrical power and energy services. This proposition probes United States' vulnerability to SIW by first examining the inherent vulnerabilities in these critical information infrastructures and then, through a survey of the public record, chronicles the steps taken by the Federal government during the Clinton Administration to secure those critical infrastructures from the SIW threat.

RESEARCH QUESTION TWO: How do policy and decision-makers frame or theorize about high-risk, technologically-complex issues involving the development of national security policy?

As public policy decisions have become increasingly more dependent upon technology issues and solutions, the question of how Government decision makers frame or theorize about these high risk, technologically-complex, national security policy issues, becomes increasingly important in the analysis and pathology of decision making.

The professional bureaucracy has traditionally been looked to as the source of subject matter expertise and professional guidance in matters of policy development and implementation for the Federal Government. That may have changed. Lindblom and Woodhouse posited that the professional bureaucracy may be incapable of making rational policy decisions in the Information Age, suggesting that the professional bureaucracy falls victim to the defense of "narrowed interests," thus losing an ability to objectively frame new subject matter, such as that associated with Information Technology.[9]

Neustadt and May argued that decisions made by organizations reflect organizational "presumptions, "which are based upon routines and operating modes that have become entrenched into the organizational culture over time."[10] These "presumptions" make it difficult for organizations to frame or theorize about new or complex technologies and resultant policy paradigms.

Finally, Thompson argued that organizations strive to align themselves structurally within their core technology and their task environment. When the environment and technology become out of alignment, organizational dysfunction results. An organization's ability to maintain a viable technology is key to an organization's survival and its ability to frame and address complex, new decision-making issues. As Thompson wrote:

> Organizations must find and maintain a viable technology--that it must have some capacity to satisfy demands of the task environment, and that these demands may be changing. In the society geared to complex organizations, technologies change as cause/effect understandings change; hence a technology that was effective yesterday may be inadequate today...Questions of which technologies to retain, which to expel, and which to adopt may not be daily matters for any complex organizations, but they are potential problems for every organization in a modern society.[11]

This research question examines the extent to which emerging technologies play a significant role in the ability of the decision maker to adequately frame or theorize about complex issues of national security.

Proposition 4: The emergence of Information Assurance as a major policy issue compels government organizations to become both adaptive and directive in maintaining their power base vis-à-vis the evolving policy environment and their organizational competitors.

Government organizations exist in large part because they have a defined role, or purpose, that helps bound and justify their organizational

existence. That justification is conditional upon an appropriate co-aligning, in both time and space, of such organizationally-intrinsic factors as the value set, the operational structure, the task orientation, i.e., the organizational goals and objectives, and the technology core of the organization. As Thompson observed, organizational survival rests on the co-alignment of technology and task environment, within a viable domain, and of organization design and structure appropriate to that domain.[12]

When faced with an external environmental change, organizational maintenance, if not survival, is dependent on the organization's ability to adapt or redirect its core to accommodate the changing environment. This proposition probes the assumption that organizations will reactively adapt or proactively direct change in their core behavior in response to high-risk, technologically-complex policy issues, such as Information Assurance.

Proposition 5: Technical complexities, such as those associated with the Information Revolution, may exceed the capacity of the permanent bureaucracy to effectively react to emerging policy needs in a timely manner, giving rise to alternative venues for policy evolution.

The role of policy maker has been usurped by a growing number of political appointees brought into the public administration by each newly elected Federal administration. Meier contended that this practice establishes a barrier between professional administrators (bureaucrats) and policy makers (elected officials). It isolates the career professionals from

becoming actively engaged in the policy debate and denies the elected officials the opportunity to tap into years of the career professionals' prior experience in performing policy trade-off analyses and assessing policy costs and risk.[13]

Lindblom and Woodhouse argued that bureaucratic policy making can actually reduce the intelligence of policy making. This happens when administrators:

> Focus on protection of their own budget, power, or policy turf; fall into preoccupation with process instead of results; and when administrators become captured to an indefensible extent by one narrow set of interests, and fail to attend to considerations necessary for sensible action within their realm of responsibility.[14]

This proposition probes this administrative dichotomy by analyzing the role played by the professional bureaucracy, vice that of appointed administrators, in evolving high-risk, technologically-complex, national security policy.

Proposition 6: Organizational history creates predictable decision-making patterns of behavior that resist change in framing and theorizing about even complex, high-risk issues involving national security policy.

Neustadt and May believed that organizations tend to look to their own histories when making decisions about current policy. These authors cited the Cuban Missile Crisis of October 1962, describing how President Kennedy

and his ExComm paid particular attention to organizational histories, focusing on how organizations behaved without asking explicitly how they behaved over time and why. President Kennedy, they wrote:

> Seemed to understand in his bones the tendency of large organizations to act today as they acted yesterday. He pursued his own hunches about American performance. Among other things, he sent the CIA to photograph Air Force planes at Florida bases. The pictures showed that, contrary to his orders, the planes were lined up in the highly vulnerable standard position--wing tip to wing tip--just as in Manila twenty-one years before. Schooled in the inertia of military procedures as a junior officer in World War II, Kennedy was annoyed but not surprised.[15]

Decisions tend to be made by organizations with set routines and operating styles that over time have become entrenched as part of their organizational culture. For the decision maker, it is important to understand how an organization thinks and reacts to choice opportunities in advance of that organization being tasked with making and executing a policy related decision. Neustadt and May suggested that the technique of placement, or identifying an organization's "institutional proclivities" by drawing inferences from the time line of its relevant historical experiences, is one method of predicting how organizations will act under conditions of uncertainty.[16]

This proposition probes whether organizational history plays a significant role in the decision maker's ability to frame technologically-complex, high-risk issues involving national security policy.

RESEARCH QUESTION THREE: What effects do emerging and complex evolutionary shifts in society have on the framework of governance and the administrative institutions associated with it?

Change is as much a constant in political or organizational life as it is in every other facet of existence. When change comes upon an entrenched policy or government bureaucracy, survival depends on the organizational ability to adopt a decision-making strategy for dealing with that change.

James D. Thompson suggested that while decision-making strategies can be introduced to maximize goal satisfaction within well known environmental circumstances, rapid changes in society or in society's core technologies can create decision dilemmas for which there are no clear views of either cause/effect relationships or certainty of organizational decision preference. In such cases, Thompson stated, the organization must rely on inspiration to make its choice. Where inspiration is not forthcoming, the organization will, when possible, attempt to avoid the problem altogether (decision-avoidance strategy).[17]

Neustadt and May, speaking from their "lens of history" research perspective, discussed the role that presumptions play in the decision making process. They spoke of "three intricately interrelated reasons" why presumptions are important:

> First, presumptions--items *Presumed* [Neustadt/May cap/italics]--figure in the definition of the situation. Second, by the same token, they help to establish concerns and, along with a sense of how concerns evolved, shape definitions of aims, of

> concrete objectives. Third, above all else, presumptions influence options and choices among them.[18]

The decision maker's presumptions concerning the environment and issues in question define the decision space, determine the objectives to be met, and bound the choices and options considered. Harboring presumptions about the environment and issues to be addressed that do not accurately reflect emerging and evolutionary shifts in the fabric of society would limit the effectiveness of subsequent policy and its government administration.

The Information Age and Information Technology have profoundly impacted and significantly altered many of the economic and informational foundations that underpin the global society. Public Administration's ability to both recognize and then modify its own organizational foundations to accommodate these emerging and complex evolutionary shifts in society are keys to maintaining an effective framework of governance and the administrative institutions associated with it. This research question, and its subordinate propositions, examines the impact that the Information Age and Information Technology have had on the framework of Federal governance in the United States during the eight-year Clinton Administration.

Proposition 7: Government policy often fails to evolve in step with the major societal developments induced by powerful change agents, such as Information Technology, even when the change induced is so pervasive as to reshape society and its core institutions substantially.

Schon stated that an individual's and organization's inability to keep pace with significant environmental change is due to the threat that change represents to organizational stability and identity status quo--what Schon called the "stable state."[19]

Belief in and anchoring to a stable state serves to protect individuals and organizations from the impact that change may have upon the fundamental constancy of the core framework of their institutions and policies. As a result, the organization, as a whole, has an inherent resistance to change that manifests itself in a tendency of both individuals and organizations to actively resist change, even beneficial change, to maintain the status quo. Schon called this resistance "dynamic conservatism."[20]

This proposition examines the efficacy of Schon's "stable state" construct, probing both the adaptability and the resistance to adaptation exhibited by government organizations when confronted with technically-complex, high-risk change agents, such as Information Technology.

Proposition 8: The complexity and pervasive impact of a significant change agent, such as Information Technology, leads to the adoption of cooperative behavior and strategies between otherwise competing organizations.

Thompson held that under cooperative strategies, the effective achievement of goals is dependent on the exchange of commitments, sharing of power, and the reduction of potential uncertainty for both parties.[21]

Based upon Thompson's precepts, reaching effective closure on high risk Information Technology policy issues requires the adoption of co-opting and coalescing behavior between agencies within the Federal Government, as well as between the public and the private sectors.

Selznick observed that a process of "dynamic adaptation" takes place at the boundary where policy gestation and administration meet. Organizational processes profoundly influence the kinds of policy that can be made, while policy shapes the internal mechanisms of organizations in ways that cannot be accounted for on the premise of organizational efficiency.[22]

Allison wrote that issues of policy are often decided as a result of bargaining among the policy makers, who seek to achieve a balance between personal/organizational needs and those of the collective, i.e. the Bureaucratic Politics Model, or Model III. Based upon these constructs, this proposition probes the assumption that individuals and organizations will adopt some form of cooperative strategy in order to effectively address technically-complex, high-risk issues, such as Information Assurance policy.

Proposition 9: Policy issues devoid of political capital may elevate to the top of the agenda hierarchy through the advent of a series of catalyzing events.

Kingdon has suggested that the problems underlying policy issues are often not self-evident by policy metrics, or indicators. An external catalyst or intervention is required to elevate the problem to the attention of both the

general public and decision makers within government. That intervention often comes in the form of what Kingdon called a "focusing event."[23] A focusing event is a defining moment that occurs often randomly, such as a national crisis or natural disaster, becoming a powerful symbol associated with a specific issue. This symbol succeeds in riveting the attention of the public and the policy maker on the policy matter that, as a result of the event, is now of immediate importance to both.

Edelman believed that these events create "condensation symbols," or representations that evoke the emotions associated with an event. Symbols condense complex ideas into easily understood and transmitted representations, in which the meaning of the symbol and its underlying ideas is generally shared by the propagator of the symbol and its recipients.[24]

Birkland expanded the Kingdon construct further to define a potential focusing event as:

> An event that is sudden, relatively rare, can be reasonably defined as harmful or revealing the possibility of potentially greater future harm, inflicts harm or suggests potential harms that are or could be concentrated on a definable geographic area or community of interest, and that is known to policy makers and the public virtually simultaneously.[25]

This proposition probes the efficacy of the focusing event concept by identifying causalities between physical cyber-related events and any specific Information Assurance policy-related reactions by government.

RESEARCH QUESTION FOUR: Within the high-risk, high-technology national security policy arena, who exercises the greatest influence and leverage among policy makers and why?

Kingdon suggested that the professional bureaucracy is the most influential entity in shaping government policy, due to its experience in administering government programs and dealing with the varied interest groups and congressional interests associated with government programs. Kingdon emphasized the value of the relationships and access accorded the professional bureaucracy to elected decision makers and their key staff as further evidence of their importance to the policy making process. But of what value is the professional bureaucracy in addressing high-risk, technologically-complex national security issues for which there is no organic experience base?

Birkland and Kingdon have held that policy entrepreneurs are the essential element in the policy gestation process. In cases of a universal issue, such as national security, and in instances where there is no well-defined constituency to marshal support for a specific policy choice, i.e., a "free rider" condition, through what fulcrum, e.g., political, economic, or technical, can the entrepreneur gain his leverage?

Formally constituted standing and ad hoc committees, called Presidential Commissions or Councils, are often formed by the Executive Branch to evaluate issues of national policy importance. However, there is a

lack of widespread agreement in the literature on the usefulness of Presidential Commissions as catalysts for change to existing public policy, or for their role in the introduction of new policies and the garnering of the requisite support in the Congress, from which essential funding flows. Senator Edward Kennedy (D-MA) is quoted as saying that Presidential Commissions are "the nation's conscience" being "rejected" or "ignored" by "deaf Presidents, deaf officials, deaf Congressmen, and perhaps a deaf public."[26]

Finally, there are the elected officials, such as the President of the United States, select influential members of Congress, and senior members of their respective appointed staffs who play a significant role in the evolution of national security policy.

This research question and its subordinate propositions seek to determine whom, within the high-risk, high-technology national security policy arena, exercises the greatest influence and leverage among policy makers.

Proposition 10: Policy entrepreneurs are most effective in promoting policy or changes to policy within political arenas having a well-defined constituency.

Policy entrepreneurs are essential participants in the policy community. Birkland observed that entrepreneurs are engaged within the policy community due to their unique technical expertise within the policy field, their political acumen and ability to facilitate the brokering of

agreements and deals leading to new programs and policies, and due to their connection to a problem as a representative of a particular constituency. Birkland found that policy entrepreneurs are particularly important because they lead groups and coalitions that seek to use focusing events for their symbolic potential, thereby advancing issues on the agenda. [27]

Kingdon defined policy entrepreneurs as, "people willing to invest their resources in return for future policies they favor."[28] He further asserted that policy entrepreneurs are essential to the success of a policy initiative; that they bring several key resources into the political fray. He asserted that the ministrations and intervention of a skilled policy entrepreneur considerably enhance a policy issue's prominence on the decision agenda.[29]

This proposition examines Birkland's and Kingdon's assertions concerning the role of the policy entrepreneur in the context of the Information Assurance question.

Proposition 11: The most influential group in the evolution of policy is not the collective professional bureaucracy, but the visible cluster of elected officials made up of the President, the prominent members of Congress, and senior members of their appointed staffs.

Kingdon noted that the importance of the professional bureaucracy in alternatives exploration and policy implementation is tempered by its dependence on political appointees, the president, or members of Congress

to "elevate" their ideas to a place on the policy agenda where they can be assured of receiving serious attention.[30]

Even so, Lipinsky argued, "the latitude of those charged with carrying out policy is so substantial that policy is effectively 'made' by the people who implement it."[31] Jenkins-Smith echoed Lipinsky, expressing a concern that with the "technicization of society," elected officials would become wholly dependent on technical experts within and outside the standing bureaucracy to shape the execution of policy.[32]

This proposition examines which group at the Federal level is most influential in the high-risk, technologically-complex national security policy-making arena.

Proposition 12: Private sector participants in the evolution of high-risk, high-technology policies influence those policies through participation in organized interest groups, industry associations, and through government-solicited participation on Presidential Commissions and Committees.

If elected officials become "wholly dependent on technical experts... to shape executable policy,"[33] then to whom do the key decision makers turn for this requisite technical expertise? In past administrations, technical expertise within the Federal Government has been the purview of the professional bureaucracy. As Kingdon noted, the professional bureaucracy has a wealth of experience in administering current government programs, in dealing with

the interest groups and the congressional politics surrounding these programs, and in planning possible changes in such programs. A final resource of professional bureaucrats is their set of personal relationships and their access to elected decision makers and their key staff.[34]

The Executive Branch also relies on both formally constituted standing and ad hoc committees, called Presidential Commissions or Committees, to evaluate issues of importance to the political agenda prior to sponsoring a bill, issuing an Executive Order, or making an administrative ruling. Rourke and Schulman postulated that Presidential Commissions are created because of a serving president's, "dissatisfaction with the way the ordinary executive agencies perform as policy-making institutions."[35]

Wolanin, in publishing a comprehensive study of Presidential Commissions, categorized them into three base types: policy analysis commissions, long-range educational or technical commissions, and window dressing bodies. Wolanin argued that both the policy analysis and long-range educational or technical commissions are similar, in that their charters, functions, and outputs are actually focused on an empirical analysis of public policy and toward the discovery of useful solutions to problems of interest to the nation.[36] Window dressing commissions, Wolanin said, are designed "to help sell or market a proposal to which the president is already committed."[37]

Smith, Leyden, and Borrelli, re-labeling Wolanin's pejoratively-named "window dressing commissions," as "political commissions," argued that these commissions do engage in essential research and the collection of

decision-useful information. However, they posit that the information provided to the president and the Executive Branch by these commissions is much more of a political than of a technical nature.[38] Their study tested the proposition that the findings and resultant recommendations of political commissions, or those formed to promote presidential policy, are more likely to gain acceptance and catalyze presidential and/or government action than those of advisory commissions.[39] Their results while not necessarily definitive, strongly suggest that it is the determinations of political commissions that catalyze agenda setting and decision making of the executive branch.

The role of the policy entrepreneur as catalyst has been briefly examined in this context. Both Kingdon and Birkland see the entrepreneur as essential to moving a policy up the agenda and along its own lifecycle. It is therefore appropriate to surmise that entrepreneurs would seek the access to decision makers that a Presidential Commission might afford and conversely, that a president might seek out distinguished and influential entrepreneurs from the private sector as commissioners?

This proposition tests the degree to which Presidential Commissions and Committees influence the evolution of national security policy involving high-risk, technologically-complex issues, such as Information Assurance.

Proposition 13: Successful policy gestation requires the strong advocacy of a policy "champion" of sufficient political stature and

political leverage to carry the policy agenda through to a successful implementation.

This proposition probes beyond the persuasive limits of the policy entrepreneur; beyond the bargaining and compromising capabilities of highly visible, elected officials and their high-leverage administrators; even beyond the influence of "distinguished individuals"[40] that may be sought out to serve on Presidential Commissions and Committees. This proposition tests whether policy of a critical national significance, i.e., survival, can be propagated through the system in the absence of a policy champion, or an aspect of what Weber defined as a "charismatic leader."[41]

The charismatic leader relies upon extraordinary personal qualities, demonstrable success, and an ability to overcome routinization and institutional obstacles in the way of achieving important objectives. The charismatic leader is one to whom followers have an emotional attachment; one with a certain presence or ability to inspire followers to greater achievement. But charismatic leadership is not simply inspirational, it must be creative as well, devising solutions to solve the problems of others. Such leadership provides a "spark" that permits societies to grow and develop.[42]

This proposition examines the role of the charismatic leader in policy formulation and whether such leadership is a requisite in the highly automated and bureaucratized public administration of the 21st Century.

Proposition 14: Balkanization of the Federal Information Assurance community results in an ineffective and fragmented policy.

The cohesiveness of relevant communities of policy and technical specialists within a given policy arena vary significantly. Kingdon observed that within some policy areas, the supporting communities of specialists and subject-matter experts function through closed, almost fraternalistic interactions, even when individuals within the group represent many different organizations.[43] Conversely, other groups are much more diverse and fragmented.

The degree of fragmentation within such systemic groups is important because, as Kingdon noted, "the first consequence of system fragmentation is policy fragmentation."[44] The Federal Government, with its myriad of overlapping and often conflicted agencies and bureaucratic institutions, would appear to be a likely victim of a process where policy is developed and implemented in a very compartmentalized, organizationally-closed fashion. This proposition probes this assumption.

RESEARCH QUESTION FIVE: Are existing decision-making frameworks (Classical Models) successful in determining and then addressing high-risk, technologically-complex questions of national security policy?

A useful approach to the study of organizational decision making is through the framework of a decision-making model. Allison used this framework approach, borrowing heavily from Simon and his rationality

constructs, in defining a Rational Actor Model, which Allison labeled the Classical Model, or Model I. However, he believed that this model proved inadequate in explaining the decision processes employed during the Cuban Missile Crisis of October 1962, which Allison analyzed as a case study. Accordingly, Allison proposed two, additional constructs, based upon political analyses, to explain the actions of organizations and political actors not easily explained by either the Rational Actor Model or by its associated quantitative analyses. He proposed two additional models: the Organizational Process Model, or Model II, and the Governmental (Bureaucratic) Politics Model, or Model III.[45]

The Organizational Process Model evolved its decision-making framework based upon predictive behaviors identified through decision-making trends that reflect established and fixed values, procedures, and processes of the organization.[46] The Governmental (Bureaucratic) Politics Model, evolved its decision-making framework based upon the internal politics of large organizations and the internal negotiations and bargaining that take place between individuals and component organizations as they jockey for beneficial position, often at the expense of sister or even parent organizations. Decisions are made within the confines of the political reality, not the rational one.[47]

Cohen, March, and Olsen created the Garbage Can Model to define the process by which a complex organization arrives at decisions while

institutional preferences are problematic, uncertainty exists in its technologic core, and for which individual participation in the decision process is fluid. Choice opportunities are described as a garbage can into which various problems and solutions are dumped by the participants, each to swirl around until such time as a problem and a solution bond together and a decision, by default, is made. March and Olsen contended that organizations existing within these environmental conditions operate as "organized anarchies."[48]

Kingdon's analysis of organizational decision making focused on how choice opportunities compete for position on the political agenda. Kingdon emphasized the importance of focusing events and "windows" of opportunity for addressing specific agenda items. Windows occur when there is a convergence of issues, solutions, opportunities and the right decision-making participants, often through a focusing event, in the same time and space.[49]

This research question examines the efficacy of these constructs, as representative of classic Public Administration models for decision making. It examines whether Classic Models of decision making provide an adequate framework for the analysis of national security decision making and policy evolution in the Information Age.

Proposition 15: Rational choice and operations research models are useful in framing and quantitatively comparing alternatives in complex decision environments, offering optimal normative solutions to aid in the policy decision evolution.

Rational choice theory and operations research are the heart of the analytic process and approach to policy analysis and decision making. The analytical goal of rational choice and operations research is to explain social and political events and phenomena in mathematically-precise terms.

Shepsle and Bonchek, in articulating the underpinnings of the rational choice approach, identified four essential criteria. First, the "individual" is employed as the unit of analysis. The "individual" may represent a person, a country, or any other entity to which a single, unified decision "voice" may be ascribed. Second, since prediction and explanation, rather than description, are the goal, "individuals" are characterized by their beliefs (their rationality) and their preferences for final outcomes. Third, that the "individuals" in the analysis are rational, acting in accord with their preferences and beliefs as to the cause and effect relationship of decisions and subsequent actions. Fourth, that acting rational requires a ranking of final outcomes, a determination of expected utilities for each option, and then the selection of the course of action that has the highest expected utility.[50]

Dr. Russell Ackoff, one of the founders of the field of operations research, offered a pessimistic view of the discipline in 1979, when he said, "the future of operations research is past":

> Managers are not confronted with problems that are independent of each other, but with dynamic situations that consist of complex systems of changing problems that interact with each other. I call such situations *messes* (Ackoff's italics). Problems are abstractions extracted from messes by analysis; they are to messes as atoms are to tables and

> charts...Managers do not solve problems: they manage messes.[51]

In Ackoff's view, the complexities of policy making in the 21st Century would outstrip the ability of the operations researcher to accurately simulate the real world, making any analytical results and their derived conclusions suspect.

This proposition probes the usefulness of the analytic approach to policy analysis through the employment of rational choice theory and operations research in the decision-making process.

Proposition 16: A structured, system-engineered approach to problem analysis, decision making, and policy evolution is an effective alternative to political decision-making processes and models when dealing with high-risk, technologically-complex issues involving national security policy.

March, Cohen, and Olsen's "organized anarchies," within which the Garbage Can Model operates, are characterized by a myriad of things happening within the organization simultaneously. These include changing perceptions and understanding of issues and decision options; the impact of evolving technologies; the ebb and flow of internal alliances and preferences; the uncertainty involved with changes in people, ideas, opportunities, and solution space. March and Cohen introduced the concept of "temporal

sorting" as a mechanism for comprehending the confusing picture of decision making within such organized anarchy.[52]

Kingdon, in building upon the garbage can construct, focused on agenda setting mechanisms as a key to managing the problem, decision-making participant, solution, and choice opportunity "streams" of the garbage can. Kingdon stressed the strategic imperative of not overloading the agenda during such a convergence and the danger to items having real expectations for action through an overloading of the agenda as a result of an insistence on addressing everything relative to the issue at once. By limiting consideration to a single agenda item, the opportunity for opposition to coalesce is limited.[53]

The systems engineering approach offers an effective alternative to the political process model approach by emphasizing performance-based policy making through the identification of specific policy functions and performance requirements and then defining and selecting from a set of candidate solution alternatives that best satisfy those requirements. This proposition probes the validity of this assertion.

Proposition 17: The PIES Model offers an effective alternative construct for theorizing about and framing high-risk, technologically-complex national security policy to the "Garbage Can" and "Streams" models.

The PIES model, offered by the writer, proposes a mechanism for "channeling" the Garbage Can's problem, decision-making participant,

solution, and choice opportunity streams and Kingdon's political, policy, and problem Streams Model." These forces, or vectors, in the PIES construct, act as directional influences upon policy evolution through a system-engineered, structured analysis of policy goals and objectives, functional and requirements analyses, alternatives analysis/selection, and validation/ execution stages of each of seven policy lifecycle phases (set of evolvable policy goals and objectives, implementation alternatives, risk and failure considerations, and political filters).

Given that the political, policy, and problem vectors have, as all vectors do, both "mass" and "direction," their interaction with the policy construct results in measurable influences on the policy evolution. Unlike the Garbage Can or Streams Models, the proposed model suggests that policy can be evolved within a more structured, systems engineering-based construct. And while not immune to the ebb and flow vagaries central to the Garbage Can and the Streams Models, the proposed construct treats these interactions as measurable influences to be factored into the policy calculus, not forces of "organized anarchy" to which the decision-making process is held thrall.

This proposition assesses the comparative value of the PIES model against Public Administration's classic political process models, as represented by the Garbage Can and Streams models.

[1] Jan M. Lodal, Deputy Under Secretary of Defense for Policy, "Implications for National Defense," Proceedings from the Conference on National Security in the Information Age, ed. General James P. McCarthy, USAF [Ret](United States Air Force Academy, 28 February-1 March 1996), 97.

[2] Bruce D. Berkowitz, "Warfare in the Information Age," in *In Athena's Camp: Preparing for Conflict in the Information Age,* ed. John Arquilla and David Ronfeldt, 79-98 (Santa Monica, CA: RAND, 1997), 181.

[3] Roger C. Molander, Peter A. Wilson, David A. Mussington, and Richard F. Mesic, *Strategic Information Warfare Rising* (Santa Monica, CA: National Defense Research Institute, RAND, 1998), xi.

[4] Col. Alan D. Campen, USAF (Ret), "It's Vulnerability, Not Threat-Stupid!," *SIGNAL*, Vol. 52, No. 1 (September 1997), 69.

[5] Jeff Cooper, "Strategic Implications of the Information Age," Proceedings from the Conference on National Security in the Information Age, ed. General James P. McCarthy, USAF [Ret](United States Air Force Academy, 28 February-1 March 1996), 85-86.

[6] Lodal, 97.

[7] Ibid., 85.

[8] Molander, 28.

[9] Charles E. Lindblom and Edward J. Woodhouse, *The Policy-Making Process*, 3d ed (Upper Saddle River, New Jersey: Prentice Hall, 1993), 62-63.

[10] Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York, NY: The Free Press, 1986), 136.

[11] James D. Thompson, *Organizations in Action* (New York, NY: McGraw-Hill Book Company, 1971), 145.

[12] Thompson, 147.

[13] Kenneth J. Meier, "Bureaucracy and Democracy: The Case for More Bureaucracy and Less Democracy," *Public Administration Review*, vol. 57, no. 3 (May/June 1997), 197.

[14] Lindblom and Woodhouse, 63.

[15] Neustadt and May, 13.

[16] Ibid., 275.

[17] Thompson, 135.

[18] Neustadt and May, 136.

[19] Donald A. Schon, *Beyond the Stable State* (New York: W.W. Norton & Company, 1971), 11.

[20] Ibid., 32

[21] Thompson, 126-127.

[22] Phillip Selznick, *Leadership in Administration* (Berkeley, CA: University of California Press, 1984), 35-36.

[23] John W. Kingdon, *Agendas, Alternatives, and Public Policies* (New York, NY: HarperCollins College Publishers, 1995), 94-95.

[24] Murray Edelman, *The Symbolic Uses of Politics* (Urbana, Illinois: University of Illinois Press, 1985), 6.

[25] Thomas A. Birkland, *After Disaster; Agenda Setting, Public Policy, and Focusing Events* (Washington, D.C.: Georgetown University Press, 1997), 22.

[26] Thomas Cronin, *The State of the Presidency* (Boston: Little, Brown, 1975), 63.

[27] Ibid.,18.

[28] Kingdon, 204.

[29] Ibid., 205.

[30] Ibid., 32.

[31] Michael Lipsky, "Standing the Study of Public Policy Implementation on its Head," in Walter Dean Burnham and Martha W. Weinberg, eds. *American Politics and Public Policy.* (Cambridge, MA: MIT Press, 1978), 397.

[32] Hank C. Jenkins-Smith, *Democratic Politics and Policy Analysis* (Pacific Grove, CA: Brooks/Cole Publishing, 1990), 41.

[33] Ruth Gillie Kruger, *Analyzing American Social Policy: A Study of the Child Support Provisions of the Personal Responsibility and Work Opportunity and Reconciliation Act of 1996,* DPA Dissertation, University of Southern California, December 1998, 43.

[34] Ibid., 33

[35] Francis Rourke and Paul Schulman, "Adhocracy in Policy Development," *Social Science Journal,* vol. 26, no. 2 (1989), 131-142.

[36] Thomas Wolanin, *Presidential Advisory Commissions* (Madison: University of Wisconsin Press, 1975),13.

[37] Ibid., 15.

[38] Daniel Smith, Kevin Leyden and Stephen Borrelli, "Predicting the Outcomes of Presidential Commissions: Evidence from the Johnson and Nixon Years," *Presidential Studies Quarterly,* Vol. XXVIII, no. 2 (Spring 1998), 273.

[39] Ibid., 278-283.

[40] Executive Order 12882, 23 November 1993.

[41] Hans H. Gerth and C. Wright Mills, *From Max Weber: Essays in Sociology* (New York, 1958), 246, cited in Edelman, 77.

[42] Robert Denhardt, *Theories of Public Organizations* (Monterey, California: Brooks/Cole Publishing Company, 1984), 31-32.

[43] Ibid., 118.

[44] Ibid., 119.

[45] Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston, MA: Little, Brown and Company, 1971), 5.

[46] Ibid., 6.

[47] Ibid., 6-7.

[48] James G. March and Johan P. Olsen, *Ambiguity and Choice in Organizations* (New York: Columbia University Press, 1982), 175, 247-249.

[49] Kingdon, 194-195.

[50] Kenneth A. Shepsle and Mark S. Bonchek, *Analyzing Politics* (New York: W.W. Norton & Company, 1997), 35.

[51] Russell Ackoff, "The Future of Operations Research is Past," *Journal of Operational Research Society,* Vol. 30, No. 2 (New York: Pergamon Press, Ltd., 1979), 90-100.

[52] James G. March and Johan P. Olsen, *Rediscovering Institutions* (New York: The Free Press, 1989), 11.

[53] Kingdon, 185.

CHAPTER FOUR

BACKGROUND--WAVES OF CHANGE AND THE INFORMATION AGE CHALLENGE TO NATIONAL SECURITY

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

The global community is in the relative infancy of a new age of civilization, the Information Age, the third great, fundamental paradigm shift in the history of humankind. The Agricultural Revolution reshaped and changed the global society ten millennia ago. The Industrial Revolution radically altered the basic fabric of civilization a short 350 years ago. Now, the United States finds itself in the vanguard of the next, great fundamental paradigm shift in the framework of human existence, what futurist Alvin Toffler defined as the "Third Wave."[1]

The purpose of this chapter is to provide essential historical framing and background to the Information Assurance study, tracing key events and developments brought about through the advent of the Information Age. The impact that Information Technology, the Internet and global interconnectivity, and Strategic Information Warfare (SIW) and cyber terror have had on the national and global societies is examined in detail. The chapter is organized topically. Chronologically ordered data is provided in support of each topical area.

WAVES OF CHANGE AND THE THREE AGES OF HUMANKIND

The First Wave of change, launched by the Agricultural Revolution 10,000 years ago, sparked the transition of humankind from hunter-gatherers to farmers. The First Wave catalyzed the formation of the great peasant societies of antiquity and the establishment of the first permanent towns and cities. The First Wave witnessed the advent of formalized trade employing bartering and the first use of exchange systems involving the concept of money. The First Wave also witnessed the first organization of societies by the instruments of centralized authority and government. First Wave cultures continue to exist in parts of the world today, principally in the remoter parts of Africa, Asia, and South America. In all First Wave cultures, arable land is the binding force and the basis for the economic system, life, culture, family, organizational structure, and politics of the society.[2]

The Second Wave was catalyzed by the Industrial Revolution. With its origins in Great Britain's late 17th Century textile industry, the Industrial Revolution represented a fundamental shift in the focus of society away from the arable land and into the factory and cities. Populations moved, en masse, as labor resources migrated to the great, centralized industrial complexes in search of work. Natural resources, infinitely renewable under the mild tensions of an agrarian culture, were exploited and the natural balance stressed to meet the global appetite and nation-state competition for essential raw materials.

The decentralized, loosely confederated, feudal, monarchic governments of the agrarian society were supplanted by the tightly integrated, economic and regulatory frameworks, professional administration and associations (i.e., guilds, trade groups, etc.), and technical specializations of industrialization and centralized government. The Industrial Age became the catalyst for the evolution of large structural and control organizations in society, the foundations of the bureaucratic state. As Hart and Scott opinioned, "Whatever is good for man can only be achieved through modern organization."[3]

The Information Age, what Toffler defined as the Third Wave, began in 1955, mid-way through the first decade in the history of the United States in which white-collar and service workers outnumbered blue-collar production workers. This was also the first decade in which advanced technologies, such as those that made possible commercial jet travel, the television, the computer, and many other high-impact technological developments, emerged from the research laboratory and went directly into the societal mainstream.[4]

INFORMATION TECHNOLOGY AND THE OPENING OF PANDORA'S BOX

The Microprocessor Revolution

The key enabler for the Information Age has been the invention and evolution of the microprocessor. Thirty-five years ago, state-of-the-art, room-

sized mainframe computers were both computationally challenged and prohibitively expensive. In contrast, over the past ten years, the individual microprocessors embedded in commercial desktop computers designed for general purpose use in the office and the home have exceeded the total computational power of those mid-1960s mainframe computers several times over.

Microprocessors have become so relatively inexpensive and commonplace in the societal mainstream that their value as mass marketing and consumer information collection tools have exceeded their unit cost. For example, in February 1999, a Pasadena, California, firm offered free personal computers to the first 10,000 adults holding a major credit card and willing to trade their electronic privacy in exchange for computer ownership. Free-PC.com offered these upper-end computers to individuals willing to disclose personal information advertisers covet, such as age, income, hobbies, and other details of their private lives. More importantly, these individuals agreed to allow Free-PC.com to electronically monitor the use of their computers 24 hours a day.[5]

Privacy advocates noted that through this Faustian deal, consumers unable to afford a home computer were willing to trade individual privacy in exchange for a $500.00 computer--albeit one that exceeded the computational capability of those 1965 mainframe computers--and access to the Internet and the electronic commerce mainstream. The response to the Free-PC.com offer captured the attention of other commercial companies

hoping to broaden their markets: within 24 hours of making the offer, all 10,000 personal computers had been placed.[6]

Societal acceptance of the role of computers and computer networks as a fundamental part of daily life, coupled with accelerating advances in Information Technology spurred by quantum leaps in microprocessor design and software innovation, have fundamentally changed the dynamics of life in the Information Age. Prior to 1996, nearly every computer built was designed as a stand-alone data processor. Within each of these computers, the core logic arrays were designed to address problems in linear fashion, i.e., each element of the computational problem in sequence and at the rate of a single transaction at a time. By 1996, personal computers were being mass produced, designed around inexpensive logic chips the size of postage stamps, each of which cost less than $50.00 to produce and market. By 2000, those costs had been halved, while processor capacity had increased four fold. Each of these integrated circuits, produced by the hundreds of millions, had the capacity for executing instructions at a rate measured in millions of theoretical processes per second (MTOPS).[7]

These new and inexpensive microprocessors were designed to solve all elements of the computational problem simultaneously, thus increasing both the speed and through-put of the computer, as well as their capacity to resolve highly complex and integrated problems within a single processor. Most importantly, the new problem-solving logic of this generation of microprocessor permitted them, for the first time, to be easily networked

together. Networking is the core technology that permits the creation of massively parallel processing strings of individual computers, each capable of executing complex instructions and solving complicated problems that only the most powerful supercomputers could tackle less than five years ago.

Figure 4-1 graphically illustrates the growth in personal computer performance, measured in the hundreds of theoretical processes per second in 1992, to a projected 16,000 million theoretical processes per second in 2004.[8] A rule of thumb in the computing industry is that the computational power of commercial microprocessors doubles every eighteen months. This axiom, known as Moore's Law, was named after Gordon Moore, who in 1965 and as head of research and development at Fairchild Semiconductor Corporation, predicted that the number of integrated transistors etched into

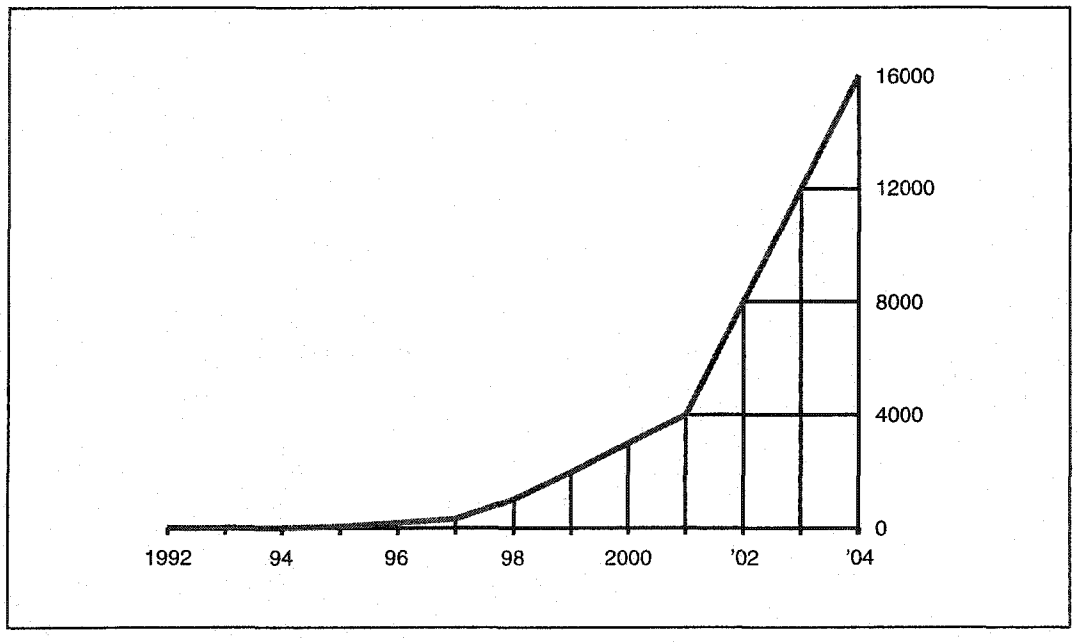


Figure 4-1: Growth in Computing Power 1992-2004 as Measured in Millions of Theoretical Operations per Second (MTOPs)[9]

a silicon microchip would double every year from the original four in 1961.[10] In 1968, Moore, now Chairman and CEO of Intel, revised his prediction to a rate of doubling every eighteen months. In the past thirty years, the actual rate of doubling has varied between nine months and two years, but the average rate of change has remained consistent with Moore's prediction.[11]

This near-exponential advance in computer processor technology, manifesting itself in state-of-the-art, off-the-shelf commercial products for a world market that is increasingly difficult, if not impossible for the United States to control, poses a growing national security challenge:

> We used to be able to control these things pretty effectively because there were only a few hundred machines we had to worry about and a comparable number of organizations we didn't want to have them. Now, companies are producing microprocessors by the tens of millions that are more powerful than some of the most powerful supercomputers we had ten years ago, and they are doing it around the world, How are you going to control that?[12]

Under provisions of Public Law 105-85, the 1998 National Defense Authorization Act (NDAA), exporters must provide the Commerce Department with prior, written notice of an intent to ship computer systems having greater than 2,000 MTOPS (millions of theoretical operations per second) capacity to countries on the government's restricted list (i.e., Tier III countries, including India, Pakistan, all Middle East countries, Maghreb, the countries of the former Soviet Union, China, Vietnam and Central Europe). Upon written notification, United States export control agencies have ten

days to inform the seller it must apply for an export license prior to shipment. In July 1999, President Clinton raised that level to 6,500 MTOPS. That decision became effective on 23 January 2000, at the end of the mandatory 180-day Congressional notification period.[13]

However, the ability to create massively parallel processors from even today's home computers circumvents this restriction. As a result, Export Restrictions List countries can legally obtain computing capacity to satisfy many of their more complex and military-related simulations and modeling needs, enabling these countries to produce some advanced weapons and commercial products on par with the United States (see Table 4-1).[14]

Millions of Theoretical Processes per Second (MTOPS):	**Potential Military Use:**
4,000 MTOPS	Designing some aircraft radar and antisubmarine sensors.
12,000 MTOPS	Forecasting the weather to optimize the timing of military actions.
21,000 MTOPS	Modeling the impact of missiles on buildings to ensure that the missiles do no more than the intended damage.
32,000 MTOPS	3D modeling of how chemical warfare gases pass through different materials, to aid in the design of protective gear.
70,000 MTOPS	3D modeling of an operating submarine to help design a vessel that is difficult to detect, or of a shell striking a tank to aid in better armor.
100,000 MTOPS	Modeling the aging process in nuclear weapons to help ensure that they still operate or are replaced.

Table 4-1: Typical Military Use of Computing Power/Capacity[15]

Market forces often are at odds with national security considerations. Clinton Administration policy decisions, with respect to computer export controls, have sought a balance between the two. Easing computer export restrictions on Tier III countries, such as China, are viewed by some as pandering to special interests. Clinton Administration officials portrayed their decisions as a defense of the United States computer industry and a recognition of the global computer market reality that powerful computers are globally available, rendering United States' export restrictions ineffective.[16]

Cooperative international commercial ventures, especially in the microprocessor-controlled, digital telecommunications arena, inevitably result in the exchange or transfer of at least some sensitive technologies. A variety of Congressional hearings and inquiries were held during the Fall of 1998, concerned with the transfer of sensitive missile technology to China, which allegedly occurred in 1996 through a joint commercial venture with two, major United States defense contractors, Hughes and Loral Space and Communications. Congress investigated whether the two United States companies compromised national security by providing sensitive technology to China during post-launch failure analyses after the unsuccessful launch of a United States commercial communications satellite aboard a Chinese missile.[17]

An Air Force intelligence assessment made in late 1997, over a year after the data transfer allegedly occurred, concluded that China may indeed

have improved its ballistic missile technology as a result. The CIA disagreed with the Air Force finding, stating in 1998 that whatever unintentional technology transfer did occur did no harm to the national security interests of the United States. This was the substance of the testimony provided the Senate Commerce Committee by Principal Deputy Assistant Secretary of Defense Franklin Miller on 17 September 1998 when he testified, "I do not believe there has been any improvement to Chinese ICBM capability (as a result of any technology transfer)."[18]

As demonstrated in the China missile case, Global Market ventures often involve the exchange of some critical information and technology between United States corporations and foreign companies or governments. When these foreign entities employ dual use technologies to gain a market or military advantage over the United States, both United States trade and national security policies are called into question.

In the Beginning: Origins of the Internet

Microprocessors alone have not created the Information Age. Although microprocessor-based computers have evolved into powerful, relatively inexpensive, stand-alone tools, it is the ability to network these computers into ever-expanding communities of interconnected devices that has been the catalyst for the Information Age global change society.

Key to understanding the set of issues involved in the Information Age evolution of the nation's critical information infrastructures is an

understanding of the evolution of that networking phenomenon. The Internet is the systemic, network "glue" that has made global electronic interconnectivity a reality. With the concurrent advent of multi-tasking computers, the Internet has made worldwide electronic commerce a reality, bringing both benefit and risk to United States' critical information infrastructures.

In 1966, when Robert Taylor, head of the Advanced Research Projects Agency's (ARPA) Information Processing Techniques Office, proposed improving the research information sharing efficiency of ARPA's far-flung research staff, critical infrastructure protection had yet to surface as an issue of United States national security concern.[19] What Taylor needed was a way to link ARPA's research and development centers together. He tapped Larry Roberts, a gifted computer scientist at the Massachusetts Institute of Technology's Lincoln Laboratory, to figure out a way to network these geographically dispersed centers together via computer.

By 1968, Roberts and his colleagues had developed a specification for this new "computer network," dubbed ARPANET. It would employ a message parsing technology originated by Paul Baran, a RAND Corporation researcher working in Santa Monica, CA under contract to the United States Air Force. In 1965, fully three years before Taylor's team issued its Request For Proposal (RFP), the DOD had judged Baran's "message block" or "packet switching" ideas too technically advanced for its own, relatively new Air Force Defense Communications Agency (AF/DCA) to tackle. AT&T, to

whom the Air Force turned for help, also felt the job to be technically infeasible. As a result, both the Air Force and AT&T lost the opportunity to "father" what would initially serve as the ARPANET, but which later would evolve into the Internet.[20]

In 1969, the Cambridge, MA engineering firm of Bolt Beranek and Newman, Incorporated, led by computer scientist Severo M. Ornstein, bid for and won the right to engineer and implement the first node of the ARPANET. The DOD approved the bid and commissioned ARPANET to promote networking research.[21] By 1971, ARPANET was an interconnected network of 15 nodes, representing research institutions across the country. In 1972, an ARPANET demonstration for the International Conference on Computer Communications so impressed the research community in attendance that a new computer was interfaced into the network every 20 days from then on.[22]

Throughout ARPANET's early years, the influence of the military on the new technology was minimal. Beginning in the early 1970s that began to change and by 1975, military message traffic on the ARPANET had increased geometrically. AF/DCA was subsequently ordered to take over control of the network. During this same time period, ARPA was experimenting with new military applications for ARPANET's packet switching technology; experiments that were to have a direct bearing on an evolving concept--a network formed between many other networks--the Internet.[23]

The most significant technical challenge faced by ARPA in maturing the Internet concept was evolving a technique for interconnecting independent computer networks that, in effect, spoke different computer languages. That particular challenge was overcome by ARPA's Robert Kahn and his associate, Vinton Cerf. Working through the early 1970s, Kahn and Cerf devised a message exchange protocol that would provide essential message addressing, routing, traffic management, and other electronic postal services to make networking of networks possible. In May 1974, Kahn and Cerf published their results and the first and still most widely employed of the computer networking protocols, Transmission Control Protocol (TCP), was established.[24]

By 1982, DOD formally adopted the Transmission Control Protocol/ Internet Protocol (TCP/IP) as the ARPANET and DOD standard.[25] ARPANET access required TCP/IP-compliance and the Internet was born. By 1984, the number of host computers connected to the Internet exceeded 1,000. Recognizing the civilian potential for trafficking on the new Internet, in 1984, the DOD split ARPANET in two. The new military half, MILNET, would ensure the military had its own reliable computer network, while the rump ARPANET continued to serve other users.[26]

In 1984, the National Science Foundation optioned to establish its own high-speed computer network "backbone" to interconnect its supercomputer research centers. By 1986, the NSFNET, connecting five supercomputer centers on a 56-kilobit/second backbone, was brought on-line. Interest in the

use of NSFNET quickly grew as NSFNET diversified, linking together government and university research centers across the country over telecommunication lines that were up to 25 times faster than ARPANET lines. By 1989, NSFNET was supporting over 100,000 installed computer nodes.[27] NSFNET use had become far greater than that of the ARPANET. ARPANET was obsolete, On 1 June 1990, it was de-installed, ending the system's 21-year life.[28]

In the post-ARPANET era, two events occurred in rapid succession that transformed the NSFNET into the World Wide Web. In 1991, NSF officials opened their network to commercial users, ushering in the era of the Internet Service Provider (ISP) and e-Commerce. In 1992, British physicist Timothy Berners-Lee, working at the Center for Nuclear Research in Geneva, Switzerland developed a software suite allowing him to organize and link information from any number of Internet nodes. Hypertext Markup Language (HTML), as the new software was named, would allow anyone wanting to access a reference file to simply click on a word, opening that file immediately, without having to search a directory for the document. This was made possible by implanting in the trigger word the command that would open the file. This reduced the complexity of navigating the Internet to a few computer mouse clicks[29]

The release of the HTML software by CERN, coupled with the NSFNET backbone capabilities, ushered in a new era for the Internet. By 1992, the combination of faster computers and graphical user interfaces

(GUIs) created an explosion of Internet interest and uses. At the end of 1992, there were one million host computers linked to the Internet/World Wide Web.[30] In 1993, Mosaic, a graphical "Web browser," developed at the NSF-funded National Center for Supercomputing, was released for public use, causing traffic on the World Wide Web rapidly escalated. By 1994, Netscape and other start-up companies had formed to develop commercial web browser technologies and products. By 1996, the number of Internet hosts had reached 12.8 million subscriber systems.[31] Through the end of 2000, growth continues unabated.

Between 1990 and 1999, the number of United States households owning at least one personal computer rose from 22% to 53%, while the number of United States computers shipped annually increased from 9 million to 43 million. The number of households with Internet access grew from 0 to 38%. The total number of global Web sites grew from 313,000 to 56 million. Sales by United States software firms more than doubled, from $63 billion to $141 billion.[32]

Universal Use of Commercial Standards and Products

One of the most significant bi-products of commercial globalization has been the evolution of universal standards. Standards are essential for the interconnectivity of essential Information Technologies. Without standards, networking of computers would be impractical.

The impact on national security of the transfer of enabling technology or technical information, as a bi-product of universal standards and international commerce, is very real. As the Information Age needs for the Global Information Infrastructure are addressed, many dual-use technologies are at the heart of technology transfer policy issues.

Dual-use technologies are those originally developed either specifically for national security applications or commercial purposes, but which have significant applicability in either sector. Examples of dual-use technologies include information security (e.g., encryption), communication, navigational, network, electronics design, advanced manufacturing and space flight technologies. Such technologies can be used offensively, as a means of market penetration, and defensively, as a means of ensuring or preserving economic competitiveness.[33]

Investing in dual-use technologies and accepting the inevitable conditions the government imposes on such technology development and propagation, can have unforeseen consequences. Homogeneity versus heterogeneity in the design of computer hardware and software has been the key architectural issue for the computer industry and its customers over the last thirty-five years. Market forces, and the emergence of international computing, networking, and electronic data interchange (EDI) standards, have precipitated a major paradigm shift in the computer industry. Vendor-proprietary systems, i.e., unique hardware and software, sharing little or no commonality with any other vendor's hardware or software, an accepted

industry standard through the early-1980s, had given way to standards-based systems, employing common interface buses, operating systems, exchange protocols, languages, and data formats. This standards-based evolution paved the way for the unprecedented, computer-based, worldwide electronic interoperability, e.g., the Internet and the World Wide Web.

Life cycles of six to eight months for Information Technology products make the development and implementation of standards critically important. For the military, standards are so fundamentally essential to interservice and international force operations that they are viewed as a major factor in enhancing force survivability. In 2001, standards dictate the methods and processes by which the United States military's various command, control, communications, and intelligence (C4I) systems evolve and once fielded, how they interoperate.[34]

Interface standards are used to specify the characteristics of systems, subsystems, equipment, assemblies, components, items or parts to permit interchangeability, compatibility, or communications. In keeping with current Department of Defense acquisition reform policies, inserting defense requirements into commercial standards is DOD's preferred approach for ensuring interoperability.[35]

The Defense Department's Joint Technology Architecture (JTA), the foundation for all information systems within the Department of Defense, is predicated on 160 standards, of which a growing majority are commercial.

Defense Information Agency's (DISA) Information Processing Standards Department Chief Wilbert Berrios noted in July 1997:

> There is a special list of mandated standards within this architecture for all of the services to use at a minimum in building their systems. This architecture provides approximately 160 standards, with 60 percent as commercial standards. The remaining 40 percent are military-specific standards.[36]

The DOD's reliance and use of commercial standards and off-the-shelf products was greatly accelerated through the findings of President Ronald Reagan's Blue Ribbon Commission on Defense Management, the Packard Commission. The Packard Commission, named in honor of its Chairman, David Packard, co-founder of commercial computer giant Hewlett-Packard, was formed on 15 July 1986, under the auspices of President Reagan's Executive Order to study the operations of the Defense Department.[37]

Among its many findings and recommendations, the Packard Commission urged the President to establish mandates for the use of commercial products and standards throughout the DOD:

> Rather than relying on excessively rigid military specifications, DOD should make greater use of components, systems, and services available "off-the-shelf." It should develop new or custom-made items only when it has been established that those readily available are clearly inadequate to meet military requirements.[38]

Ironically, the government's embracing of commercial-based, global electronic exchange and computer-based interoperability standards had the unintended consequence of creating heightened vulnerabilities in United

States electronic infrastructure in two, fundamental ways. First, by relying on commercial-off-the-shelf software products for a large percentage of its computing needs, the government limited its product selection to those developed in response to the commercial market demand. Limiting the physical variety and number of the product set greatly reduced the complexities associated with gaining unauthorized access into these commonly-held systems.

Second, by discouraging the development of more costly, mission-unique microprocessors, the government's reliance on commercial vendors to satisfy its computing needs has increased significantly. Most of these suppliers are foreign owned and located in countries outside the jurisdiction of the United States. Since the microprocessor is the very heart of every computer, modern weapon system, satellite system, transportation system, and telecommunications system in world-wide use today, this issue remains of significant strategic concern in 2001.

On March 23, 1996, in the Washington, D.C. offices of the RAND Corporation and during a RAND-facilitated exercise undertaken for the United States Defense Advanced Research Projects Agency (DARPA), this concern was formally examined. Using "The Day After" exercise methodology developed over the past several years under the leadership of RAND scientist, Roger Molander, RAND conducted:

> An exercise informing DARPA staff and selected representatives of the user community of the principal features of (defensive) information warfare (IW) and identifying for

participants the future demands that IW may place on DARPA information technology programs.[39]

The exercise examined the case pathologies of a recent series of cyber-based attacks on the United States critical information infrastructures. The results of the exercise revealed that a major enabler for these attacks was the "limited diversity in our key infrastructure systems," i.e., the standards-based evolution and drive toward commonality and interoperability has created vulnerabilities in the nation's computer systems. The real irony was that commonality and specialization, two attributes of Industrial Age culture, had helped drive system diversity out of the market. Market pressures, principally driven by first government and then commercial insistence on systems commonalties, had created this particular vulnerability in United States critical information infrastructures.

Specifically, the exercise revealed a host of vulnerabilities in the United States' microprocessor-based, digital telecommunications designs, revealing that all of the digital telephone switches employed by the United States telecommunication industry are manufactured by one of three companies: Nortel, Siemens, or AT&T. All three of these companies' digital switches are based on either Compaq's DEC VMS or AT&T UNIX operating systems. Most Internet nodes in the United States today operate over common versions of the UNIX operating system. The United States telephone signaling system uses the Internet's Simple Message Transmission Protocol (SMTP). A flaw discovered in any of these common

components would expose the entire network to cyber exploitation and potential large-scale service disruption.[40]

The analogy in biological systems is striking. Through the study of natural systems, biologists have identified the phenomenon of bio-diversity, nature's method of assuring the survival of an individual species. By allowing subtle differences within the genetic coding of members of an individual species, nature ensures that each member of the species is genetically unique, with each having variable levels of susceptibility to the same diseases, thus insuring the survival of naturally-selected members of the species.

In a similar manner, government may now be called upon to serve in "nature's role," mandating that sufficient dissimilarity be engineered into critical systems as a hedge against cyberattack. Without such intervention, the commercial trend toward uniformity and "massification" of critical system hardware and software components will continue to place the United States' critical information infrastructure at risk.

Data and Access Protection: Encryption and Encryption Export Controls

One of the most sensitive of computer technologies controlled by the United States Government is encryption. Encryption is the process of encoding data or communications in a form that only the intended recipient can understand. For most of its history, cryptography, the science of information encryption, was the exclusive purview of military and intelligence

organizations. These government organizations built and maintained their own cryptographic systems out of view of a general public who, in an essentially paper-based world, had no need for such tools or information protections.

With the advent of the Information Age, the need to protect electronic data from unauthorized access and use became an imperative for individuals and governments alike. The Internet has not been as successful a commercial medium for electronic commerce as it could be, because some of those who might otherwise use it feel that the data transmitted is not secure. Encryption of data transmitted over the Internet could provide that needed level of protection.

For several decades, the United States Federal Government has been concerned about the proliferation of commercial encryption products, especially digital ones. Domestically, the government agued, the widespread sale and use of strong encryption would retard law enforcement's ability to perform legitimate wiretaps and to read computer data seized through lawful means. Internationally, government control on the export of encryption products has traditionally been even more restrictive. Current restrictions on the sale and export of advanced encryption software is grounded on the presumption that its use would severely weaken the ability of law enforcement and national security agencies to intercept and decode the electronic communications of terrorists, transnational criminal organizations, and governments hostile to the United States.

To control the commercial proliferation of sophisticated encryption software, the Federal Government devised a two-step strategy. First, it resorted to a law, the Arms Export Control Act (22 U.S.C. 2571-2794), designed to control the export of arms and munitions. Encryption software beyond a certain strength, in this case forty bits, "qualified" as a munition under the Act, and was therefore illegal to export without a hard-to-get Federal license.[41]

The second step of the strategy was to adopt a Public Key Encryption (PKE) standard and a key escrow program, requiring software vendors and encryption users to escrow keys to all cipher products with the United States Government. The first of these key escrow, or "spare key" programs, was the now infamous Clipper Program, which made the term Clipper virtually synonymous with key escrow. The program made its much-heralded public debut on 13 April 1993. Since its debut, the government has worked hard to promote key escrow as a practice to be extended to all domestically sold encryption products. The government has consistently held that widespread use of strong encryption without government key escrow would effectively end the use of wiretapping as a tool for fighting crime.[42]

The computer industry, the American business community, and privacy advocates united in vehement opposition to this government-mandated key escrow scheme. As a result, the government's Escrowed Encryption Standard (ESS) proved hugely unpopular. Consequently, software developed by American commercial companies largely ignored

provisions for serious access protection, making most of the world's commercial-off-the-shelf (COTS) software extremely vulnerable to fairly simple cyberintrusion techniques and tools.[43]

When coupled with the strict export controls and associated technical limitations that have been applied to information security products developed within the United States for international sale, these government policies had a debilitating effect on the commercial software industry. Domestically-produced encryption products developed for export were limited, by law, to first 40-bit, then 56-bit maximum key lengths. Because of tightly controlled government regulations and oversight, the licensing process for the export of these products was very restrictive. As a result, the international market for these products was largely abandoned to foreign-based vendors, many of whom are state-sponsored and, therefore, outside the jurisdiction of United States export control laws. Israel and France are two of the more prominent sponsors of information security product engineering and development. The domestic market niche was left to a few United States software security firms, most of whom had strong ties and a business base with the United States defense and intelligence communities.

Until recently, encryption software available from foreign sources was considered an insignificant factor in computer-related law enforcement or national security issues. Until very recently, foreign-engineered products lagged in technical sophistication in comparison to equivalent American products. That has changed.

With the advent of the Internet and electronic commerce, the need for broader-based encryption tools for securing electronic funds transfers, electronic data exchanges, interpersonal electronic communications, and e-Commerce transactions became an absolute imperative, creating a commercially-based "irresistible force" pitted against a restrictive, government encryption policy "immovable object."

WARFARE AS A REFLECTION OF THE AGES OF HUMANKIND

The Information Age has created entirely new structures for global trade, global economics, and a global society at a rate that threatens to overwhelm countries whose development has not kept pace. Countries, such as Tibet in Asia, and Zambia and Botswana, in Africa, continue to exist much as they have for thousands of years as essentially agrarian societies. Other small countries, such as Malaysia, Singapore, and Indonesia, embracing Third Wave approaches and technologies, have become global trading giants, with economic wealth and power far in excess of their physical size and organic natural resource base.

In stark contrast, developing countries such as India and, particularly, China, having struggled for decades to transform themselves into Second Wave industrial nations, must now face the daunting prospect of having to integrate yet a third infrastructure into uncomfortably coexistent Agrarian and Industrial cultures. Internal tensions created by the incessant social, cultural, economic and technological clashes of competing "societies within a society"

have created significant internal governance challenges for these nations. These forces of competing national will and character make such nations a major concern of United States national security policy.

As much as it has had a profound influence on the evolution of new structures for global trade, global economics, and a global society, the Information Age has had an equally profound effect on the art of war. Warfare by any nation-state is a reflection of its society, its culture, and the critical national infrastructures that sustain it. Table 4-2 summarizes the attributes of each Age of Man (Toffler's Waves) and the impact each has had on the nature of war.

During the Agrarian Age, the link between war and the land was strong. The goal of Agrarian Age warfare was control of the land. The objective was the destruction of an adversary's ability to defend his land while ensuring an ability to defend one's own. The Industrial Revolution brought about a fundamental shift in both the rationale for waging war and in how wars were to be fought. The combination of scientific/technical advances and manufacturing processes led to weapons of increasing sophistication and lethality, setting the stage for the Industrial Age wars of the 20th Century.[44]

The shift to an Industrial Age culture precipitated a shift in the objective of war itself, which was no longer control of the land, but control of the principal sources of Information Age wealth: raw materials and the means of production. Military campaigns focused on control of an adversary's

sources of raw materials and destroying his labor base and production capacity.

Wave:	First Wave:	Second Wave:	Third Wave:
Age of Humankind:	Agrarian Age	Industrial Age	Information Age
Physical Security Provided By:	Small warrior class, supported by mercenaries, augmented by large groups of peasant militia	Professional military augmented by massed citizen soldiers	Numerically small, high technology military directed by information-centric leaders
Dominant Societal Force:	Land Lords, family, tribe, city, state	Nation-state; Industrialists/factories	Electronic commerce; non-governmental organizations (NGOs); global trade *conglomerates*
Economy Controlled By:	Trade/barter	Money	Electronic symbols (e.g. monetary net worth = summation of data base values)
War Characterized By:	Representational Conflict	Massive armies; high casualties	Information Attacks; minimal physical casualties
Ultimate Destructive Capability:	Individual stabbing weapons employed en masse; early firearms and gunpowder	Weapons of mass destruction (nuclear, chemical, biological)	Critical Infrastructure destruction
Goal of Conflict:	Control of the land; destroy enemies ability to defend and control land	Destruction of adversary's means of industrial production	Destruction or control of adversary's capacity for coordination of socio-economic inter-dependencies
Leadership:	Heroic Leader; Ruling Elite	Hierarchical	Lower level empowerment; flatter decision structures
Information Based Warfare:	Limited	Yes	Yes
Information Tech Dominant In War:	No	Limited	Yes
Information War:	No	No	Yes

Table 4-2: Attributes of the Three Ages of Humankind and Their Impact on Nation Conflicts

The ultimate expression of Industrial Age warfare was the Second World War (1939-1945). Fought across six of the world's seven continents

and all of its oceans, World War II was responsible for the deaths of over fifty million people, left hundreds of millions of others physically or psychologically scared for life, and devastated much of the industrial heartland of Western civilization.[45]

The atomic bomb, the penultimate statement of Industrial Age power, ushered in an entirely new calculus in nation-state conflict. No longer simply a matter of destroying the military and war-making capacity of an enemy, the new object of strategic war was to lay waste an adversaries entire societal infrastructure, such that it caused it to cease to exist as a functioning society. Only the stark reality of Mutual Assured Destruction (MAD) staved off nuclear Armageddon during the years of the Cold War.

With the ascendancy of the Information Age, the objectives, implements, and rules of war continued to evolve. Where superior mass and mobility were the keys to success in Industrial Age conflict, the Information Age determinates of success are much more a factor of who knows what and when. An ability to achieve dominant battlefield awareness, while denying an adversary the same, is the key to military success in the Information Age.[46]

The Gulf War, perhaps the last, major Industrial Age clash of arms for the United States, was also the first true conflict of the Information Age. Launched initially from the air on January 17, 1991, Operation Desert Storm, the campaign to drive Iraqi forces out of occupied Kuwait, culminated in a massive, blitzkrieg-style armored attack that began February 24, 1991, and

resulted in the utter annihilation of the in-theater Iraqi land forces by February 27, 1991. On paper, the conflict Iraq's Saddam Hussein promised to be the "mother of all battles," could well have been. Instead, the "mother of all battles" became the "highway of death" for the overmatched Iraqi military forces. Coalition losses totaled less than 400 killed in action compared to Iraqi losses of over 100,000 soldiers killed in action. An even greater number of Iraqi troops surrendered or were captured in a "war" fought over the span of only 100 hours.[47]

How was this possible? At the start of the Gulf War, the 900,000 man Iraqi army outnumbered the coalition forces by a factor greater than two to one in armed personnel, tanks, artillery, and every other category of military equipment, save combat aircraft. Iraq's modern military equipment and state-of-the-art combat systems included many of the best weapon systems available on the international arms market.[48] The Iraqi's were well entrenched, enjoyed relatively short lines of communication and logistics, and were fighting on their "home turf."

The coalition edge in Desert Storm was Strategic Information Warfare (SIW). The real-time intelligence, gathered and utilized by coalition forces in the Gulf War through networked command, control, communications, computers and intelligence (C4I) systems, allowed United States forces to know exact locations and force dispositions of the major Iraqi military units at all times and in all environmental conditions. At the same time, United States offensive SIW capabilities denied the Iraqis a reciprocal view of the forces

arrayed against them. In the modern, dynamic battlefield, continuous movement is essential to survival. Having instantaneous knowledge of exactly who and where the adversary is, is a tremendous tactical advantage. Coupling that advantage with the application of massive, precision-guided firepower, employed strategically to decapitate the Iraqi national command authority's command, control and communications infrastructure, and the results become fairly predictable.[49]

When Saddam Hussein poured his troops across the border into Kuwait on August 1, 1990, no one could know that his actions were about to provoke the most profound change in modern military tactics and strategy since the German blitzkrieg of World War II. Desert Storm was a sobering event. The decisive coalition victory over what had previously been the fourth largest and best-equipped military power on the planet did not pass unobserved. Governments and military planners began to study and apply the lessons of the Gulf War immediately. Iraq's military was defeated, but not just by force of arms. Iraq was defeated in large part by overwhelming information superiority and an associated revolution in military affairs (RMA), enabled by the Information Revolution and Information Technology.

THE INFORMATION AGE REVOLUTION IN MILITARY AFFAIRS (RMA)

The high value placed by Americans on the lives of their service personnel has led to the development of military strategies and methods that have become progressively, less dependent on a quantitative superiority of

personnel and material and more and more on a qualitative superiority in war-fighting technology, i.e., more advanced equipment, enhanced training, superior doctrine.[50]

The United States' longstanding quest for qualitative superiority in its military systems, a cornerstone of its strategic military planning, continues, but has been significantly affected by increasing costs and decreasing budgets.[51] The need for qualitative superiority is two-fold. First, it is needed as an offset to the general quantitative advantages enjoyed by many potential adversaries. Second, popular and political support for overseas military interventions is enhanced by the United States' ability to wage casualty-free warfare, i.e., no American lives lost and minimal loss of military hardware, inflicting maximum military and infrastructure damage on its adversaries, while gaining maximum political leverage. Information superiority has become a cornerstone of that strategy.

The Gulf War and Operation Desert Storm established this new paradigm of warfare in which human casualties and capital losses for the informationally inferior protagonist is exponentially greater than those of the informationally superior one. The new paradigm of high-tech warfare, moreover, requires the United States to be prepared to plan and execute military operations in an unconventional way. To be successful in that prosecution, difficult policy issues that will determine the future national direction must be addressed now.[52]

In the future, electronic operations will be decisive in their own right and the systems incorporating electronic and information technologies will take the art of warfare into an entirely new dimension.[53] But technology alone is not adequate; it cannot ensure victory. Military success in the future will require the development of an entirely new set of operational concepts obtained from the integration of new technologies designed to facilitate them.

These operational concepts are only realizable if substantial organizational transformations occur within the hierarchical military infrastructure of the United States. Public and private organizations move from technical to strategic superiority by achieving the necessary transformations that promote organizational adaptability. Organizational change itself, therefore, is a key element of technological innovation that grows in critical importance during periods of technical innovation and change. Bracken observed:

> The United States can no longer (just) rely on technological advantages to sustain economic and military leadership. The competition in both areas will focus on adaptations of new technologies in organizational structures that are flexible enough to continuously reinvent themselves and that can exploit the connections made possible by the information technology revolution. The real constraints will increasingly shift, however, from access to advanced technology or physical networks to the ability to develop new organizations capable of exploiting precision, flexibility, and integration. The incentives to absorb the inevitable transition costs will come from dynamic, adaptive global organizational networks. The key will not be to protect United States institutions from today's competitors, but to nurture patterns of innovations that will exploit new opportunities.[54]

Therefore, the current revolution in military affairs has much in common with the basic precepts of the Clinton Administration's National Performance Review (NPR), itself based on David Osborne's *Reinventing Government* tenets.[55] Both are predicated upon similar contentions: hierarchical bureaucracies, of whom the military is among the most rigid, create impediments to the rapid decisions and organizational flexibilities demanded by the technologies of the Information Age.

This rigidity was demonstrated on more than one occasion during the 1991 Gulf War. As an example, during Desert Storm, the United States Air Force was faced with the operational dilemma of having to plan a strategic air campaign against Iraqi critical infrastructure targets, for which there was no established doctrine. Since the end of World War II, U.S. strategic doctrine, concepts of operations (CONOPS), and training had all been predicated on strategic nuclear warfare. With the advent of atomic weapons, most Air Force doctrine could not identify with the concept of strategic attack with conventional weapons. It was not until Air Force planners were forced to think "out of the box" in Iraq that a new concept of operations emerged, enabled by innovative, information-based technologies. Doctrine had denied the realization of the full utility of that innovative technology. It took an organizational change, driven by a wartime imperative, to drive home this doctrinal adaptation that maximized the utility of the available technology.[56]

Successful military innovation is a process that involves far more than the integration of new technologies or even the evolution of new operational

concepts. Both must be thoroughly acculturated into the force structure, doctrine, training, operational patterns, and, most importantly, the decision-making processes of the military organization, if technological innovations and their associated CONOPS are to yield their expected dividends.[57] Recent literature has broadened the definitions of security to include economic, ecological, and human service concerns, i.e., telecommunications, banking, electronic commerce, privacy. But it has offered little in the manner of suggesting appropriate answers for addressing this broadened scope of national security administration challenges.[58] Including new dimensions of space and information conflict, Information Age warfare threatens to overwhelm policy makers and military commanders with decisional options that they have neither the training nor the experience to address.

Reorganizing the United States' apparatus of Government to execute a unified, strategic, national security policy without the inevitable trial and error experience of actual operations is difficult, if not, ultimately, impossible. As Weigley described it:

> The technology of war does not consist only of instruments intended primarily for the waging of war. A society's ability to wage war depends on every facet of its technology: its roads, its transport vehicles, its agriculture, its industry, and its methods of organizing its technology. As Van Crevald puts it, "behind military hardware there is hardware in general, and behind that there is technology as a certain kind of know-how. As a way of looking at the world and coping with its problems."[59]

The Advent of Cyberwar and Netwar

The United States military is the world's leader in planning, preparing, and integrating technology and operational concepts for offensive cyberwar. Arquilla, et.al., define cyberwar as "information-oriented military warfare," a term increasingly synonymous with high intensity conflict (HIC) between nation states. Netwar refers to an emerging mode of conflict and crime at the societal end of the spectrum, involving measures short of traditional war in which the protagonists use network forms of organization and Information Technologies to execute low-intensity conflict (LIC), operations other than war (OOTW), and nonmilitary modes of conflict and crime.[60]

The United States is the only country in the world today with a complete array of sophisticated technologies for denial of command, control, communications, surveillance, intelligence, and network integration making large-scale, offensive cyberwar a viable alternative to more conventional means of warfare.[61] Cebrowski and Garstka go so far as to state that networked information systems give the United States total dominance of the battlespace and induce informationally inferior adversaries to avoid conventional conflict rather than face certain destruction.[62] Recent events in Iraq, Kosovo, and Yugoslavia have not totally born out Cebrowski's and Garstka's claim, but they are instructional in several areas germane to this discussion. The facts support the premise that informationally superior United States forces enjoy a qualitative advantage of significant magnitude over their adversaries.

Advances in information technology are rapidly changing the telecommunications infrastructure and affecting military operational implications. This is the assessment of MGen John F. Stewart (USA-Ret), former commander of the United States Army Intelligence Center.[63] The evolving battlespace involves friendly and enemy information systems that employ both military and commercial technologies and systems to achieve tactical and strategic superiority. The modern, physical battlespace demands tailored, globally interconnected information systems. These systems are heavily dependent on commercial technologies and products.[64] The concept of network-centric warfare, adopted by DOD, took center stage in the Joint Chiefs of Staff's blueprint for cyberwar, "Joint Vision 2010." The policy paper, released in July 1996 by then-Chairman of the Joint Chiefs of Staff, General John M. Shalikashvili, blueprinted DOD's operational concept of joint war fighting, placing information networks and their ability to disseminate large volumes of information quickly, at the center of military strategy for the next decade.[65]

Largely as a result of the evolution of the microprocessor, the globally interconnected command and control systems described in "Joint Vision 2010" can now extend their reach all the way down to the individual foot soldier. To that end, the United States Army is developing Land Warrior, an interdependent combination of body armor, weapons, and command, control, and computerized communications that in the near future will personalize the Information Technology-driven RMA to every infantryman in the United

States Army. The computer- and radio-controlled system carried in the soldier's backpack sends geographic coordinates to a Global Positioning System satellite and receives precise location information from GPS in return, with the data presented on a digital battlefield map projected onto the soldier's heads-up helmet display. The positional data is also cross- and down-linked, via two-way command and control data link, to the soldier's operational commanders.[66]

In addition to the real-time, individual command and control capabilities offered by the new system, basic infantryman combat capabilities are substantially enhanced through the Information Technology embedded in the system. A video camera on the soldier's weapon subsystem is connected to the helmet-mounted, video eyepiece. Soldiers can fire their weapon overhead, around corners, or behind them while reducing their exposure to enemy fire.[67]

This new technology promises to greatly enhance the situational awareness of the tactical battlespace for the average soldier. It also provides a source of two-way voice and visual data, linked in real-time from the field of operations to local commanders, and all the way back to the National Command Authority, if desired.[68]

The Army plans to outfit 5,000 soldiers with the system by late 2000 and more than 34,000 by 2010. Soldiers in the light, mechanized, air assault, Ranger and airborne forces will carry the system. The pre-production unit cost of $200K per system is expected to drop to $35-42K when the system is

in full production.[69] This quantum advance in individualized, battlefield informational awareness has been made possible through the application of Information Technology and the continuing microprocessor revolution.

Information Warfare: The New Battlefield

Information Warfare is a critical developmental component to the current, Information Age Revolution in Military Affairs (RMA). Information warfare is defined as the actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems, while leveraging and protecting United States' military information and information systems.[70]

Strategic Information Warfare (SIW) uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. Little in the way of special equipment is required to launch a sophisticated SIW attack on another's computer systems. The basic attack tools--computers, modems, telephones, and software--are essentially those employed by hackers and criminals today. Compared to the often technologically sophisticated and prohibitively expensive military forces and weapons that in the past posed a strategic threat to a nation's infrastructures, SIW tools are cheap and readily available sources of near-instantaneous, strategic military power.[71]

Potential regional adversaries and peer competitors at the strategic level may find Strategic Information Warfare tools and techniques useful in

challenging the United States and its global interests. In the near term, weapons having SIW utility may be employed by regional adversaries in asymmetric strategies in lieu of more conventional military and political force, where the United States has a significant advantage.[72]

A well-orchestrated and coordinated cyber attack, whether in the shape of a massive frontal assault on the National Information Infrastructure, or through a much more sustained and subtle infiltration of the national, electronic-based infrastructure, offers perhaps the single, best opportunity to any adversary for asymmetric leverage and damage to the United States.

While isolated attacks or accidental encroachments into proprietary enclaves within the National Information Infrastructure (NII) can have a debilitating impact on those individually targeted institutions, a deliberate attack directed against the NII itself would potentially be of devastating, strategic proportion, impacting nearly every aspect of daily life in the United States. At this level, such an attack on the nation's infrastructure must be viewed as a strategic assault on the vital national interests and security of the United States.

A recent illustration of vulnerability in the nation's National Information Infrastructure to even unsophisticated cyber intrusion was demonstrated at the onset of NATO's air campaign against Yugoslavia. In early April 1999, the Pentagon acknowledged it had been targeted by at least two, carefully orchestrated cyber attacks on its computer networks, with one attack originating in Yugoslavia and the other originating from "a foreign source"

sympathetic to Yugoslavia and opposed to the NATO air strikes.[73] NATO Headquarters in Brussels, Belgium reported that computer hackers in Belgrade, Yugoslavia, temporarily disabled its main Internet Web site by bombarding it with empty electronic mail messages in a simple, but effective, denial of service (DOS) attack.[74]

In response, President William Clinton approved a covert plan presented him by National Security Advisor Sandy Berger, authorizing the Central Intelligence Agency to initiate a cyber attack against the personal financial assets of Yugoslavia's President Slobodan Milosevic and members of his immediate family. On May 24, 1999, President Clinton signed a National Security Finding, instructing the CIA to use government SIW experts (hackers) to tap into the foreign bank accounts of the Milosevics and "appropriate" any funds found therein.[75]

Congressional critics were quick to question both the wisdom and the legality of the plan, which directed the CIA to stage the electronic "breaking and entering" of foreign banks located in Russia, Greece, and Cyprus. The President's Finding authorizing the removal of Milosovic's assets, estimated in the tens of millions of dollars, did so without benefit of due process or International Law. While inviting the almost inevitable diplomatic backlash, the strategy also opened the door to possible computer counterattacks by Yugoslavia on banks in the United States and allied NATO countries. The potential of such a "banking cyberwar" undermining global confidence in the international banking system as a result, is very real. Such a result would

have an exponentially greater impact on the United States than on Yugoslavia.[76]

Both Yugoslavia and NATO were quick to take advantage of the pervasive reach of the Global Information Infrastructure (GII) superhighway for information dissemination and propaganda purposes during the NATO air campaign and Serbian "ethnic cleansings" in Kosovo during April and May 1999. World Wide Web sites, established by both factions as electronic "bully pulpits," argued the protagonist's respective views before an electronically interconnected, worldwide audience. NATO's Web sites were originally established to support the reporting of war crimes in Kosovo, while pro-Serbian Web sites appeared at the same time, denouncing in broken English, the NATO "insanity" and the "terrorism" by the Kosovars.[77]

In another example, Chechen rebel leaders were quick to establish an official web site (http://www.kavkaz.org), providing an outlet for "official" news and propaganda and a counter to Russian victory claims in the war in Chechnya. The failure of Russia's considerable Information Warfare capability to disable, jam, or even effect the rebel Web presence, is testimony to the robustness of the Global Information Infrastructure (GII) and the ever-increasingly sophisticated and commercially available tools spawned by the Information Age. [78]

The United States Space Command in Colorado Springs, CO (CINCSPACE) was designated by President Clinton as the national focal point for the evolution of policy and capabilities for Information Operations-

Attack and Defense (IO-A/D), with defense as the first priority. The overall goal was to evolve a tightly-coupled offensive and defensive capability that expands the United States' dominance in IO/A, while providing critical infrastructure protection without compromising our own ability to gather and exploit critical national security information.

Each of the uniformed military services are well into the process of evolving subordinate organizations and technical capabilities to promote both offensive and defensive Information Warfare. These service-centric organizations and their charters will remain within their respective service branches, while all IW-A/D activities and their technical findings will now be coordinated by United States Space Command as part of the national effort.

The Naval Surface Warfare Center (NSWC), Air Force Information Warfare Center (AFIWC), and the Army Research Laboratory (ARL) all track, analyze, and evolve defenses against cyber attacks for their respective military branch. All report that the essentially sophomoric behavior of the traditional freelance computer hacker, whose motive for perpetrating a successful cyber intrusion into restricted computer systems once was limited to peer bragging rights, has given way to the malicious, nation-state sponsored, intrusion-for-hire professionals, who steal information and intentionally cripples systems. Stephen Northcutt, the head of Intrusion Detection for the Naval Surface Warfare Center stated:

> Over the last six months, we've found that hackers are making money off their fun. They break into a system, cop some information and sell it. Today, it's about organized crime and

> espionage...These attacks are often successful, and the number doubles each year as Internet use increases and hackers become more sophisticated.[79]

For its part, the United States Air Force has established an organic think tank, or battlelab, to aid in concentrating and coalescing the service's cognitive efforts to attain a position of information superiority. Col. James Massaro, commander of the Air Force Information Warfare Center said:

> Information superiority, like air superiority, has been declared a core competency by the Air Force. We are determined to attain superiority not just for ourselves, but to also provide it to the other services and to the nation as a whole.[80]

The Air Force's Information Warfare Center at Kelly Air Force Base in San Antonio, Texas was created in 1993 by merging the Air Force Electronic Warfare Center and the Air Force Cryptologic Support Center.[81] A component of the Air Intelligence Agency's Air Force Information Warfare Center, the mission of the new Information Warfare Battlelab (IWBL) is to support the full spectrum of Air Force operations by identifying "innovative and superior ways" to plan, train, and deploy assets and influence information warfare and information operations doctrine and tactics to meet current and emerging threats and missions.[82]

The IWBL staff is divided into three components: support, vulnerability analysis, and operations concept. The latter two operate as "Red Team" (attack) and "Blue Team" (defense) entities, with SIW attack and defend missions respectively. Each team independently determines Air Force

system vulnerabilities and then evolves joint operational concepts for defeating the SIW threat.[83]

Supporting the IW-D component of the AFIWC activity is the Air Force Computer Emergency Response Team (AFCERT). Like its Army and Navy counterparts, AFCERT serves as the primary defensive measure against unauthorized attempts to access Air Force information networks. Effective defense of the information networks is essential to the protection of the Air Force's on-line decision making and command and control processes. An adversary gaining access to these networks could interfere with the electronic flow of critical decisions and directives, potentially altering a conflict's outcome.[84]

CRITICAL INFRASTRUCTURE PROTECTION

The national security interests of the United States are being profoundly affected by the on-going Information Revolution and an exponentially-growing dependence on vulnerable elements of the National and Global Information Infrastructures (NII/GII). As the post-Cold War evolution of national security and military policy continues to grapple with an uncertain future, the all-pervasive evolution and adoption of information technologies in all aspects of the national society presents a new kind of strategic vulnerability, never previously contemplated or addressed by those charged with "providing for the common defense."

The American people have never known widespread deprivation as a result of denial of vital human services through the failure of the nation's critical infrastructures. Denial of the use of the nation's electronic computerized networks would deprive the United States of the use of most aspects of those critical electronic infrastructures the society has become so dependent upon: telecommunications, transportation, electronic banking, water, power, emergency services, government services, and so on.

Destruction of a nation's critical infrastructure foundations ultimately results in that country's inability to function as a cohesive society. The violent death of tens of millions of its citizens is not a requisite for the destruction of the United States as a functioning society. The threat is real and its potential will continue to grow as Information Age technologies proliferate, bringing access to a globally interconnected electronic world to those having malicious designs on some or all of it.

The critical infrastructure at risk is best described as the basic structural building blocks, or foundations, of the nation. Often overlooked in philosophical discussions of "foundations" are basic infrastructure components such as interstate highways, telecommunications, oil and gas production and distribution systems, police and emergency services, healthcare systems, and even the Internet. These and other critical infrastructures are vital societal underpinnings of the United States.[85]

Protecting the Nation's critical infrastructure has long been a subject of government concern. Dams, bridges, tunnels, power plants, and other

important physical structures have been specially protected for the past 50 years. Physical terrorist acts against these types of infrastructures, though not well known, have occurred with some regularity in the United States, even during peacetime. A prime example were the 70 separate attacks in the Pacific Northwest on remote power transmission lines owned by Pacific Gas and Electric (PG&E), perpetrated by America's own New World Liberation Front, during the 1970s.[86]

Protection of the nation's telecommunications and information infrastructures has only been of major government concern since the Cuban Missile Crisis in October 1962. Difficulties in maintaining secure communications among the United States, the Soviet Union, NATO, and foreign heads of state had threatened to complicate the crisis further.[87]

Immediately after the crisis, in November 1962, the National Security Council (NSC) formed an interdepartmental committee to examine the existing communication networks and to institute necessary changes, including the formation of a single, unified communications system to serve the President, DOD, diplomatic and intelligence activities, and the civilian leadership.[88]

As a consequence, President John Kennedy established the National Communications System (NCS), by Presidential Memorandum, on 21 August 1963. The mission of the NCS is to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of Management and Budget in creating and implementing

policy and provisions for national security and emergency preparedness communications for the Federal Government.[89]

In September 1982, President Ronald Reagan established a civilian telecommunications advisory committee counterpart to NSC's NCS, to provide analysis and advice to the Executive Branch on national security and emergency communications issues. The President's National Security Telecommunications Advisory Committee (NSTAC) was created in September 1982 by Presidential Executive Order 12382, amending Section 706 of the Communications Act of 1934.

Using the NCS-NSTAC symbiosis as a model, the Defense Science Board Task Force on Information Warfare–Defense (4 Oct 1995 to 25 Nov 1996)[90] and the President's Commission on Critical Infrastructure Protection (PCCIP, 15 July 1996 to 20 October 1997)[91] strongly endorsed the concept of a strategic partnership between the United States Government and industry as necessary to evolve the requisite capabilities to defend the nation's critical information infrastructures from cyber intrusion and exploitation.[92]

The 1991 Gulf War brought home the vital importance of critical infrastructures to national defense. Dominance over Iraq's information and communications ensured victory by the United States and coalition forces over a well-armed military force with minimum allied losses. Other nation's have drawn similar conclusions.

The probability that future adversaries would exploit the tools and technologies of the Information Age to disrupt, destroy, or hold in thrall the critical infrastructures of the United States, is very real. With the advent of cyberwar and cyber terrorism, governments, non-governmental organizations (NGOs), and solitary individuals need not destroy or kill to gain an asymmetric political leverage unobtainable to them by conventional means. Large-scale or massive disruption of key strategic infrastructure components, such as electronic banking, power, transportation, and telecommunication, on even a temporary basis, would have a major, debilitative effect on national morale and the nation's collective sense of security.

Vulnerability of these government and private sector infrastructure assets to an adversary employing SIW tools was examined over a three-month period beginning in June 1997, as part of a military exercise sponsored by the Joint Chiefs of Staff called ELIGIBLE RECEIVER. ELIGIBLE RECEIVER featured a series of scripted attacks on selected energy and telecommunications infrastructures around the United States. Exercise controllers introduced "no notice" SIW events into the exercise, forcing military commanders to react to the unforeseen loss of key computer-based assets and critical infrastructures.[93]

Companies providing electrical services in selected cities during the exercise were subjected to scripted cyber attacks over a period of several weeks, making the attacks appear totally random and unrelated. At the same time, an attacking "Red Team," made up of military and civilian computer

experts and employing software tools and techniques posted on hacker bulletin boards on the Internet, penetrated DOD computer networks, disabling and disrupting key information assets through denial of service attacks. With no insider information and working within the constraints of United States law, the "Red Team" spent three months probing, examining, and exploiting vulnerabilities in several hundred unclassified computer systems and networks. Not only were many of these systems and networks penetrated, but the "Red Team" was able to gain system administrator (root) privileges, and thus total control over many of them.[94]

CYBER TERRORISM: FROM HACKERS TO INSIDER THREATS

The Information Age has spawned a number of Information Technology-related phenomena, not the least of which is the computer hacker. The word hacker has two very different meanings. Originally, the term hacker was applied to creative software engineers and programmers, who were literally software wizards. Through their creativity, the modern software industry was born. By the mid-1970s, the term hacker became synonymous with a class of young computer zealots, characterized as "computer-savvy teenagers and over-zealous programmers, who were unlikely to engage in criminal or malicious activities, and were thought to be motivated by curiosity and technical challenges."[95]

By the early 1980s, hackers had emerged as a unique sort of technological and sociological icon of the Information Age. The successful,

unauthorized access to restricted information systems and non-malicious, temporary control of those computer systems, made accessible through remote networked connections, became the goal of the hacker. Demonstrating the technical acumen necessary to electronically infiltrate computer systems, especially those protected by elaborate security systems, such as banks and financial institutions in the private sector, and the Defense Department in the public sector, became the hackers' ultimate intellectual gratification.

In 1982, a group of university students, using mainframe computer terminals, modems, and long distance telephone lines, hacked into the Department of Energy's Los Alamos National Laboratory in New Mexico and the Columbia Medical Center. This seminal event marked the emergence of an institutional awareness concerning the vulnerability of networked computer systems in the United States.[96]

At about the same time in 1982, a new generation of computer hacker emerged, but this group was motivated more by greed and malice than by intellectual curiosity. By 1982, some hackers, realizing both the value of information harvested from unauthorized break-ins to restricted information sources and the potential profit derived from the sale of that information, evolved into a new form, the cyber criminal or terrorist. Unlike the hacker, the cyber criminal or terrorist is motivated by greed, political goals, theft, or malicious intent. These motivations have been the catalysts underlying cyber attacks on DOD and other restricted data sources, as well as the source for

the insertion of malicious codes and the launching of global denial of service attacks by this most dangerous version of the modern computer hacker.[97]

The Federal Government has been slow to recognize the real threat posed by cyber terrorism. In November 1985, President Ronald Reagan tasked Vice President George Bush to chair a task force on terrorism. The Vice President's Task Force on Combatting Terrorism included most of the Cabinet Secretaries, a Senior Review Group, an Analysis Group, a Liaison Group, and a Staff Working Group. The Executive Director of the Study was Admiral James L. Holloway, USN. The Task Force was briefed by more than 25 Federal agencies and visited 14 operations centers to observe United States' antiterrorism capabilities first hand. The Task Force met with over 100 subject matters experts including statesmen, military officers, scholars and law enforcement specialists, and traveled to embassies and military commands throughout the world.[98]

In February 1986, the Task Force issued its final report. In its 34 pages, terrorist threats to United States' critical infrastructures and technology are not addressed. In fact, there was no mention anywhere in the *publicly-released* version of the report on the issues of cyber terrorism, computer hacking, or Strategic Information Warfare.

In June 1986, Dr. Robert Kupperman, a Laboratory Fellow at the University of California at Berkeley's Los Alamos National Laboratory, chaired a panel on terrorism under the auspices of the Center for Strategic and International Studies (CSIS), located at Georgetown University in

Washington, D.C. The distinguished panel included, among others: The Right Honorable Lord Chalfont of the United Kingdom's House of Lords; Lee Colwell, Adjunct Professor at the University of Southern California and Deputy Director of the FBI; Richard Helms, formerly Director, CIA; General Edward Meyer (USA, ret.); Admiral Thomas Moorer (USN, ret.); and Robert Selden of the Los Alamos National Laboratory.[99]

The CSIS Panel's report on terrorism entitled, "Combating Terrorism: A Matter of Leverage," was issued in June 1986. Unlike the Vice President's Task Force, the CSIS Panel publicly-acknowledged the advent of cyber terror and the cyber terrorist threat to the nation's critical infrastructure:

> Terrorists are clearly becoming more technologically adept...Nowhere is this more evident than in the attacks on the technological infrastructure, the lifeblood of highly developed societies...The greatest strength of modern western society, its strong technological base, is also its Achilles heel. Technological societies survive by virtue of a sophisticated service network of electric power grids, computer and telecommunications links, oil and natural gas refineries, pumping stations and pipelines, transportation systems and water networks. Taken together, these systems form an intricate, interdependent, and extremely fragile infrastructural web.[100]

By 1999, cyber terrorism was widely acknowledged as a core tool in the terrorist spectrum. A 1999 RAND study prepared for the United States Air Force and entitled, "Countering the New Terrorism," concluded that contemporary terrorists would be likely to increasingly rely on advanced information technologies for both offensive and defensive purposes, as well

as to support their organizational structures.[101] The RAND study termed this new type of terrorism as "netwar" and the new terrorists as "cyber terrorists":

> To be more precise, netwar refers to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age...this term is meant to call attention to the prospect that (computer) network-based conflict and crime will become major phenomena in the decades ahead.[102]

Assault on the Public Sector

The past ten years have witnessed an alarming increase in the number of cyber crimes and terrorist events perpetrated against the Federal Government, the United States military, and the United States Defense Department. Cyber attacks on military computer systems are of particular concern, as vital military operations and highly sensitive national security information may be placed at risk as a result.

The Defense Department alone maintains some 660 major installations around the globe, supported by 1.5 million computers and 28,000 computer systems, many of which are linked to more than 1,000 publicly-accessible World Wide Web sites or home pages. Fully 95% of all military communications travel over the same phone lines that the public employs to access the Internet.[103]

Increasingly, military computer systems and networks have come under various kinds of cyber attack. Most of these attacks are non-malicious in nature, but an increasing number of recent attacks

have taken a decidedly different tone. According to the General Accounting Office, the Department of Defense suffered over 250,000 cyberattacks a year from 1997 through the end of 1999.[104]

The military, though the most visible, is not the only government component that has come under increasing cyber assault in recent years. The results of a 1998 computer crime survey conducted by the Federal Bureau of Investigation (FBI) revealed that 53% of Federal agencies had suffered some form of cyber attack. Another 20% had no organic ability of assessing whether they had been victimized by cyber attack or not. Cyber terrorists have stolen and destroyed sensitive data and software, crashing entire computer systems and networks, while denying computer service to authorized users, and preventing government personnel from performing their duties. Perhaps the most disturbing trend to be uncovered by the study was that for the first time, most of the documented security breaches originated from outside the departments surveyed.[105]

Attacks on government computers are reason for serious concern. Considering the many crucial functions the United States Government depends on that are made possible through the use of computers, unauthorized access to and break-ins of computer networks have the potential for seriously crippling the ability of the United States Government to conduct business, provide essential services, and even to wage war.

The lack of effective intrusion detection and proper investigatory capabilities within the military services is particularly telling. In 1995, the Air

Force Office of Special Investigations (OSI) investigated 129 incidents of hackers or cyber terrorists breaking into Air Force computer systems, but only 29 of those investigations were concluded successfully.[106] Furthermore, of the 250,000 total break-ins against U.S. military computer systems and networks in 1995, 162,500 or 65% were successful, but only 150 were actually detected and reported.[107]

The Cuckoo's Egg

Perhaps the most comprehensive public account, documenting the systematic assault and break-in of defense industry and Defense Department computer systems, was captured in author Cliff Stoll's 1989 masterpiece, *The Cuckoo's Egg*. In August 1986, Stoll, an astronomer by trade at the Keck Observatory at the Lawrence Berkeley Laboratories and an amateur hacker by avocation, was pressed into service as a computer systems manager, the result of funding cuts at the University (Stoll's grant money ran out).[108]

Stoll discovered a 75-cent accounting error in the University of California at Berkeley's computer timeshare billing program. This led Stoll to discover that a hacker, identified by the moniker, or handle, "Hunter," had penetrated Berkeley's computer systems, using them as a conduit to break into United States Government and DOD systems and stealing sensitive military information. Based upon the pattern of data searches initiated with

each subsequent break-in, Stoll concluded that the hacker's objective was to attain United States anti-ballistic missile technology.[109]

As he pursued the intruder and sought the attention of government and law enforcement agencies concerning his discoveries, Stoll encountered a series of roadblocks and bureaucratic challenges. First, Stoll was unable to locate computer-literate law enforcement officials with an appreciation of the technical nature of the criminal activity he was observing and recording. Local and Federal agencies contacted by Stoll initially expressed only a passing interest in what, to them, appeared to be a simple case of low-value, electronic breaking and entering (i.e., $.75). It wasn't until government investigators learned of the potential threat to national security that Stoll succeeded in attracting the attention of the FBI and CIA.[110]

Second, because the intruder's electronic trail disappeared each time the telecommunications connection was broken, the intruder could only be traced while he was on-line. But because the intrusions occurred for the most part late at night or early in the morning, i.e. in the middle of the night for the continental United States, there were few, if any, law enforcement personnel available for Stoll to contact during those events. Stoll eventually traced the hacker's telephone connections to Hanover, Germany, but adding an international element and additional, multiple time zones to the equation served only to complicate his investigation.[111]

To keep the hacker on-line long enough to successfully trace the connection, Stoll resorted to generating phony-looking Strategic Defense

Initiative (SDI) data to maintain the intruder's interest. This finally led to a successful trace and identification of the cyber intruders. Markus Hess of Hanover, Germany along with accomplices, Dirk Brezinski, a resident of Berlin, Germany, and a computer programmer/troubleshooter for the German computer firm Siemens, and Peter Carl, also from Berlin and a cocaine addict, were selling data obtained from the break-ins to intelligence services of the Soviet Union. Their attacks were motivated entirely by greed.[112]

Hess, Brezinski, and Carl were eventually tried and convicted of espionage by a German court on 16 February 1990. All three received one- and two-year sentences, the most allowed under Germany's existing computer crime laws. Released on probation, the perpetrators live as free men in Germany. Markus Hess currently writes networking software for an Internet company in Hanover.[113]

Defense Information Under Fire

As Stoll's *Cuckoo's Egg* demonstrated, the Defense Department's vast data repositories are major targets of choice among the world's cyber terrorists. The attraction is three-fold: first, the mystique associated with successfully hacking into secure data enclaves operated by the DOD; second, the significant resell value for almost any data purloined from Defense computer break-ins; third, the political capital to be made in "putting a dent" in the military capabilities of the world's sole remaining superpower.

One of the most alarming cyber attacks perpetrated against the United States military occurred during March and April 1994 and targeted the Air Force Research Laboratory (AFRL) located at Griffiss Air Force Base in Rome, New York. This break-in raised serious computer network security concerns within the military and received a great deal of public attention. The cyber attack involved two hackers, who broke into the base's computer network and illegally obtained a number of computer system passwords through the use of a sniffer program. The hackers installed the sniffer program to read and capture passwords used by military personnel as they logged into the Griffiss computer backbone network. The purloined passwords were used to access over 100 separate computers on the Internet, including a South Korean nuclear research facility, from AFRL. This particular intrusion was especially alarming because it made it appear that a cyber attack was being launched from a United States Air Force facility against a sensitive national facility within the sovereign territory of South Korea.[114]

On 12 May 1995, the Air Force OSI detachment stationed at Bolling AFB in Washington, D.C., apprehended the perpetrators before any more damage could be done. The cyber criminals were identified as sixteen year old Richard Pryce of London, England, and twenty-one year old Matthew Bevan of the United States. Investigators were able to follow the pair's cyber trail to an on-line chat room, where their identities were revealed after a government informant exchanged on-line messages with the two. Each

member of the pair was indicted and convicted on two counts: conspiracy to gain unauthorized access to government computers and conspiracy to cause unauthorized modification to government computers.[115]

In another, now famous case, from 1 to 26 February 1996, two 16-year high school students from Cloverdale, California, assisted by Ehud Tanebaum, a teenage boy in Israel, systematically targeted and hacked United States Defense Department Network Domain Name Servers, exploiting a well-known vulnerability inherent in SUN's computer operating system, SOLARIS. The case, dubbed SOLAR SUNRISE by the Defense Investigative Service and FBI, was a carefully coordinated attack, targeting important elements of the DOD's unclassified networks, including key systems for the Global Transportation System, Defense Finance System, Medical, Personnel, Logistics, and the official unclassified email system.[116]

All three individuals involved in the SOLAR SUNRISE attacks were eventually tracked down and apprehended. The two United States juveniles, whose names were sealed under court order, were tried in juvenile court and convicted of crimes associated with the cyber intrusions. The Israeli teenager, Ehud Tanebaum, was held for prosecution and convicted of similar charges by an Israeli court in 1996.[117]

Lessons learned through the SOLAR SUNRISE experience are continuing to be assessed and acted upon by various agencies of the United States Government. SOLAR SUNRISE clearly demonstrated that DOD computer network and systems intrusion detection indicators and warning

systems are inadequate and need significant improvement. As a result of the identified intrusion detection deficiencies, intrusion detection and characterization of unauthorized access remain problematic for DOD computer systems.[118] However, worse was yet to come.

In January 1999, DOD computer security experts detected what they described as "sophisticated, patient, and persistent" attempts to penetrate sensitive military computer systems in the Pentagon. Begun at a low level of access, this cyber attack, code named MOONLIGHT MAZE by DOD computer security officials, represents one of the most potentially damaging breaches of United States' computer security in history. The implications of this attack have been serious enough that for the first time in its history, the DOD ordered all its military and civilian employees to change their passwords by the end of August 1999.[119]

The intrusions were traced to the Russian Academy of Sciences in Moscow, Russia. The state-sponsored Russian Academy, in concert with Russia's top military laboratories, employs many of Russia's finest cryptologists, computer scientists, and cyber spies. Under the direction of the Russian Government, these cyber experts have targeted networked computer systems of the United States Departments of Defense and Energy. Their efforts have led to the compromise of classified naval codes and engineering data on United States guided missile systems.[120]

During their assault, the MOONLIGHT MAZE intruders evolved newer, more sophisticated cyber attack tools, allowing them near-undetected entry

to United States Defense systems. Electronic "residues" left behind enabled United States computer experts to reconstruct their attack techniques. Intelligence sources report that the intruders were successful in acquiring root level access to many of the systems penetrated, giving them near-total access to even the most vital components of the affected systems. After that, "we're not certain where they went, " stated Representative Curt Weldon (R-PA), who chaired classified Intelligence Oversight Committee hearings on the MOONLIGHT MAZE episode.[121]

Although further intrusions by the Russian Academy hackers have not been detected since 14 May 1999, suspicions are that the attacks continue unabated but may no longer be detectable by current technical means. As a Federal interagency task force continues assessing the damage and technical lessons learned from this series of cyber attacks, a key question remaining to be answered is whether the Russians were able to penetrate DOD classified computer systems through their successful penetrations of DOD unclassified systems. Computer firewalls between the classified and unclassified enclaves, designed to prevent this occurrence, may have failed to keep the environments separate, bringing into question the security of any networked computer.[122]

In an interview on 6 October 1999, Senator Jon Kyl (R-AZ), Chairman of the Senate Judiciary Subcommittee investigating the MOONLIGHT MAZE case, called the public unveiling of the attack, "extraordinarily significant," but only one part of a recent series of worrying incidents. "Terrorism, espionage,

deliberate attempts to disrupt...insider activities, hacking, all these activities are currently going on," Kyl said. "Its mind-boggling."[123]

On 12 July 2000, Federal agents arrested Raymond Torricelli, the 20-year-old, self-proclaimed leader of a sophisticated group of Internet hackers, on five counts of illegally breaking into computers at NASA and the Jet Propulsion Laboratory (JPL) in Pasadena, California. Authorities said Torricelli of Rochelle, New York, gained access to more than 800 computers across the country. When arrested, Torricelli was in possession of 76,000 stolen passwords and 100 stolen credit cards, all hacked off the Internet.[124]

Torricelli, who had been under surveillance for several years, was accused of using one of the NSA computers he compromised to host an Internet chat room devoted to hacking. Torricelli's April 1998 intrusions at JPL were so serious that the Lab was forced to shut down one computer and permanently decommission another. The task of the first of these computers was satellite design and mission analysis of future space flights; the other computer was used for email and as an internal Web server.[125]

United States Magistrate, Judge Mark D. Fox, released Torricelli on a $50,000 personal recognizance bond. If convicted of the charges pending against him, Torricelli faced up to ten years in prison and a $250,000 fine on charges of credit card fraud and illegal password possession; five years in prison and a $25,000 fine on a charge of password interception; and one year in prison and a $100,000 fine on each of two charges involving unauthorized access to NASA computers.[126]

What *Cuckoo's Egg*, SOLAR SUNRISE, MOONLIGHT MAZE, and the host of other intruder assaults on government computer systems revealed is that significant technical and organizational deficiencies continue to exist in the ability of the government to defend itself against and respond to cyber terror incidents. Fundamentally, government agencies are not organized adequately to detect and defend their own automated information systems and critical infrastructures. As problematic are the jurisdictional issues and operational concept disconnects between key law enforcement and investigatory agencies within the DOJ and DOD charged with fighting computer hacking and computer crime. These fundamental issues must be resolved successfully before the United States Government can develop and implement a successful critical infrastructure protection policy and an apparatus to execute it.[127]

Assault on the Private Sector

Government computer assets have not been the only targets of cyber terror. Institutions in the private sector have also increasingly come under assault by hackers, or cyber terrorists. E-Commerce and the News Industry, having fully appreciated and embraced the competitive advantages presaged by Information Age technology perhaps faster than other industries, have become particularly vulnerable to cyber terrorist intrusions into their informational "stock and trade." Web sites, established for the posting and accessing of electronic information, have increasingly fallen prey to cyber

terrorist manipulations, placing the Web host potentially at risk for e-Commerce-related financial losses, libel, or other damages, as a result.

On September 13, 1998, administrators at the *New York Times* were forced to shut down their World Wide Web site for some nine hours, after an unsuccessful battle for control of the site with an organized group calling itself, "Hackers for Girlies." The hackers replaced the newspaper's homepage with pornography, obscenities, and threats directed at John Markoff, a *New York Times* reporter and recent publisher of a book focused on computer hacking entitled, *Take Down.*[128]

In a similar event, the *Los Angeles Times* reported that EBAY, Inc. was penetrated by a hacker who managed to take down the EBAY homepage on the World Wide Web and invade content files supporting the company's electronic commerce on the Internet. According to a report obtained by the *Times* from *Forbes Digital Tool*, a 22 year-old college student, operating under the moniker MagicFX, attacked the popular Internet auction site on Saturday, 13 March 1999. After gaining access to the site, the intruder managed to manipulate auction prices, post fake advertisements, divert traffic to other web sites, and even demonstrate an ability to "disable the entire network."[129]

On April 1, 1999, 30 year-old, computer programmer, David L. Smith, was arrested and charged with launching the prolific Melissa e-mail virus. This virus, a form of computer program called a macro, was embedded in a Microsoft Word attachment to an e-mail message that said: "Here is that

document you asked for...don't show it to anyone else." Once opened, the macro was designed to self-install onto the host computer's core memory and to be replicated by mailing itself to the first 50 individuals listed in the email directory of the host computer.[130]

Smith's arrest took place after six days of extensive electronic detective work by Internet security investigators and law enforcement officials, who were first notified of the existence of the virus on March 26, 1999 by Internet Service Provider (ISP) America On-Line (AOL). AOL contacted the New Jersey Attorney General's Office, Division of Criminal Justice's Computer Analysis and Technology Unit and led them to an Internet account illegally appropriated for use from Scott Steinmetz, a civil engineer from Lynnwood, Washington. From there, investigators followed the electronic trail to a bulletin board at a World Wide Web (www) address frequented by computer hackers, then to an Internet service provider (ISP) in Tennessee, and finally to an apartment in Aberdeen Township, New York, an hour from New York City, where Smith's personal computer was found still connected to the Internet.[131]

This joint government-industry cooperation resulted in an arrest and the containment of the Melissa virus in just six days. However, in just three of those six days, officials estimate the virus infected a minimum of 100,000 computers. By the sixth day and the end of the crisis, AT&T reported that roughly 45,000 of its 140,000 employees had reported suffering from infected computers. Network Associates reported 60,000 infected computers, while

Lucent Technologies, the spin-off communications laboratory of AT&T, and Microsoft itself, were both forced to shut down their respective intranet services to keep the virus from spreading entirely through their email systems. In one documented case, 32,000 copies of the virus multiplied within a single organization in less than one hour. Steve White, noted anti-virus expert at IBM's Watson Research Center, stated: "This is clearly the first page in a new chapter on viruses. I expect a lot of copycats."[132]

White's prophecy came true on 8 May 2000, when another rampaging email virus, dubbed the "Love Bug," infected hundreds of thousands of Internet users in the United States and millions more world-wide via the World Wide Web. The Love Bug, also known as the "ILOVEYOU" virus by virtue of its email address header, much like the Melissa virus which had caused an estimated $80 million in damages in the year previous, targeted Microsoft Outlook users. But where the Melissa Virus took the better part of a week to propagate and do its damage, the Love Bug spread in a matter of hours, unleashing a flood of malicious code each time a user clicked on the file attachment accompanying the "I love you" message header. Among its victims were the English House of Commons, the United States Defense Department, and the National Security Agency (NSA), each of whom were forced to shut down parts of their intranets and email systems to fully eradicate the electronic infection.[133]

The Love Bug, one of the Internet's most dangerous pathogens yet, resembled a virus, a self-replicating worm, and a password-stealing Trojan

horse, all in one relatively simple program. The Love Bug represented a new stage in the evolution of electronic pathogens. Unlike Melissa, the Love Bug was not programmed to simply replicate and email itself to the first fifty addresses in an infected user's electronic mail directory. The Love Bug's replicating worm software was programmed to mail itself to every address in each infected user's address directory. Meanwhile, the virus software would attack and delete any digital photographs or music files on the victim's computer hard drive, while the Trojan horse component would redirect the victim's browser to a site that would download a separate "sniffer" program to the victim's computer, which was programmed to steal passwords off the host network.[134]

The response to the outbreak of the Love Bug virus was mixed. The FBI's National Infrastructure Protection Center (NIPC) first learned of the virus at 0545 EDT on 8 May 2000 from an industry source. But NIPC took nearly five hours, from 0545 to 1100, to issue its first alert concerning the virus, through a posting on the NIPC web page. That was nearly five hours after the first Federal agencies began to be affected by the virus. The posted notice was only a brief advisory and did not offer any advice or direction for containing the spread of the virus through government and commercial computer networks. NIPC's lack of an effective, early-warning and containment plan significantly increased the adverse impact on the affected agencies. Of the 20 major Departments and agencies surveyed, only seven were spared significant damage as a result of the viral infestation.[135]

The NIPC partially managed to redeem itself in the subsequent investigation to find the source of the virus. Within hours of the first reported outbreaks of the Love Bug in the United States, the NIPC had marshaled an assessment and containment team and was investigating the source of the virus. Within 24 hours of the outbreak, the FBI discovered that the origin of the virus was a 23 year-old student named Onel de Guzman, who went by the computer alias of Spyder, and who was enrolled at the AMA Computer College just outside Manila in the Republic of the Philippines. de Guzman's proposed college thesis involved the development of a Trojan horse virus, which like the Love Bug, was intended, "to steal and retrieve Internet accounts," that would offer users, "more time on the Internet without paying." A thesis review committee at the college had rejected de Guzman's proposal on the grounds that it was both illegal and immoral. Refusing to change his proposal, de Guzman was denied the opportunity to graduate.

Branded as a criminal outside the Philippines, de Guzman was hailed a hero at home. The headline of the Manila Standard on 15 May 2000 read, "THE COUNTRY'S FIRST WORLD CLASS HACKER!" At de Guzman's school, a fellow student proudly proclaimed, "It's a cool thing and I respect it. It publicized our school."[136]

Less than two weeks later, yet another virus appeared to threaten the Internet, prompting Federal officials and computer software vendors to issue global alerts, warning users against opening email infected by the virus dubbed, NewLove.vbs, or simply Herbie. Upon receiving an early warning

alert about the virus on 18 May 2000, the FBI's NIPC went into immediate action, contacting major businesses overnight and warning them by early Friday morning, 19 May 2000, that the virus could destroy computer files and replicate itself to all the addresses and electronic mailboxes listed in an infected computer's email address books.[137]

Estimating that the new virus had infected some 1,000 computers by that Friday morning of 19 May 2000, Attorney General Janet Reno called an early-morning press conference in Washington, D.C., to announce that Federal officials from the NIPC had opened an investigation into the cyber attack. Michael Vatis, Director of the NIPC, stated during the news conference that, "We don't know yet exactly how widespread this is. We jump on these things as quickly as we can."[138]

However, within days it became apparent that the virus would not be as virulent or widespread as its predecessors, prompting private-sector complaints over the government's apparent inability to recognize and respond appropriately to a truly sophisticated cyber attack. A number of industry experts said that while viruses, such as the NewLove virus, could be highly destructive, a greater damage would be done in exaggerating the estimates of damage and undermining the credibility of government and industry computer security experts and organizations, like the NIPC. "It's like the boy who cried wolf," stated Richard Power, Editorial Director of the private sector Computer Security Institute. "There is a serious problem in cyberspace, but hyperbole takes away from the message."[139]

The negative publicity generated from various computer virus scares and cyber attacks triggered outrage among some members of Congress, who blamed the software industry for fueling the publicity and then profiting from the resultant sales of anti-virus software products. During a hearing of the House Science Committee's Panel on Technology on 17 May 2000, Congressman Anthony Weiner (D-NY) charged the industry with "utter and abject failure...to protect against these viruses:"

> It seems to me we have had a little time to figure out how to block this. In ain't gonna get any easier than this. They're not going to knock on your door with a disk and say, "This is going out Monday morning."[140]

Insider Threat: The Threat from Within the Organization

Insider threats to the security of organizational information and proprietary data are not new. Banks, security exchanges, and financial institutions have long recognized and respected the threat posed by the unauthorized or illegal access by rogue insiders. Similarly, the insider threat to government-held information, and especially national security information, is not new. But by virtue of the Information Age advances in Information Technology, the tools to facilitate that unauthorized access are new. In the wrong hands, Information Technology offers a variety of difficult-to-counter mechanisms through which the theft of large volumes of a company's or nation's most sensitive and closely guarded secrets can be enabled with virtually the press of a button. Digital technology and computer networking

have greatly increased the potential for insider information espionage in the Information Age.

National security information is not the only type of government information of interest; nor are employees of the DOD and DOE the only focus of insider threats to government information systems. Criminal exploitation of a wide variety of information contained in government information systems, is on the rise.

A 1998 "Computer Crime and Security Survey," conducted jointly by the Computer Security Institute and the FBI's International Computer Crime Squad based in San Francisco, California, provides data collected from 520 security practitioners employed by United States corporations, government agencies, financial institutions, and universities. Government agencies were not singled out, so the survey does not speak to public-private sector differences. However, taken as a group, of those organizations reporting an unauthorized use of their computer systems in the previous year, 36% reported they had experienced such incidents from inside their organization. Overall, 89% identified disgruntled employees as the likely source of their unauthorized intrusion. 39% said that the insider attacks had cost the parent organization a measurable financial loss.[141]

In 1988, Libyan intelligence obtained the names, addresses, and home phone numbers of more than 1,000 Federal employees at United States military and intelligence agencies in the Washington, D.C. area.

The data was supplied to a Libyan agent by the agent's wife, employed as a computer operator with the Virginia Department of Transportation. Through her offices, this individual accessed the Metropolitan Washington Council of Governments for carpooling purposes, gaining legal access to proprietary information that could have been used illegally to assist in Libyan terrorist operations against United States Government personnel.[142]

In 1993, the General Accounting Office (GAO) reported that insiders posed the greatest threat to the Federal Government's National Crime Information Center (NCIC). In its study, GAO cited 56 specific cases of intentional insider misuse of NCIC information. Most of these cases of misuse were benign, e.g., employees accessing the Center's databases to determine if a friend or a relative had criminal records. Some were "for profit" intrusions, i.e., selling information to private investigators conducting background investigations. Others were for political leverage.[143]

Some instances of unauthorized insider intrusions into the NCIC databases were not so benign. The GAO cited at least one extreme example of a former law enforcement officer using insider contacts to obtain information used to track down a former girlfriend and murder her. In another case, an NCIC terminal operator used her position to conduct background searches for her boyfriend, who was a drug dealer. The boyfriend used the NCIC employee to check the criminal histories of new clients to determine if they were undercover drug agents.[144]

In July 1997, a former United States Coast Guard employee used her programming skills to access the Coast Guard's national personnel database and to delete important data that caused the host computer system to crash. The crash wiped out almost two weeks' worth of personnel data used to determine promotions, transfers, assignments, and disability claim reviews. It took 115 Coast Guard employees more than 1,800 hours to recover and reenter the data deleted, at a cost to the government of over $40,000. Upon her arrest, the employee stated that previous attempts to report improper and illegal conduct by a Coast Guard computer contractor had been ignored. She subsequently filed an EEO complaint, alleging a hostile work environment, and then resigned her job. The FBI was tipped to the possibility of an insider job by the precision with which the subject files were accessed.[145]

In September 1998, during hearings before the Senate Committee on Governmental Affairs, the Government Accounting Office (GAO) released a report in which it cited significant information security weaknesses at 24 federal agencies. GAO and agency Inspectors General audits over the past two years identified six areas where poor control over access to sensitive data and computer systems were discovered. In particular, the report singled out the Veterans Affairs Department (VA) and the Social Security Administration (SSA) for inadequate security practices that placed sensitive medical and personal records at risk. [146]

The VA was cited for failing to prevent unauthorized system access from remote locations via its network. A GAO auditor gained access to the

VA's network and successfully accessed Privacy Act data, including veterans' loan information and personal medical information in both inpatient and outpatient files.

In the case of the SSA, SSA's Inspector General found serious weaknesses in access, continuity of service, and software program changes that placed systems at risk to cyber intrusions. The report by the Inspector General cited the SSA for employing dial-in modems on the agency's network that were not even password protected. The report cited a 1995 case in which a dozen SSA employees, taking advantage of these system security weaknesses, accessed account numbers and other personal data belonging to some 20,000 individuals. This data was sold to a West African crime syndicate, which used the information to activate and use fraudulently obtained credit cards for purchases totally $70 million. The SSA employees responsible were fired or resigned and fined an average of $100, the maximum penalties applicable under existing law at the time.[147]

During Senate hearings called to investigate these cyber security lapses, Senator Fred Thompson (R-TN), Republican Committee Chairman of the Senate Committee on Governmental Affairs, stated that it would take a major cyber event, resulting in wholesale data and service disruption, to convince agency officials that their systems are at serious risk. "There's not one thing from a government-wide standpoint that has been done to highlight this problem and to instruct people as to specific things that are expected of them in these agencies," stated Thompson at the hearing.[148]

In January 1999, the National Security Agency published a draft report of its study on government insider threats to United States critical Information systems entitled, "The Insider Threat to United States Government Information Systems: A Disaster Waiting to Happen?" The report's focus is on vulnerabilities inherent in government information systems that an insider might exploit. A critical component to this particular threat, the report cites, is the growing vulnerability created by the very nature of networked computer systems:

> The vulnerability of an insider simply removing sensitive or classified information from work is further compounded by the ever-expanding access a typical employee has to information as a result of (computer system) networking. The connectivity may even be greater than is generally known because configuration of networks is often lacking. In general, most United States Government employees with legitimate access to government systems and networks can browse and download information from several systems and networks. Use of applications and graphics packages provide them with additional privileges such as read and write capabilities. Employees, depending on their job function, may have the ability to modify, manipulate, and delete data they have access to, or they may be able to download or upload information regardless of sensitivity. Besides copying and physically removing information, an insider could also copy the information into an email file and send it, undetectable by human review, to themselves or someone else over the Internet from their office.[149]

In January 1999, as NSA was publishing its report on insider threats, an insider scandal was breaking at the Department of Energy's Los Alamos National Laboratory in New Mexico. Fifty-nine year-old scientist, Dr. Wen Ho Lee, a Taiwan-born, naturalized United States citizen, was investigated by the FBI and the DOE for alleged security violations in the theft of nuclear

weapons data from the National Lab. Two months later in March 1999, Lee was fired from his job and identified by United States law enforcement and security officials as the prime suspect in a growing espionage case involving the transfer of W-88 nuclear warhead engineering data to China.[150]

Lee, a veteran employee of the Top Secret Weapons Design Division at the Los Alamos Lab, was arrested on 10 December 1999 and indicted under the Atomic Energy Act and the Espionage Act for allegedly downloading years worth of nuclear warhead engineering and test data onto an unsecured portable computer, then transferring the information to removable (floppy) computer disks. Seven of the copied computer disks could not be produced. Lee claimed that they had been lost. As a result, Lee was jailed, without bail, on a 59-count indictment for espionage.[151] In August 2000, Lee was released from custody due to a lack of evidence.

The Lee case is the latest in a series of cases in which trusted insiders have used their offices and associated accesses to restricted information to satisfy personal, political, or financial needs. It is a sobering reality that the unauthorized, illegal accessing and electronic extraction of restricted government data has been made significantly easier by the same set of Information Technology tools and knowledge that have enabled the Information Age.

SUMMARY

Since its advent in 1955, what Alvin Toffler defined as the Third Wave, the Information Age, has reshaped the world by creating new, Information Technology-based structures for global trade, global economics, and a computer networked global society. Industrialized societies, such as the United States, have been transformed into predominantly service provision societies. Small countries, such as Malaysia, Singapore, and Indonesia, which have embraced Third Wave approaches and technologies into their societal mainstreams, have become global trading giants, with economic wealth and power far in excess of their physical size and organic natural resource base. In contrast, developing countries, such as India and China, now face the challenge of incorporating Information Age technologies and structures into rigidly controlled, hybrid First/Second Wave cultures.

As a nation's dependence on electronic commerce and networking grows, the scope of its national security policy challenge increases accordingly. As a nation's government, businesses, organizations, and citizenry become ever more dependent on electronic means for satisfying basic service delivery, the greater the potential for societal disruption or even collapse in the event of a loss of electronic infrastructure connectivity during a national crisis.

The Internet and its offspring, the World Wide Web, the National Information Infrastructure (NII), the Defense Information Infrastructure (DII), and now the emerging Global Information Infrastructure (GII), have ushered

in an era of unprecedented, real-time, global communication. Government investment in revolutionary computer network technology, beginning with the ARPANET, provided both the catalyst and technology foundation for the subsequent private sector investment in commercial computer networking, electronic commerce and e-business, that has fundamentally transformed United States society.

But universal connectivity in the Information Age carries with it a national security burden the United States has only recently begun to address. In the wrong hands, the connectivity and Information Technology tools that enable the World Wide Web and modern telecommunications, electronic banking, and electronic commerce offers unlimited access to those who would use these tools to do harm to the organizations and institutions of the United States. The critical infrastructures which underlie the complex, interdependent, information networks that are the electronic life blood of the United States, are vulnerable to hackers, cyber terrorists, insider threats, and nation states who would employ Strategic Information Warfare (SIW) techniques to undermine the government and society of the United States.

The more pervasive the electronic dependence, the more likely that an adversary will find and exploit access to more critically important enclaves within this electronic network. Even simple social engineering techniques, such as that found in the innocuous electronic, "you've got mail," message from the Melissa virus, "I Love You!," or the even more enticing, "You are one step away from winning $1 Million Dollars! Open this message NOW!," which

masks the presence of a password-collecting sniffer program, worm, virus, Trojan Horse or other invasive software tool, places the entire interconnected electronic network at risk. It is a mathematical certainty that a universal mailing of this type will result in at least one "someone," with the "right" electronic connections, opening the mail message, and unleashing the malicious software on some critically important enclave of the National Information Infrastructure. Human nature will not be denied.

Recent experiences with the Melissa and Love Bug viruses have only served to demonstrate the predicted statistical probabilities. In the case of the "Love Bug," this simple computer virus did billions of dollars of commercial damage globally and managed to penetrate NSA's secret code breaking computer system, as well as a host of other classified systems operating off of the Pentagon's secret network, SIPRNET.[152] A virus of this type can only proliferate, especially in a secure or classified computer or network enclave, through the witting or unwitting intervention of a host user.

What Cuckoo's Egg, SOLAR SUNRISE, MOONLIGHT MAZE, and a host of other intruder assaults on government computer systems fundamentally revealed that government agencies are not reliably organized to detect and defend their own automated information systems and critical infrastructures. Even more problematic are the continuing jurisdictional issues and operational concept disconnects between the key law enforcement and investigatory agencies within the DOJ and DOD, which are

charged with fighting computer hacking, computer crime, and cyber terrorism.[153] The commercial and private sectors are no better off.

What, then, should the role of the Federal Government be in assuring universal information access and fidelity in this, the Information Age? In establishing the policy framework for the future Clinton Administration during the 1991-1992 presidential campaign, William Jefferson Clinton established three policy elements and one underlying framework to develop America's electronic infrastructure. First, the future President articulated a strategy for government investment and promotion of electronic commerce through the development of a high-speed, high-bandwidth Next Generation Internet. This Next Generation Internet would be a cornerstone of a Clinton Administration drive to, "Reinvent Government," in accord with prevailing commercial business "best practices," employing the Internet as the core mechanism for service provision and an electronic government.

Second, President Clinton would promote tight control over computer systems and electronic data encryption technology. Using existing laws and Executive Orders, President Clinton, with the strong support of the national law enforcement and Federal Defense and security communities, established restrictive domestic and export controls over the proliferation and sale of strong encryption products. In doing so, the Clinton Administration attempted to preserve the government's hold on the propagation of advanced encryption technologies and maintaining an instantaneous law enforcement and Defense access to intercepted electronic information. Strong electronic

security could be assured through the use of Public Key Encryption (PKE) technology and an encryption key escrow program, with the government established as the key holder.

Third, the future President, acknowledging the need to create a secure electronic infrastructure, called for the creation of a critical infrastructure protection program, establishing "Information Assurance" as an essential foundation for national security and the expansion of electronic commerce in the United States and globally.

Underlying each of these three interconnected policy elements was a fundamental construct, first articulated on the campaign trail and held fast during all eight years of the Clinton Presidency. That would be the precept that the future of electronic commerce and Information Assurance could only evolve from an essential partnership between government and the private sector. There was one, major catch to this policy foundation: while government would invest in advanced computer and networking technology research and development, it would be the private sector which would be expected to shoulder the majority investment in exchange for ownership of America's future "electronic superhighway." That ownership responsibility would result in a hybrid, public-private sector Information Assurance-based mandate to "provide for the common defense" under tenets of Clinton Administration Information Technology, Encryption, and Critical Infrastructure Protection policy. All of these are discussed, in turn, in Chapters Five through Seven.

Chapter Five, Federal Information Technology Policy and Legislative Initiatives During Clinton Administration (1993-2000), examines the evolution of United States Federal Information Technology policy during the Clinton Administration. Major Congressional and Clinton Administration actions, taken in support of the nation's critical information infrastructure, electronic commerce, the Internet, and Information Technology is examined.

Chapter Six, Federal Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), examines the role of Federal encryption policies and export statutes in shaping the role of Information Technology applications within the society. The focus on encryption policy as the major component of Information Assurance during the Clinton Administration is also examined.

Chapter Seven, Critical Infrastructure Protection Policy and Legislative Initiatives During the Clinton Administration (1993-2000), examines the role played by United States' critical information infrastructure as the foundation of the electronic society, focusing on efforts by Congress and the Clinton Administration to evolve an effective policy for safeguarding those national assets.

Chapter Eight, Analysis of Federal Information Technology/Information Assurance Policy (1993-2000), employs the Policy as an Incremental Evolutionary Spiral (PIES) model, developed in Chapter Three, to analyze each of the three case study elements presented in Chapters Five, Six, and Seven.

[1] Alvin Toffler, *The Third Wave* (New York: William Morrow and Company,1980), 25-35.

[2] Ibid., 37.

[3] David K. Hart and William Hart, "The Organizational Imperative," *Administration and Society*, vol. 7, no. 3 (November 1975): 259.

[4] Ibid., 208.

[5] Karen Kaplan, "In Giveaway of 10,000 PCs, the Price Is Users' Privacy," *Los Angeles Times* (8 February 1999), A1.

[6] Ibid., A13.

[7] Peter G. Gosselin, " Trade Controls on Computers No Easy Goal," *Los Angeles Times* (14 June 1999), A20.

[8] Helena Webb, "Regulating Computer Exports," *Los Angeles Times*, (14 June 1999), A20.

[9] Webb, A20.

[10] Ibid., 344.

[11] Ensign James A. Calpin, U. S. Navy Reserve, "The Tyranny of Moore's Law," *Proceedings*, Vol. 126/2/1, 164 (February 2000), 64.

[12] Seymour E. Goodman, Stanford University, quoted in Peter G. Gosselin, "Trade Controls on Computers No Easy Goal," *Los Angeles Times* (14 June 1999), A20.

[13] The White House, Office of the Press Secretary, "Export Controls on Computers," 1 February 2000, 2.

[14] Webb, A20.

[15] Ibid., A20.

[16] Peter G. Gosselin, "U.S. Computer Curbs on China May Ease," *Los Angeles Times* (2 July 1999), A4.

[17] Associated Press, "Pentagon Official Denies Technology Aided China," *Los Angeles Times* (18 September 1998), A25.

[18] Ibid., A25.

[19] Peter Grier, "In the Beginning, There Was ARPANET," *Air Force Magazine*, vol. 80, no. 1 (January 1997), 68.

[20] Ibid., 66-68.

[21] Office of the Press Secretary, The White House, "Background on Clinton-Gore Administration's Next-Generation Internet Initiative," 3.

[22] Grier, 68.

[23] Ibid., 69.

[24] Ibid., 69.

[25] Office, 3.

[26] Ibid., 3.

[27] Ibid., 3.

[28] Grier, 69.

[29] James Adams, *The Next World War* (New York, NY: Simon and Schuster, 1998), 163.

[30] Grier, 69.

[31] Office, 3.

[32] Robert J. Samuelson, "Puzzles of the 'New Economy'," *Newsweek*, vol. CXXXV, no. 16 (17 April 2000), 48.

[33] Mark Z. Taylor, "Dominance Through Technology," *Foreign Affairs*, vol. 74, no. 6 (November/December 1995), 19.

[34] Clarence A. Robinson, "Orchestrating Standards Buoys Cooperative Combat Operations Operations," *SIGNAL*, vol. 51, no. 11 (July 1997), 55.

[35] Ibid., 56.

[36] Ibid., 57.

[37] President's Blue Ribbon Commission on Defense Management, *A Quest for Excellence: Final Report to the President by the President's Blue Ribbon Commission on Defense Management*, (Washington, D.C.: GPO, June 1986), 1.

[38] Ibid., 60.

[39] John Arquilla and David Ronfeldt, *In Athena's Camp* (Santa Monica, CA: RAND, 1997), p. 253.

[40] Ibid., 266.

[41] Diffie, 106 and Adams, 217.

[42] Diffie 7-12.

[43] Ibid., 9-10.

[44] John Keegan, *The Second World War,* New York: Penguin Books, 1989, 16.

[45] Ibid., Forward.

[46] Department of the Air Force, United States Air Force, "Global Engagement: A Vision of the 21st Century Air Force" (Washington D.C.: GPO, 1997), 14.

[47] H. Norman Schwarzkopf and Peter Petre, *It Doesn't Take a Hero* (New York, NY: Linda Grey Bantam Books, 1992), 300.

[48] Ibid., 300.

[49] John Arquilla and David Ronfeldt, "Cyber War Is Coming!" in *In Athena's Camp: Preparing for Conflict in the Information Age,* ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 1997), 39.

[50] Norman Davis, "An Information Revolution in Military Affairs," in *In Athena's Camp: Preparing for Conflict in the Information Age. E*d. John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corp., 1997. 79-98.

[51] Stephen J. Blank, "Preparing for the Next War," *Strategic Review*, vol. 24, no. 2, Spring 1996, 17-25, as cited in Arquilla and Ronfeldt, *In Athena's Camp,* 74.

[52] Blank, 62.

[53] Raoul Henri Alcala, "Guiding Principles for Revolution, Evolution, and Continuity in Military Affairs," as cited in Bracken and Alcala, *Whither the RMA: Two Perspectives on Tomorrow's Army* (Carlisle Barracks, PA: Strategic Studies Institute, United States Army War College, 1994), 27-29.

[54] Paul Bracken, *Future Directions for the Army*, in Bracken and Alcala, *Whither the RMA: Two Perspectives on Tomorrow's Army* (Carlisle Barracks, PA: Strategic Studies Institute, United States Army War College, 1994), 1-14.

[55] David Osborne and Ted Gaebler, *Reinventing Government* (Reading, MA: Addison-Wesley Longman, Inc., 1992), 112.

[56] Blank, 64-65.

[57] Jeffrey R. Cooper, "Another View of the Revolution in Military Affairs," *Conference Proceedings of the Fifth Annual Conference on Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, United States Army War College, 1994), in Arquilla and Ronfeldt, *In Athena's Camp*, 119.

[58] Blank, 73.

[59] Russell F. Weigley, "War and the Paradox of Technology," a review of Van Creveld, 1989, p. 1, *International Security* (Fall 1989), 196.

[60] John Arquila, David Rofeldt, and Michele Zanini, "Networks, Netwar and Information Age Terrorism," in Ian O. Lesser, et.al., *Countering the New Terrorism* (Santa Monica, CA: RAND Corp., Inc, 1999), 46.

[61] John Arquilla and David Ronfeldt, "The Advent of Netwar, " *MR-789-OSD*, 1996, 3, as cited in Arquilla and Ronfeldt, *In Athena's Camp,* 119.

[62] Vice-Adm. Arthur K. Cebrowski, USN, and John J. Garstka, "Network-Centric Warfare-Its Origins and Future," *Proceedings*, vol. 124/1/1, 139 (January 1998), 29.

[63] Clarence A. Robinson, Jr., "Information Warfare Demands Battlespace Visualization Grasp," *SIGNAL*, vol. 51, no. 6 (February 1997), 17.

[64] Ibid, p. 17.

[65] Bob Brewin, "DOD Lays Groundwork for Network-Centric Warfare," *Federal Computer Week Editorial Supplement* (10 November 1997), 1.

[66] Gregory Slabodkin, "Suit of Armor Fits 21st Century," *Government Computer News,* vol. 17, no. 8 (9 March 1998), 48.

[67] Ibid., 45.

[68] Ibid., 45.

[69] Ibid., 45.

[70] Leonard Tabacchi, DISA DII Master Plan Manager, Defense Information Systems Agency (DISA), "Defense Information Infrastructure Master Plan," Executive Summary, Appendix C: Foundation-Technology Support (6 November 1995), 4.

[71] The White House, The President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, 17.

[72] Roger C. Molander, et al, *Strategic Information Warfare Rising* (Santa Monica, CA: National Defense Research Institute, RAND, 1998), xi.

[73] Michael Elliott, et. al., Mission: Uncertain," *Newsweek*, vol. 133, no. 14 (April 5, 1999), 31.

[74] Ibid., 31.

[75] Gregory L. Vistica, "Cyberwar and Sabotage," Newsweek, vol. 133, no. 22 (May 31, 1999), 38.

[76] Ibid., 38.

[77] Michael Elliott, et al., "Special Report: The Cyberwar," *Newsweek*, vol. 133, no. 15 (April 12, 1999), 31.

[78] Sergei L. Loiko, "Chechnya: Dozens of Russians Killed," *Los Angeles Times,* 4 July 2000, A6.

[79] Ibid., 38.

[80] Greg Caires, "Air Force Seeks Information Superiority Through New Battlelab," *Defense Daily* (30 July 1997), 1.

[81] "Air Force Gets Infowar Assist," *Government Computer News*, vol. 17, no. 39 (23 November 1998), 3.

[82] Ibid., 1.

[83] John Knowles, "IW Battlelab to Go Operational This Month," *Journal of Electronic Defense*, vol. 20, no.6 (June 1997), 26.

[84] Caires, 2.

[85] Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructure* (July 1998), 1-1.

[86] CSIS Panel on Terrorism, *Combating Terrorism: A Matter of Leverage* (Washington, D.C.: The Center for Strategic and International Studies, June 1986), 9.

[87] Graham Allison, *Essence Of Decision: Explaining the Cuban Missile Crisis,* (Boston, MA: Little, Brown and Company, 1971), 1-2.

[88] Ibid., 1.

[89] Ibid., 1.

[90] Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)* (Washington, D.C.: Department of Defense, Office of the Undersecretary of Defense for Acquisition Technology, November 1996), 43.

[91] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection,* 13 October 1997.

[92] Ibid., 45.

[93] Ibid., 8.

[94] Ibid., 8.

[95] The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection,* Version 1.0, January 2000, 7.

[96] Cliff Stoll, *The Cuckoo's Egg* (New York, NY: Pocket Books, 1990), 9.

[97] Ibid., 7.

[98] The White House, Office of the Vice President, The Vice President's Task Force on Combatting Terrorism, letter from Vice president George Bush accompanying the release of the "Public Report of the Vice President's Task Force on Combatting Terrorism" (Washington, D.C.:U.S. GPO, February 1986), 2.

[99] CSIS Panel on Terrorism, inside cover.

[100] Ibid., 8.

[101] Ian O. Lesser, et. al., *Countering the New Terrorism* (Santa Monica, CA: RAND Corp., 1999), 41.

[102] Ibid., 42.

[103] Neil Munro, "Pearl Harbor," The Washington Post (16 July 1995), C3.

[104] Sharon Gaudin, "Hacks Gain in Malice, Frequency," *Computerworld*, vol. 32, no, 41 (12 October 1998), 38.

[105] William Jackson, "Agencies Say Security is a Bigger Task Than Y2K," *Government Computer News*, vol. 18, no. 13 (10 May 1999), 6.

[106] "Pentagon Computers are Easy Prey for Hackers, GAO Warns," *Los Angeles Times* (23 May 1996), A1.

[107] Ibid., A1

[108] Stoll, 1.

[109] The White House, The President's Working Group on Unlawful Conduct on the Internet, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet," March 2000, 26.

[110] Stoll, 78-88.

[111] Op. Cit., 26.

[112] Stoll, 322-328.

[113] Ibid., 352-353.

[114] John J. Fialka, "Pentagon Studies Art of 'Info War' to Reduce Its Systems Hackers, *The Wall Street Journal* (3 July 1995), A20.

[115] M.J. Zuckerman, "Hacker Pair Illustrate Pentagon's Vulnerabilities," USA Today (23 May 1996), A3.

[116] Ibid., 8.

[117] Ibid., 8

[118] Ibid., 8.

[119] Gregory Vistica, "We're in the Middle of a Cyberwar," *Newsweek*, Vol. CXXXIV, no. 12 (20 September 1999), 52.

[120] Ibid., 52.

[121] Ibid., 52.

[122] Ibid., 52.

[123] Bob Drogin, "Yearlong Hacker Attack Nets Sensitive U.S. Data," *Los Angeles Times* (7 October 1999), A15.

[124] John J. Goldman and Usha Lee McFarling, "Man Accused of Hacking Into NASA Computers, *Los Angeles Times* (13 July 2000), A15.

[125] Ibid., A15.

[126] Ibid., A15.

[127] Zuckerman, 8.

[128] Sharon Gaudin, "Hackers Disrupt N.Y. Times Site," *Computerworld*, vol. 32, no. 38 (September 21, 1998), 6.

[129] "Hacker Invades EBay Online Auction Site," *Los Angeles Times* (20 March 1999), C2.

[130] Ibid., A15.

[131] Ibid., A1.

[132] Ibid., A15.

[133] Brad Stone, "Bitten by Love," *Newsweek*, Vol. CXXXV, No. 20 (15 May 2000), 42.

[134] Ibid., 43.

[135] United States General Accounting Office, "Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000," Statement of Joel C. Willemssen, Director, Civil Agencies Information Systems, Accounting and Information Management Division, GAO before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, United States House of Representatives, 22 June 2000, 8.

[136] George Wehrfritz, "Raiding the 'Love Bug,'" *Newsweek*, Vol. MM, No. 21 (22 May 2000), 44.

[137] Jube Shiver, Jr. and Charles Piller, "U.S. Role Hit as Latest Computer Bug Scare Fizzles," *Los Angeles Times* (20 May 2000), C1.

[138] Ibid., C3.

[139] Ibid., C1.

[140] Ibid., C3.

[141] Computer Security Institute and the FBI International Computer Crime Squad, San Francisco Office, "Computer Crime and Security Survey," cited in Department of Defense, National Security Agency, "The Insider Threat to United States Government Information Systems (Draft)," January 1999, 2.

[142] Department of Defense, National Security Agency, "The Insider Threat to United States Government Information Systems (Draft)," January 1999, 3.

[143] Ibid., 3.

[144] Ibid., 3.

[145] Ibid., 4.

[146] Frank Tiboni, "Thompson Upbraids Agencies Over Systems Securities," *Government Computer News*, vol. 17, no. 35 (19 October 1998), 9.

[147] Ibid., 9.

[148] Tiboni, 9.

[149] Ibid., 4-5.

[150] The Washington Post, "Hearings Reveal FBI Had Doubts Lee Was China Spy," *Los Angeles Times* (7 March 2000), A22.

[151] Bob Drogin, "Defense Shows Holes in Case Against Scientist," *Los Angeles Times* (19 August 2000), A12.

[152] George Wehrfritz, "Raiding the 'Love Bug,'" *Newsweek,* vol. MM, no. 21 (22 May 2000), 44.

[153] Ibid., 8.

CHAPTER FIVE

INFORMATION TECHNOLOGY POLICY AND LEGISLATIVE INITIATIVES DURING THE CLINTON ADMINISTRATION (1993-2000)

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

The purpose of Chapter Five is to chronicle the specific actions and activities by the Federal Government in support of United States' Information Technology policy during the eight years of the Clinton Administration. This case study provides a chronological ordering of the policy-specific activities and associated impacts of Federal Information Technology policy decision makers operating within the three branches of the Federal Government between the years 1993 and 2000.

The chapter is organized by calendar year. For each calendar year, significant Federal Information Technology policy activities undertaken by the Clinton Administration, Congress, and the Federal Judiciary are chronicled. For the purposes of this study, a "significant Federal Information Technology policy activity" is defined as: an administrative action, e.g., the publication of an Executive Order, formation of a Federal Advisory Commission, issuance of a report or formal policy statement by the White House; activity on a related bill by Congress; or a hearing or judgement rendered on a related case brought before a Federal court. In years where no significant Federal

Information Technology policy activity was manifest, no annotation in the chapter chronicle was made.

BACKGROUND--SETTING THE STAGE

On 16 April 1992, during a campaign speech at the University of Pennsylvania's Wharton School of Business, Arkansas Governor and Presidential aspirant, William Jefferson Clinton, proclaimed that the United States was in need of a formal strategy for creating a national information network.

> In the new economy, infrastructure means information as well as transportation. More than half the United States workforce is employed in information-intensive industries, yet we have no national strategy to create a national information network. Just as the interstate highway system in the 1950s spurred two decades of economic growth, we need a door-to-door fiber optics system by the year 2015 to link every home, every lab, every classroom, and every business in America... We should also change the way we create infrastructure for the next century. New sources of investment capital can be tapped from the private sector, in partnership with government. For example, we should consider creating a Federal, self-financing public-private corporation to support viable infrastructure projects that can attract some private capital.[1]

With these words, candidate Clinton articulated a vision that, over time, would emerge as one of the fundamental tenets of his presidential platform. In the process, Information Technology and plans for a "National Information Network," became an underlying theme of the Clinton presidential campaign. Six months later, the details of Clinton's Information Technology plan emerged in a draft entitled, "Technology: The Engine of Economic Growth--A National Technology Policy for America."

Technology: The Engine of Economic Growth--A National Technology Policy for America

On 18 September 1992, Governor Clinton outlined the fundamentals of his future technology program. In his offering, candidate Clinton stressed renewal of the "civilian technology base" and the construction of an Information Superhighway, composed of advanced communication networks and computers, as the number one technical policy priority of a Clinton Presidency:

> First and foremost, a Clinton-Gore Administration will emphasize the need to renew our civilian technology base. America cannot continue to rely on trickle down technology from the military to maintain competitiveness of its high-tech and manufacturing industries. Civilian industry, not the military, is the driving force behind advanced technology today. Only by strengthening our technology base can we solve the twin problems of national security and economic competitiveness.[2]

As the future Vice President, the serving Senator from Tennessee, Albert Gore, Jr., would lead the efforts of a new administration to implement the Clinton/Gore national technology strategy.

> The Vice President will take on the task of organizing all facets of government to develop and implement my Administration's technology policy. As a first step, he will establish a central focus for the coordination of government activities related to civilian technology and create a forum for systematic private sector input into United States Government deliberations about technology policy and competitiveness.[3]

The keystone of Governor Clinton's five-part Information Technology vision was the building of a 21st Century information infrastructure for the United States. Key to this envisioned infrastructure initiative would be the

development of an "Information Superhighway," the heart of which would consist of an advanced information infrastructure and communications network "backbone," designed to facilitate collaborative research and development activities throughout both public and private sectors.[4]

National Performance Review: Reinventing Government Through Information Technology (IT)

A second cornerstone of William Jefferson Clinton's 1990-1991 campaign for the White House was grounded in his conviction that government had become inefficient and lacked the ability to be responsive to the electorate. Clinton called for a "national performance review" of the Federal bureaucracy, with a goal of reforming the Federal administrative structure along the lines advocated by Reinventing Government advocate and guru, David Osborne. The Clinton Administration National Performance Review (NPR), also known as Reinventing Government, spearheaded by Vice-President Albert Gore, Jr., would become the latest in a series of 20th Century United States Presidential initiatives focused on making the United States Federal Government more responsive to the needs of its collective citizenry.[5] Appendix B provides a thumbnail summary of these 20th Century administrative reform initiatives.

On 1 September 1993 and as an underpinning to the NPR, the Clinton Administration unveiled a broad-based roadmap intended to catalyze fundamental changes in the way government utilizes Information Technology

to perform its mission. The plan articulated thirteen specific statutory, regulatory, and process initiatives the Clinton Administration would attempt to undertake in pursuing its Reinventing Government through Information Technology goals.[6]

To lead this effort, Vice President Gore created NPR's Information Technology (IT) Team. The team consisted of Information Technology professionals, budget, and logistics personnel from both the public and private sectors. The team undertook formal training in Quality Functional Deployment (QFD) techniques, used to help define NPR projects and to provide a framework for NPR decision making and on-going, evaluative activities. QFD is a structured, total quality management (TQM) method used by planning groups to clarify issues and problems to be addressed and to identify strategies to obtain optimal results, while achieving stated objectives within a predetermined timeframe.[7]

The team identified a number of fundamental issues requiring specific Administration attention to sufficiently enable Information Technology to serve as the technical catalyst for maximizing government service delivery efficiency:

- The Information Technologies currently employed by the Federal Government are not delivering what the customer needs, nor is its potential being fully utilized;
- The Federal Government does not adequately coordinate the systems now in place;

- There is insufficient understanding of who the customers for Information Technology are and what their needs are;
- Too many barriers exist within the government, both regulatory and legislative, to use Information Technology effectively;
- All levels of the government workforce need continuous education in Information Technology.[8]

Why Information Technology? Clinton Administration NPR and Reinventing Government advocate David Osbourne's tenets were optimized within an Information Technology-rich administrative environment. They were designed to work best in societies where an established electronic information infrastructure makes virtual government possible. Developing nations, those evolving from agrarian to industrial societies, face many of the organizational and control challenges faced by the United States at the turn of the 19th and 20th centuries. Their social, economic, and political issues are very different from an emergent Information Age society, such as the United States. Technology-dependent NPR was tailor-made for Information Age process improvement initiatives. [9]

NPR's intensive reliance on Information Technology as its organizational and administrative change agent cannot be overstated. Vice President Gore summed up this key dependency in this manner:

> With computers and telecommunications, we need not do things as we have in the past. We can design a customer-driven, electronic government that operates in ways that, ten years ago, the most visionary planner could not have imagined.[10]

Through his support for Information Technology and the NPR initiative, President Clinton made good on his campaign pledge to become the nation's "High Tech President." The record of the Clinton Administration, particularly that of the First Administration from 1993-1996, supports this contention. From its first days, the Clinton Administration committed itself to creating a public-private partnership for the development of a National Information Infrastructure (NII), featuring high-performance computing and a Next Generation Internet (NGI).

President Clinton's initial act in support of this goal was directing the Office of Science and Technology Policy (OSTP) to establish the Information Infrastructure Task Force (IITF) in May 1993. This was followed, in September 1993, by Executive Order 12864, establishing the United States Advisory Council on the National Information Infrastructure (NII).

CONGRESS--1991

S.272: The High-Performance Computing Act of 1991 (Public Law 102-194)

On 24 January 1991, during the 1st Session of the 102nd Congress and prior to his joining the Clinton presidential ticket, Senator Albert Gore, Jr. (D-TN) sponsored Senate Bill 272 (S.272), legislation supporting government research and development in high-speed computing and high-capacity, high-speed networking.[11]

The High-Performance Computing Act of 1991, which became Public Law 102-194 on December 9, 1991, enjoyed bipartisan support in both the

House and the Senate. The High-Performance Computing Act of 1991 became the backbone for the United States High-Performance Computing and Communications (HPCC) Program. The HPCC would form the nucleus of the Clinton Administration's National Information Infrastructure (NII) vision.

BUSH ADMINISTRATION--1992

The High-Performance Computing and Communications (HPCC) Program

Though President Bush signed Public Law 102-194 into existence, it was his political rival and successor, President William Clinton, who made the High-Performance Computing Act of 1991 the Federal Government's flagship research and development program for advanced computing and networking technologies. As early as January 1992, Clinton Administration plans for a National Information Infrastructure (NII) were forming around results anticipated from research conducted under the High-Performance Computing and Communications (HPCC) Program. These results were key to fulfilling Clinton campaign pledges to support the demands of the globally interconnected environment and for furthering the virtual government capabilities envisioned by the Administration's National Performance Review (NPR).

> The Clinton Administration believes that the Federal Government has several important roles to play in assisting the development of this infrastructure, which will be built and run primarily by the private sector. In many ways, the High-Performance Computing and Communications (HPCC)

> Program provides the technological foundation upon which the Administration's strategy for the NII rests. [12]

HPCC activities were coordinated by the Computing, Information, and Communications (CIC) Subcommittee of the Committee on Computing, Information and Communications (CCIC), one of nine committees comprising the National Science and Technology Council (NSTC). The CIC Subcommittee would become the new moniker for the High-Performance Computing, Communication, and Information Technology (HPCCIT) Subcommittee.

Overall funding for the HPCC Program enjoyed steady support in the Congress and from the Clinton Administration during its eight-year tenure. In FY 1991, and even before the formal start of the Program, the HPCC-related activities of the original eight agencies totaled $489 million. This amount was used to establish the program's initial funding baseline. In 1992, program funding by the Congress was increased 34% to $655 million.

With the HPCC Program part of the Administration's Research and Development (R&D) portfolio, program oversight responsibility fell to the National Science and Technology Council's (NSTC) Committee on Computing, Information, and Communications (CCIC). The HPCC Program formed the core of the CIC's R&D programs.

High-Performance Computing Systems (HPCS) would serve as the focal point for all five research initiatives making up the HPCC program. The goal of HPCS R&D would be to provide the foundation for U.S. leadership in

computing, through investments in leading-edge hardware and software, and especially in algorithms and software development to be used in modeling and simulations needed to address "National Challenges"--major societal needs that computing and communications technology can help address--including design and manufacturing, health care, education, digital libraries, environmental monitoring, energy demand management, public safety, and national security. HPCC would serve as the centerpiece of the future Clinton Administration National Information Infrastructure (NII) initiative.[13]

CONGRESS--1992

S.2937: The Information Technology Act of 1992

Introduced on 1 July 1992 by Senator Albert Gore, Jr. (D-TN), S.2937, the Information Technology Act of 1992 was intended to amend the National Science and Technology Policy, Organization, and Priorities Act of 1976 and to extend the provisions of the High-Performance Computing Act of 1991. The bill would require the Director of the Office of Science and Technology Policy, through the Federal Coordinating Council for Science, Engineering, and Technology, to establish an Information Infrastructure Program and five-year implementation plan to expand Federal efforts to develop technologies for applications of high-performance computing and high-speed networking. It would also provide for a coordinated Federal program to accelerate

development and deployment of an advanced national information infrastructure.[14]

The bill was short-lived. Read twice on the floor of the Senate, the bill was referred to the Senate Committee on Commerce on 1 July 1992, where no further action was taken to advance it beyond the Committee.[15] The sense of the pre-election Senate was to await the outcome of the general elections in November, allowing a new administration offer a course of action for national investments in the Internet and related Information Technologies. Additionally, the Republicans in the Senate were in no rush to hand the Democratic ticket what seemed to be an unnecessary, pre-election victory by endorsing another Gore-sponsored, high technology bill.

H.R. 5759: The Information Infrastructure and Technology Act of 1992

On 4 August 1992, Congressman George E, Brown, Jr. (D-CA) introduced H.R.5759, the Information Infrastructure and Technology Act of 1992. H.R. was presented by Congressman Brown as the companion bill to S.2937, the Information Technology Act of 1992, introduced 1 July 1992 in the Senate by Senator Albert Gore, Jr. (D-TN).[16]

Much like S.2937, H.R.5759 was intended to build upon the merits of the High-Performance Computing Act of 1991. It would expand Federal efforts to develop technologies for applications of high-performance computing and high-speed networking. It would also provide for a

coordinated Federal program to accelerate development and deployment of an advanced national information infrastructure.[17]

H.R.5759 fared little better than its ill-fated Senate twin, and for much the same reasons. On 4 August 1992, the bill was referred to the House Committee on Science, Space and Technology, which referred it concurrently to its two Subcommittees on Technology and Competitiveness and Science. Subsequent to the Subcommittee referrals, no further action was taken on the bill.[18]

CLINTON ADMINISTRATION--1993

The Information Infrastructure Task Force (IITF)

A fundamental tenet of the Clinton Administration's vision for the National Information Infrastructure (NII) was grounded on the premise that the private sector would build and operate it. However, in recognition of the Federal Government's key leadership role in its development, in September 1993, the Clinton Administration chartered an Information Infrastructure Task Force (IITF) to coordinate and implement the Administration's vision for the NII. Created as a Federal Government interagency task force, the IITF membership included high-level representation from the various Federal agencies playing major roles in the development of telecommunications and information technologies and policy for the Federal Government.[19]

The task force operated under the aegis of the White House Office of Science and Technology Policy and the National Economic Council.

Secretary of Commerce Ronald Brown was selected to chair the IITF. The staff work for the task force was accomplished by the National Telecommunications and Information Administration (NTIA) of the Department of Commerce. Additionally, Through Executive Order 12864, President Clinton created a high-level Advisory Council on the National Information Infrastructure to provide guidance and oversight for the IITF.[20]

The IITF was organized into three working committees. The Telecommunications Policy Committee, responsible for formulating a consistent Administration position on key telecommunications issues, was chaired by the head of the National Telecommunications and Information Administration of the Department of Commerce.[21]

The Information Policy Committee, responsible for addressing critical information policy issues and chaired by the head of the Office of Information and Regulatory Affairs at the Office of Management and Budget (OMB), was organized into three working groups: a Working Group on Intellectual Property Rights, chaired by the head of the Patent and Trademark Office of the Department of Commerce; a Working Group on Privacy chaired by the Director of the Office of Consumer Affairs, Department of Health and Human Services; and a Working Group on Government Information chaired by the Director of OMB's Office of Information and Regulatory Affairs.[22]

The Applications Committee, chaired by the Director of the National Institute of Standards and Technology, assumed responsibility for implementing the recommendations of the Vice President's National

Performance Review pertaining to information technology. The Committee established a single working group, the Working Group on Government Information Technology, or GITS, to coordinate efforts to improve the application of information technology by Federal agencies.[23]

The IITF was chartered to work closely with the High Performance Computing, Communications, and Information Technology (HPCCIT) Subcommittee of the Federal Coordinating Council for Science, Engineering, and Technology (FCCSET), which in 1993 was chaired by the Director, White House Office of Science and Technology Policy. The HPCCIT Subcommittee assumed responsibility for providing technical advice to the IITF and coordinating Federal research activities in support of the development of the National Information Infrastructure.[24]

Executive Order 12864: United States Advisory Council on the National Information Infrastructure (NII)

On 15 September 1993, President Clinton issued Executive Order 12864, establishing a Federal Advisory Council, under the office of the Secretary of Commerce, to advise the President in the development of a national strategy for promoting the National Information Infrastructure (NII). EO 12864 defined the National Information Infrastructure as:

> The integration of hardware, software, and skills that will make it easy and affordable to connect people with each other, with computers, and with a vast array of services and information resources.[25]

The Council was formed as a vehicle for making recommendations to the President on the appropriate roles of the private and public sectors in developing the National Information Infrastructure. This was in accord with an evolving public and commercial applications framework envisioned for the National Information Infrastructure. The Council was asked to address issues of national security, emergency preparedness, system security, and network protection implications for the NII, while exploring a national strategy for maximizing interconnectivity and inter-operability with existing communication networks. Universal access and international connectivity issues were to be major considerations of the Council.[26]

Though the Council was free to address a wide-range of issues associated with the NII, Chairman Ronald Brown identified two main objectives as the Council's primary focus. The first was to establish a functioning working arrangement between the public and private sectors, with an aim toward encouraging private sector leadership and investment in the NII.[27]

The second was to develop a framework for the NII that was consistent with both public sector information management needs and private sector commercial applications. In support of this second objective, the Council examined various approaches for evolving a national strategy for developing and demonstrating applications in areas such as electronic commerce, government services, national security, emergency preparedness, system security, and network protection. In November of

1993, the Council issued a draft plan for evolving a comprehensive strategy by mid-year 1994.[28]

Executive Order 12881: Establishment of the National Science and Technology Council (NSTC)

On 23 November 1993, President Clinton executed Executive Order 12881, establishing the National Science and Technology Council (NSTC). The NSTC's primary function was coordinating the science and technology policy-making process of the United States Government, consistent with the stated science and technology goals of the President Clinton and his Administration. An important objective of the NSTC was the establishment of clear national goals for Federal science and technology investments in the areas of Information Technology and strengthening programs of fundamental research and development in advanced networking technologies.[29]

The cabinet-level Council, chaired by the President himself, was composed of the Vice President; Secretaries of Commerce, Defense, Energy, Health and Human Services, State, and the Interior; the Administrator of NASA; the Director of the National Science Foundation; the Director of OMB; the Administrator, EPA; the Assistant to the President for Science and Technology; the National Security Advisor; the Assistant to the President for Economic Policy; and the Assistant to the President for Domestic Policy.[30] The Council was charged by the Executive Order with assisting the President in integrating his science and technology policy agenda across the Federal Government, ensuring that information science

and technology be considered in the development and implementation of all Federal policies and programs.[31]

Executive Order 12882: President's Committee of Advisors on Science and Technology Policy (PCAST)

As a companion to the President's National Science and Technology Council, on 23 November 1993, President Clinton created the President's Committee of Advisors on Science and Technology Policy (PCAST). The 16 member PCAST was initially made up of 15 (amended to 18) "distinguished, nonfederal sector individuals," plus the Assistant to the President for Science and Technology, who served as its co-chair, along with a nonfederal member of the Council, who would be selected by the President.[32]

The PCAST was created as an advisory committee to the President under the auspices of the Federal Advisory Committee Act (5 U.S.C. App.). The PCAST was chartered to advise the President, through the Assistant to the President for Science and Technology Policy, on matters involving science and technology. In particular, it was envisioned that PCAST support would play a pivotal role within the National Science and Technology Council, securing private sector involvement and support for the Administration's science and technology initiatives.

CONGRESS--1993

H.R. 1757: The High-Performance Computing and High-Speed Networking Applications Act of 1993

The first of the post-election, Clinton Administration-endorsed Congressional measures supporting investment in Information Technology was H.R.1757, the High-Performance Computing and High Speed Networking Applications Act of 1993. Introduced on 21 April 1993 by Congressman Rick Boucher (D-VA), H.R.1767 provided for a coordinated federal program to accelerate development and dissemination of applications of high-performance computing and high-speed networking. Renamed the National Information Infrastructure Act of 1993, the bill would amend the High-Performance Computing Act of 1991 and would direct the Federal Coordinating Council for Science, Engineering, and Technology to establish a public/private sector interagency program, whose charter would be to develop applications of computing and networking under the National High-Performance Computing Program.[33]

The bill would require the Federal Coordinating Council for Science, Engineering, and Technology to develop both a comprehensive research and development investment plan and a plan to foster local network access to NII services. The bill would authorize funding of $1.3 billion for the program from FY1994 through FY1998. Funding would terminate on 1 October 1996.[34]

Initially referred to the House Committee on Science, Space and Technology on 26 April 1993, the bill was forwarded to the Subcommittee on Science for hearings on 27 April 1993. On 27 April 1993, Dr. John H. Gibbons, Clinton Administration Director of the Office of Science and Technology Policy, testified before the Congress in support of H.R.1757. In

his remarks, Dr. Gibbons articulated the Administration's fundamental policy position with respect to High-Performance Computing and Communications:

> The Clinton Administration believes that the Federal Government has several important roles to play in assisting the development of this infrastructure, which will be built and run primarily by the private sector. In many ways, the High-Performance Computing and Communications (HPCC) Program provides the technological foundation upon which the Administration's strategy for the NII rests. The HPCC is a critical part of the Administration's effort to build the NII.[35]

Additional hearings, held on 6 and 11 May 1993, were followed by a Subcommittee mark-up session on 17 June 1993. The bill, as amended, was forwarded to the full Committee on 17 June 1993, where, following the full Committee mark-up session on 30 June 1993, was ordered reported to the House for consideration. On 13 July 1993, the Committee on Science, Space and Technology reported out the bill to the full House, as amended (House Report 103-173). The bill was then placed on the Union Calendar (Calendar No. 97) for full House consideration.[36]

During the floor discussion prior to the vote on H.R.1767, Congressman Boucher, in presenting the bill, stated:

> Mr. Speaker, H.R.1757 embodies the President's vision for a national information highway capable of routing voice, video and data traveling at gigabit speeds to every school, every home, every research institute, and every business in the Nation. It clearly identifies the respective roles of the public and private sectors in deploying, owning, and operating the information infrastructure, and it specifies the Federal research and development support that should be provided to enable the creation of new networking technologies and a variety of near-term applications of the information network. H.R.1757 makes it clear we do not expect the Federal Government to own,

> manage, or deploy the information infrastructure. That will be a private sector responsibility.[37]

On 26 July 1993, the bill was called up by the full House, under suspension of the rules, and voted upon. The measure passed the House, as amended, on a vote of 326 to 61.[38] The overwhelming majority vote in support of the bill's passage was indicative of the degree of bipartisan support the bill enjoyed. However, the bill was not without its detractors. Congressman Dan Burton (R-IN) rose in opposition saying:

> Mr. Speaker, I think the thought behind this program is very good. The only problem I have with it is, why is the Federal Government going to pay $1 billion for a program that is already being worked in the private sector?...MCI is working on this, Sprint is working on it, and a great many private sector communications companies are working on these things right now. So my question is, since the private sector is working very hard on this, since they are going to make a profit out of it ...why should we be spending $1 billion over the next few years when the private sector is already working on it?[39]

Congressman Eddie B. Johnson (R-TX) also rose in opposition of the bill, but his concerns were not only focused on the issues of cost:

> In this bill I have counted the word 'develop' over 20 times. I ask anyone to answer this question: What can the government 'develop' better than the private sector? From past experience, nothing better, but definitely slower.[40]

On 27 July 1993, the bill was received in the Senate and read twice before being referred to the Senate Committee on Labor and Human Resources, on 14 September 1993. The bill was subsequently referred to the Subcommittee on Education, Arts, and Humanities, where no further action was taken.[41]

CLINTON ADMINISTRATION--1994

Information Infrastructure Task Force (IITF)

On 4 May 1994, Secretary of Commerce and IITF Chair, Ronald Brown, released for public comment, an IITF report focused on ways that the National Information Infrastructure could be used to strengthen the United States economy and "improve the overall quality of life" in the United States.[42]

The report, "Putting the Information Infrastructure to Work," closely examined the opportunities for and obstacles to growth in seven key applications areas of the NII. In directing the authoring of the paper, Secretary Brown stated that it was designed to spur public debate and discussion on how people and organizations should best use the information infrastructure:

> There's going to be a fundamental change in the way we work, the way we learn, the way we communicate. Knowing how the Industrial Revolution permanently altered American life, we can only begin to imagine how we will be transformed by becoming an information society.[43]

The report strongly reflected Secretary Brown's personal vision of the NII, including not only how its application could improve commerce, but also how the technology could be made to address a host of social welfare issues, including:

- Enhancing the competitiveness of the manufacturing base;
- Increasing the speed and efficiency of electronic commerce;

- Improving health care delivery and controlling health care costs;
- Promoting the development and accessibility of a quality education and lifelong learning;
- Making the nation more effective at environmental monitoring and assessing its impact on the planet;
- Sustaining the role of libraries as agents of democratic and equal access to information; and,
- Providing government services to the public faster, more responsively, and more efficiently.[44]

Second Network Reliability Council (NRC)

In 1994, the Network Reliability Council (NRC) was re-chartered by the FCC to assess the future of electronic threats to telecommunications network reliability. At the behest of the FCC, the Second Council continued to evaluate network performance issues as it addressed network reliability concerns arising from of increased interconnections to the public switched network (PSN) and new technologies being deployed within it. In addition, the Council was asked to provide the FCC guidelines for improving access to telecommunications services for emergency services and to evaluate regional impacts of service outages.[45]

CLINTON ADMINISTRATION--1995

Drafting Panel on the Global Information Infrastructure

Between 29 and 30 March 1995, a drafting panel on the Global Information Infrastructure met during a White House forum on the Role of

Science and Technology in Promoting National Security and Global Stability. The forum, held in Washington, D.C. and hosted by the National Academy of Science, was called to discuss the role Information Technology should play in economic development and national security. To explore these issues in depth, an ad hoc working group was formed to examine the effects that Information Technology and the development of a seamless global information network might have on United States national security, while at the same time promoting global economic development.[46]

Co-chaired by Michael Nelson of the White House Office of Science and Technology Policy (OSTP) and John Gage of Sun Microsystems, representatives from ten Federal agencies, several commercial companies, and a diverse group of subject matter experts gathered during this venue to discuss the Global Information Infrastructure (GII).

In general, the group concluded that national security problems created by statutes and treaties enabling foreign companies to engage in the United States' marketplace through electronic means, are dwarfed by the benefits accrued from increased, reciprocal global market access and investment opportunities:

> Although the group devoted more time to the possible problems that the Global Information Infrastructure will pose for United States national security, the members were unanimous in their conviction that the benefits of the GII far out-weigh the problems it prevents. There was also a consensus that the Digital Revolution is happening whether the policy makers are prepared or not and that national security and foreign policy communities must devote more attention to critical issues, such as security of telecommunications networks, encryption policy,

> improving the use of information and telecommunications technologies in foreign aid programs, and ensuring that electronic money and intellectual property can be safely transported over the GII.[47]

The output from forum became a white paper entitled, "The Global Information Infrastructure." The paper provides background material on the Clinton Administration's Global Information Infrastructure (GII) initiative, designed to catalyze development of a global "network of networks" and extend electronic commerce and Internet connectivity world-wide.[48]

This white paper reflected the underlying tenets of the Clinton Administration's GII initiative, identifying it as a comprehensive effort to address a wide range of telecommunications policy, technology policy, and information policy issues related to the establishment of world-wide electronic commerce. The drafting panel's product echoed the findings of a report published by the Information Infrastructure Task Force entitled "The Global Information Infrastructure-Agenda for Cooperation."[49]

Information Infrastructure Task Force

Shortly after the publication of "The Global Information Infrastructure-Agenda for Cooperation, " the Information Infrastructure Task Force delivered another of its study products to the White House. On June 5, 1995, the IITF released its report, "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information." Authored by the Privacy Working Group of the IITF's Information Policy

Committee, the study report defines a blueprint for privacy "rules of engagement" for the NII.[50]

The report noted the convergence of two trends, one social and one technological, associated with the rise of electronic commerce and the evolution of the NII. Both trends suggested an evolving risk to data rights and individual informational privacy. As a social trend, individuals using the NII to satisfy daily business and service delivery needs would be, by transactional necessity, unconsciously sanctioning the collection of privacy data required to document these transactions. NII transactional data would, by necessity, record privacy-related details of each transaction including data on who communicated with whom, when, and for how long, as well as who bought what, and at what price. This type of personal information is automatically generated in electronic form, and is, therefore, especially easy to store and process.[51] As more and more personal information appears on-line, detailed individual profiles could be extracted from this data in a matter of seconds and at minimal cost.[52]

The bulk of the report devoted itself to this matter, articulating a set of 34 guiding principles recommended as standards for the exchange and use of personal information on the NII. These 34 guiding principles were collectively called, "Principles for Providing and Using Personal Information."[53] The paper concluded by stating:

> New principles should not diminish existing constitutional and statutory limitations on access to information, communications, and transactions, such as requirements for warrants and

> subpoenas. Such principles should ensure that access limitations keep pace with technological developments. These principles should acknowledge that all elements of our society share responsibility for ensuring the fair treatment of individuals in the use of personal information, whether on paper or in electronic form. [54]

Executive Order 12974: Continuance of Certain Federal Advisory Committees

Pursuant to the 24-month expiration clause of the Federal Advisory Committee Act (5 U.S.C. App.), on 29 September, President Clinton extended the termination date of the President's Committee of Advisors on Science and Technology Policy (Executive Order 12882, as amended) to 30 September 1997.

CONGRESS--1995

Public Law 104-13: The Paperwork Reduction Act of 1995

On 4 January 1995, the 1st Session of the 104th Congress enacted Public Law 104-13, the Paperwork Reduction Act of 1995. The goal of the Paperwork Reduction Act was:

> To have Federal agencies become more responsible and publicly accountable for reducing the burden [cost] of Federal paperwork on the public.[55] The purpose of the Act is: To minimize the paperwork burden [to the citizenry] resulting for the collection of information by or for the Federal Government,[56] while seeking to: Improve the quality and use of Federal information to strengthen decision-making, accountability, and openness in government and society.[57] The Act also stipulates that its purpose is to: Ensure that information technology is acquired, used, and managed to improve performance of agency missions."[58]

With passage of the Paperwork Reduction Act of 1995, Congress signaled the Clinton Administration that it would join its efforts to reduce the cost of government by reducing the mountains of paper and paper documents generated annually by the Federal Government. By directing the migration of Federal departments and agencies toward a paperless environment, Congress and the Clinton Administration both hoped to reduce and eventually to eliminate the huge annual paper and printing costs of the Executive and Legislative Branches.

At the same time, the Act provided a useful platform for promoting the public use of the Internet as an alternate mechanism for securing copies of government records and publications. Prior to the Internet, these documents had previously been available, for a price, only through the Government Printing Office (GPO), department and agency printing facilities, and Federal mail order libraries. Through electronic access, these same documents could now be retrieved and downloaded to the requester, at no cost to the requester and at a minimal recurring cost to the government.

CLINTON ADMINISTRATION--1996

United States Advisory Council on the National Information Infrastructure

On 30 January 1996, the Advisory Council on the National Information Infrastructure delivered its final report to President Clinton entitled, "A Nation of Opportunity: Realizing the Promise of the Information Superhighway." In this report, the Council summarized the Administration's implementation plan

for the NII. The conclusions and recommendations served as validation for the initial 15 September 1993 submission of the IITF, "National Information Infrastructure: An Agenda for Action," which itself served as the Task Force manifesto.[59]

The report reiterated the Clinton doctrine of private sector ownership and responsibility for developing and operating the NII, with strategic research and development assistance, along with political leadership, from the Federal Government:

> While the superhighway is primarily a private sector initiative, all levels of government have significant roles to play in ensuring the effective development and deployment of the Information Superhighway...The Federal Government has a vital role in sustaining a strong research and development base in information technology, through university and corporate programs.[60]

In this final report, the Council concluded its work by espousing a set of five, overarching NII goals for the United States to embrace:

> First, let us find ways to make Information Technology work for us, the people of this country, by ensuring that these wondrous new resources advance American constitutional precepts, our diverse cultural values and our sense of equity.
>
> Second, let us ensure, too, that getting America on-line results in stronger communities, and a stronger sense of national community.
>
> Third, let us extend to every person in every community the opportunity to participate in building the Information Superhighway. The Information Superhighway must be a tool that is available to all Americans--people of all ages, those from wide range economic, social, and cultural backgrounds, and those with a wide range of functional abilities and limitations--not just a select few. It must be affordable, easy to use, and

> accessible from even the most disadvantaged neighborhood or remote dwelling.
>
> Fourth, let us ensure that we Americans take responsibility for the building of the Superhighway--private sector, government at all levels, and individuals.
>
> And, Fifth, let us maintain our world leadership in developing the services, products, and an open and competitive market that lead to development of the Information Superhighway. Research and development will be an essential component of its sustained evolution.[61]

Following delivery of this final report, the IITF was disbanded in February 1996.

Second Network Reliability Council (NRC)

The Network Reliability Council's recommendations for improving the reliability of telecommunications services for emergency communications, and its evaluations of regional impacts of service outages, were made to the FCC in the Second Council's final report, "Network Reliability: The Path Forward," which was published in February 1996.[62]

The five chapters of the NRC report discussed network reliability performance, increased interconnections, emerging technologies, essential emergency communications, and the impact of telecommuting on the public networks. In its discussions of network interconnections, the report noted that maintaining the reliability and interconnectivity of the nation's telecommunications networks depended primarily on industry standards-setting processes to establish base standards and a minimum set of

requirements that define interoperability. These standards remained voluntary, with enforcement provisions largely left to agreements among private sector service and equipment providers.[63]

The central finding of the report was that new commercial technologies seeking to interconnect with the existing wireline network, would need to conform to the existing de facto industry standards, configuring all new network interconnections to the existing wireline architecture and network interfaces. Newer service providers and telecommunications equipment developers were strongly encouraged to participate in the relevant industry standards-setting process.[64]

To facilitate this standards-making process and, ultimately, reliable interconnectivities between the nation's telecommunication service providers, the Second Council developed a series of templates to govern joint planning sessions between interconnecting service providers. The Council also developed a Network Interface Specification Template for the development of network standards and specifications.[65]

Because the Council completed its work before the passage of the Telecommunications Act of 1996, the specific provisions of the Act were not reflected in the Second Council's final report. However, in summarizing its findings in the final report, the Council made the observation:

> When it comes to development, Information Technology today is in its infancy...if we've learned anything from the development of (new) technologies, it is that growth will be wild and chaotic and what ultimately happens will defy anyone's predictions.[66]

Third Network Reliability Council (NRC)

With the passage of the Telecommunications Act of 1996 on 8 February 1996, the FCC established a Third Network Reliability Council (NRC) in April 1996. The pro-competition, deregulatory, telecommunications policy framework, ushered in by the Telecommunications Act, had the unforeseen result of complicating National Emergency Services planning. The issue of "who's in charge" landed squarely in the lap of the Federal Communications Commission (FCC). Section 256 of the Telecommunications Act required that the FCC establish procedures to oversee coordinated network planning by telecommunications service providers and participate in the development of Public Network interconnectivity standards through telecommunications industry standards-setting bodies.[67]

Accordingly, the FCC revised the charter of the NRC to support its new, expanded mission. In the process, the FCC renamed the Council the *Network Reliability and Interoperability Council* (NRIC), in appreciation of its expanded charter and to more accurately reflect the scope of its responsibilities.

The FCC charter revisions, patterned after Section 256 of the Telecommunications Act, directed the NRIC to :

- Identify, and prepare recommendations to avoid, barriers to interconnectivity, interoperability and accessibility of public telecommunications networks; barriers to the use of

telecommunications devices with those networks, and recommendations to ensure seamless transmission between and across those networks;

- Provide recommendations on how the FCC might most efficiently conduct effective oversight of coordinated telecommunications network planning and design;
- Provide recommendations on how the FCC might most effectively participate in the development network interconnectivity standards through the appropriate industry standards-setting groups;
- Continue to report on the reliability of public telecommunications networks and services within the United States.[68]

To perform the analyses and develop the recommendations requested by the FCC, on 15 July 1996, the Council reorganized into two focus groups along lines suggested by Section 256 of the Telecommunications Act of 1996. Focus Group One, Network Connectivity and Planning Oversight was first asked to determine what technical, engineering, and legal barriers existed having an adverse impact on network accessibility and interconnectivity. Second, Focus Group One was asked to recommend procedures that the FCC should establish to oversee coordinated network planning.[69]

Focus Group Two was asked to review the telecommunications standards-setting process and to make recommendations on what role the FCC should take in participating in those activities. With these mission needs statements as guidance, the Third Council began its work in August 1996.[70]

President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet

For FY1996, funding for High-Performance Computing remained at the $1 billion mark. The High-Performance Computing, Communications, and Information Technology (HPCCIT) Subcommittee became the Computing, Information, and Communications (CIC) R&D Subcommittee of the CCIC. The CIC assumed responsibility for coordinating all twelve of the agencies' collaborative R&D activities under this program.

On 1 October 1996, the CCIC reorganized its collaborative programs into five Program Component Areas (PCAs). This structure was a natural evolution from the five research and development components of the original HPCC Program. The PCAs were organized around specific technology areas targeted for high priority investment by the Federal agencies participating in the coordinated R&D programs. Many of these technology applications spanned several PCAs and numerous areas of research would necessarily contribute to more than one PCA.

From 1991 through 1996, the emphasis in High-End Computing and Communications (HECC) had addressed advanced software technologies for high performance systems, focusing on software designed to operate with scalable clusters of shared memory processors. Beginning in 1996, emphasis in the HECC PCA became reusable software for high-performance systems.

The second PCA, Large-Scale Networking Technologies (LSN), served as the second principal focus area under HPCC . The goal of the LSN R&D effort was maintaining United States' leadership in communications in high-performance network components; technologies that enable wireless, optical, mobile, and wireline communications; large-scale network engineering, management, and services; and systems software and program development environments for network-centric computing. Prior to 1996, the LSN emphasis had been on very high bandwidth optical, wireline, and wireless communications, very large aggregates of very small processors, connectivity for large numbers of universities and schools, distributed cooperative computing, and medical applications using computer-based patient records.

The third PCA focus area, High-Confidence Systems (HCS), encompassed the government's directed research in technologies associated with computer and network security, protection of privacy and data, reliability, and restorability of information services following catastrophic events, such as SIW or cyberterror attacks. Within HCS, research would be focused on the high-performance aspects of system reliability, authentication and certification of data, and privacy and security of sensitive unclassified data.

Finally, Human Centered Systems (HuCS) and Education, Training, and Human Resources (ETHR) rounded out the other two, remaining PCAs under the reconstituted HPCC program.

Executive Order 13011: Federal Information Technology

In response to the Congressional ITMRA mandate, the Clinton Administration issued Executive Order 13011, Federal Information Technology, on 17 July 1996. EO 13011 charged the Office of Management and Budget (OMB) as the lead Executive Agency for implementing consistent Federal Information Technology approaches across the Executive Branch. EO 13011 directed Executive Branch departments and agencies to improve the management of their existing information systems and the acquisition of new information technology by implementing the relevant provisions of the Government Performance and Results Act of 1993 (Public Law 103-62), the Paperwork Reduction Act of 1995 (Public Law 104-13), and the Information Technology Management Reform Act of 1996 (Division E of Public Law 104-106).[71]

EO 13011 directed Executive Branch agencies to establish clear accountability for information resources management activities by tying mission-based performance measures to agency budgets. This aligned agency performance and reporting with the mandates of the Government Performance and Results Act of 1993 (Public Law 103-62). Agency heads were directed to implement formal process reviews tying agency budget formulations with best practices assessments, and mandating the restructuring of agencies to maximize in-house Information Technology efficiencies before new investments in Information Technology were made to support existing agency workloads.[72]

EO13011 created three new IT organizations within the Executive Branch. First, the role of Chief Information Officer was created for each Executive Branch Department and agency, along with a Chief Information Officers Council ("CIO Council"). The CIO Council serves as the principal interagency forum for improving agency practices in the design, modernization, use, sharing, and performance of agency information resources. The Deputy Director for Management of OMB chairs the CIO Council, composed of the CIOs and Deputy CIOs of the thirteen major Federal Executive Departments. The Vice Chair is elected from the ranks of the CIO Council on a rotational basis.[73]

The second IT organization created by EO 13011 was the Government Information Technology Services ("Services Board"). The Services Board was established to ensure continued implementation of the information technology recommendations of the National Performance Review and to identify and promote the development of innovative technologies and practices among the Federal agencies, State and local governments, and the private sector.[74]

The third organization created out of EO 13011 was the Information Technology Resources Board ("Resource Board"). The Resource Board was established to provide independent assessments to assist in the development, acquisition, and management of selected major agency information systems.[75]

In a recurrent theme consistent with all Clinton Administration directives and orders having Information Technology content, Section 1 (d) of Executive Order 13011 directed the Executive Departments and agencies to:

> Cooperate in the use of Information Technology to improve the productivity of Federal programs and to promote a coordinated, interoperable, secure, and shared government-wide infrastructure that is provided and supported by a diversity of private sector suppliers and a well-trained corps of Information Technology professionals.[76]

And in Section 2 (b) (3), to:

> Establish mission-based performance measures for information systems investments aligned with agency plans prepared pursuant to the Government Performance and Results Act of 1993.[77]

To more effectively implement the new controls and directions mandated by EO 13011 and PL 104-106, OMB director Franklin D. Raines, immediately implemented a mandatory checklist for validating the business case rationale for each new Information Technology project, on a case by case basis. Under "Raines Rules," Information Technology investments were first certified by agency CIOs as critical to the core mission of the agency. Second, agencies had to justify the legitimacy of their organization's performing the function in-house. Finally, each agency had to substantiate how the efficiency of the agency's business processes could only be improved through additional Information Technology investment.[78]

Although signed into law in February 1996, the provisions of the PL104-106 did not take full effect until August 1996, too late to have an

impact on the 1998 budget cycle. However, in order to meet planning dates associated with the FY1999 budget cycle, all Federal agencies were required to have Information Technology strategic plans in place no later than 15 July 1999, and to update them formally by 15 July for each subsequent fiscal planning year.[79]

Clinton Administration Next Generation Internet Initiative

On 10 October 1996, President Clinton announced a major new initiative to fund necessary Information Technology research and development and begin initial development of the nation's Next Generation Internet (NGI). In his policy address announcing the initiative, President Clinton said:

> The Internet is the biggest change in human communications since the invention of the printing press. We must invest today to create the foundation for the networks of the 21st Century. Today's Internet is an outgrowth of decades of Federal investment in research networks such as the ARPANET and the NSFNET. A small amount of Federal seed money stimulated much greater investment by industry and academia, and helped create a large and growing market. The Global Information Infrastructure, still in the early stages of development, is already changing the world by linking disparate populations and cultures as part of a global electronic community. No single force embodies this electronic transformation more than the evolving medium known as the Internet. [80]
>
> Once a tool reserved for science and academic exchange, the Internet is emerging as a requisite tool of society, much as did the telephone, radio, and television before it. The Internet is being used to reshape the global community. As the Internet empowers more and more individuals and organizations, it is also changing the basic foundations of business and government. E-commerce business arenas, including computer

> software, entertainment products, information services, financial services, and other professional services, now account for over $40B in U.S. exports annually.[81]
>
> As an increasing share of business transactions occur on-line, the GII has the potential of lowering costs dramatically in the commercial marketplace, by significantly reducing the traditional overhead associated with doing retail business. Consumers are able to shop directly from their homes, tapping into a world-wide market of products and services, visualization tools (i.e., building an on-line model of how a room of new furniture might look), and financial options, all from the comfort of their homes.[82]

In making this announcement, President Clinton reinforced two basic tenets and consistent themes of his Presidency. First, the potential loss of individual privacy and informational security, as society grows more dependent on electronic commerce and the NII, compels government and private industry to join forces in a consortium to develop tools necessary to preserve Information Assurance on the Internet and for its users. Second, the private sector must play the essential lead role to define and evolve the Next Generation Internet.

> With this freedom of choice and flexibility come a danger that as society becomes more and more dependent on electronic means to perform the daily functions of life, that individual security could be compromised by still evolving issues involving the misappropriation of privacy and credit information, the enforcement of electronic contracts, government regulation, and the issue of personal liability.
>
> Government can have a profound effect on the growth of electronic commerce. By their actions, government can either facilitate or severely inhibit electronic trade through regulation and taxation. Though government played a key role in financing the initial development of the Internet, its explosive expansion has been entirely due to its commercialization by the private sector. For electronic commerce to flourish, the private sector

> must continue to lead in its evolution within a non-government regulated, market-driven arena. Where self-regulation is not sufficient (e.g., such as international trade agreements, intellectual property, taxation, etc.), government policy and intervention be driven principally by private sector interests.[83]

President Clinton identified three, near-term Administration goals for the Next Generation Internet initiative. First, to interconnect universities and national laboratories with high-speed networks 100-1,000 times faster than the current Internet. Second, to promote experimentation with the next generation of networking technologies. And third, to demonstrate new applications that meet "important national goals and missions."[84]

Included in this applications focus was a "top priority" for the Defense Department, that of acquiring a "dominant battlefield awareness" capability:

> This will give the United States military a significant advantage in any armed conflict. This requires an ability to collect information from large numbers of high-resolution sensors, automatic processing of the data to support terrain and target recognition, and real-time distribution of that data to the warfighter. This will require orders of magnitude more bandwidth than is currently commercially available.[85]

To fund this initiative, the Clinton Administration announced it would add $100 million annually to the Federal R&D budget, beginning in FY1998. While keeping with its policy that the "information superhighway" should be built, owned, and operated by the private sector, the Clinton Administration again reinforced the appropriateness of Federal R&D underwriting basic research initiatives which would be cost-prohibitive for any private sector company to address single-handedly.[86]

CONGRESS--1996

Public Law 104-104: The Telecommunications Act of 1996

The Telecommunications Act of 1996, enacted in February of 1996, fundamentally revised the Communications Act of 1934, changing United States telecommunications regulation.[87] Included among the many changes was the addition of new Section 256, entitled "Coordination for Interconnection."[88]

The general purposes of the Act was to foster innovation, competition and deregulation in telecommunications. Section 256 required the Federal Communications Commission (FCC) to establish procedures to oversee coordinated network planning by telecommunications carriers and other providers of telecommunications services, and permitted the FCC to participate in the development of public network interconnectivity standards by appropriate industry standards-setting bodies.[89]

The purposes of Section 256, as stated in the statute, were: first, to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks; and second, to ensure the ability of users and information providers to "seamlessly and transparently transmit and receive information between and across telecommunications networks."[90]

In April of 1996 the FCC revised the charter of its Federal Advisory Committee, the Network Reliability Council, to include responsibility for

advising the FCC on how it might best accomplish the responsibilities placed on it by Section 256. To reflect this mission, the Commission changed the name of the Council to "The Network Reliability and Interoperability Council."[91]

Prior to the passage of the Telecommunications Act of 1996 (Telecommunications Act), the de-facto planning and provision of "National Services" was provided by AT&T (pre-divestiture) and by the Regional Bell Operating Companies (post-divestiture).[92] National Services are those telecommunication services deployed on a national or widespread basis through the public networks. These services include toll free (800/888) calling, local number portability, dial tone, and emergency 911 service. The deregulation of the telephone industry by the Telecommunications Act changed all that. In response, the FCC and the NRC became the mechanisms through which the National Services planning void created by the breakup of AT&T would be addressed.[93]

Public Law 104-106: Information Technology Management Reform Act of 1996

On 10 February 1996, President Clinton signed into law the Information Technology Management Reform Act of 1996 (ITMRA). The enactment of ITMRA, also known as the Clinger-Cohen Act, repealed Section 111 of the Federal Property and Administrative Services Act of 1949 (popularly known as the "Brooks Act"). ITMRA also amended Section 3506, of the Paperwork Reduction Act (PRA), by establishing the position of

agency Chief Information Officer, replacing the role of, "designated senior official for information resources management," identified in the PRA.[94]

This provision of ITMRA established a new statutory direction for the management and acquisition of Information Technology within the Executive Branch. This provision was intended to establish clear accountability for agency information resources management activities, provide for greater coordination among the agencies' information activities, and to ensure greater visibility of such activities within each agency.[95] ITMRA would require the Executive Branch to tie technology investments directly to specific operating goals it would assume and be measured against in exchange for Congressional funding support.[96]

A key responsibility of the agency CIOs under ITMRA was to promote effective agency operations by implementing budget-linked capital planning for, and performance-based budgeting of, agency information technology systems. Under ITMRA, agencies would first determine whether agency information system functions could be out-sourced to other agencies or to the private sector before the affected agency could request capital for the purchase of new, organic, data processing capabilities. Agencies were directed to exhaust all internal efforts to reorganize and revise their standard operating procedures and to improve internal effectiveness before making significant Information technology (IT) investments to support that work. The Act made agency CIOs explicitly responsible for promoting improvements in agency work processes.[97]

Under ITMRA, agency CIOs were charged with enabling the development and implementation of a sound and integrated information technology approach for their respective agencies and promoting the effective operation of all major information resources and management processes.[98] It should be noted that Congress enacted the Clinger-Cohen Act in response to a lack of confidence in the General Services Administration's ability to successfully manage Information Technology projects for the Federal Government. As a result of a series of costly Information Technology project failures, Congress used ITMRA to strip control of Federal information processing systems from the GSA and turn it over to the Office of Management and Budget (OMB).[99]

CLINTON ADMINISTRATION--1997

Executive Order 13035: President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet

Beginning with the 1997 fiscal year, the President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet directed that research should be focused on state-of-the-art Information Technologies based on quantum effects and biological phenomena. There was less emphasis by the Committee than in previous years on the procurement of large-scale experimental systems, although re-competition of the NSF

Supercomputer Centers and the DOE High-Performance Computing Research Centers were conducted in 1997.

On 12 February 1997, the President announced the appointment of Ken Kennedy as Co-Chairman of the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet.[100] This announcement was followed on 21 February 1997, when the President announced the appointment of Bill Joy as Co-Chairman of the Advisory Committee. On 31 October 1997, the President announced his intention to appoint David W. Dorman, Joseph F. Thompson, Irving Wladawsky-Berger, and John P. Miller as members of the Advisory Committee.

The newly reconstituted Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet held its initial kick-off meeting in February 1997. The Committee's announced first task was to provide guidance for the Next Generation Internet Initiative announced by the President in October 1996.[101]

A Framework for Electronic Commerce

On 1 July 1997, President Clinton issued a Presidential Directive accompanying the release of "A Framework for Global Electronic Commerce," the Administration's vision statement and blueprint for the future of electronic commerce and the Internet. In his Presidential Directive, President Clinton articulated five guiding principles for the Framework:

- For electronic commerce to flourish, the private sector must lead. Therefore the Federal Government should encourage industry self-regulation whenever appropriate and support private sector efforts to develop technology and practices that facilitate the growth and success of the Internet;

- Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. Therefore, the Federal Government should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place on the Internet;

- In some areas, government involvement may prove necessary to facilitate electronic commerce and protect consumers. Where governmental involvement is necessary, its aim should be to support and enforce a predictable, consistent, and simple legal environment for commerce;

- The Federal Government should recognize the unique qualities of the Internet including its decentralized nature and its tradition of bottom-up governance. Existing laws and regulations that may hinder electronic commerce should be revised or eliminated consistent with the unique nature of the Internet;

- The Internet is emerging as a global marketplace. The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across State, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides.[102]

This Framework for Global Electronic Commerce became an important element of the Clinton Administration's agenda on trade and technology. The Framework was solidly grounded in the Clinton vision of the Global Information Infrastructure (GII) as both the catalyst for and structural foundation of business and government transactions in the 21st Century. Key to the realization of this future utility was the

Clinton Administration's belief that all parties would gain the most from a non-regulated, market-oriented approach to electronic commerce:

> Today, I have approved and released a report--"A Framework for Global Electronic Commerce"--outlining the principles that will guide my Administration's actions as we move forward into the new electronic age of commerce. This report articulates my Administration's vision for presenting a series of policies, and establishing an agenda for international discussions and agreements to facilitate the growth of electronic commerce. I expect all executive departments and agencies to review carefully the principles in this framework and implement policies.[103]

Third Network Reliability and Interoperability Council (NRIC)

The Third Network and Interoperability Reliability Council's final report entitled, "NRIC Network Interoperability: The Key to Competitiveness," was completed and presented to the Federal Communications Commission on 15 July 1997.[104]

In its final report, the Third Council expressed its conviction that the objectives of Section 256 of the Telecommunications Act of 1996--accessibility, transparency, and seamless interoperability--must be pursued in context with the other objectives of the Act, including fostering innovation, competition, and the deregulation of the telecommunications business. The report concluded by asserting that competitive market forces, voluntary standards processes, and agreements between the private sector service and equipment providers, should be relied upon as the primary vehicles by which the objectives of Section 256 would be accomplished.[105]

Executive Order 13062: Continuance of Certain Federal Advisory Committees and Amendments to Executive Orders 13039 and 13054

Pursuant to provisions of the Federal Advisory Committee Act, on 29 September 1997, President William Clinton issued Executive Order 13062, continuing Executive Order 12882, as amended, and extending the termination date for the President's Committee of Advisors on Science and Technology (PCAST) until 30 September 1999.[106]

In this same order, President Clinton revoked EO 12864, as amended by Executive Orders 12890, 12921, and 12970. EO 12864 had established the United States Advisory Committee on the National Information Infrastructure (NII). In his statement accompanying the release of EO 12864, President Clinton declared that the work of the Committee was now "completed."[107]

CLINTON ADMINISTRATION--1998

President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet

In a letter to the President dated 3 June 1998, the President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet urged that public investments in computer, communications, and other Information Technology research be significantly expanded to ensure an ever-increasing standard of living and quality of life for Americans.[108] President Clinton, responding

during a commencement address at the Massachusetts Institute of Technology on 5 June 1998, underscored his personal commitment to a strong Federal Information Technology research and development program, stating:

> In just the past four years, Information Technology has been responsible for more than a third of our economic expansion. Without government-funded research, computers, the Internet, communications satellites wouldn't have gotten started. In the budget I submit to Congress for the year 2000, I will call for significant increases in computing and communications research. I have directed Dr. Neal Lane, my new Advisor for Science and Technology, to work with our nation's research community to prepare a detailed plan for my review.[109]

On 24 July, President Clinton announced the appointment of Dr. Robert Elliot Kahn, President, CEO, and Chairman of the Corporation for National Research (CNRI) of McLean, VA, which Kahn had founded in 1986, to serve as a member of the Committee. The President's appointment continued a policy of maintaining an Information Technology research and development focus to the Committee.[110]

Executive Order 13092: President's Information Technology Advisory Committee (Amendments to Executive Order 13035)

On 24 July 1998, President Clinton issued Executive Order 13092, adding five additional members to the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet and changing the name of the Committee to the President's Information Technology Advisory Committee (PITAC). The total number of non-Federal committee members increased from 25 to 30.

On 10 August 1998, the newly renamed PITAC followed up its letter of 3 June 1998 to President Clinton with an interim report on its findings and recommendations regarding, "the importance of social and economic research on the impacts of Information Technology to inform key policy decisions."[111]

The draft report called for increased Federal support for research and development as being, "critical to meeting the challenge of capturing the opportunities available from Information Technology in the 21st Century."[112] The Committee committed to delivering a final report to the President by February 1999.

Fourth Network Reliability and Interoperability Council (NRIC)

On 30 July 1998, the FCC announced the appointment of AT&T CEO Michael Armstrong as Chairman of a re-chartered Fourth Network Reliability and Interoperability Council (NRIC). Under its amended charter, the Council's focus was made exclusive to Year 2000 (Y2K) conversion activities.

CONGRESS--1998

S.1609: Next Generation Internet Research Act of 1998

On 4 February 1998, Senator William Frist (R-AZ) introduced S.1609, the Next Generation Internet Research Act of 1998. The bill to amend the High-Performance Computing Act of 1991 would authorize appropriations for fiscal years 1999 and 2000 for the Next Generation Internet program. The bill would provide for the development and coordination of a comprehensive and

integrated research and development program on computer network infrastructure, high-speed data access, and networking technology.[113]

The bill would require the Secretary of Commerce to direct the National Research Council of the National Academy of Sciences to conduct a comprehensive study of the diverse needs of Next Generation Internet users. The proposed legislation would also require the Advisory Committee on High-Performance Computing and Communications, Information technology, and the Next Generation Internet, now PITAC by virtue of EO 13092, to monitor and provide technical advice to the President concerning the development and implementation of the Next Generation Internet program. This would include a formal reporting to the President and the Congress annually on the extent that progress was being made toward achieving the program's goals.[114]

After its second reading on the floor of the Senate, the proposed legislation was referred to the Committee on Commerce, where it was reviewed and then ordered reported out of Committee, without amendment on 12 March 1998. On 2 April 1998, Senator John McCain (R-AZ), Commerce Committee Chair, reported the bill, without amendment, to the full Senate under written report No. 105-173. Subsequently, the bill was placed on the Senate Legislative Calendar under General Orders (Calendar No. 334).[115]

On 26 June 1998, the measure was twice amended, the first, S.AMDT.3054 by Senator Frist (R-TN), and the second, S.ADMT.3055, by

Senator Leahey (D-VT). S.AMDT.3054 added $5 million to the annual authorizations in FY 1999 and 2000 for the implementation of the bill. S.AMDT.3055 directed that a study be conducted by the National Academy of Science concerning the short- and long-term effects on trademark and intellectual property rights created by the generation of a new class of Internet address domains. The amendment also directed that the study establish Internet-based intellectual property-related dispute resolution procedures.[116]

On 26 June 1998, the bill, as amended, passed the Senate by unanimous consent. On 14 July 1998, the bill was forwarded to the full House and on 21 October, to the House Committee on Science. The House Committee on Science referred the bill to its Subcommittee on Basic Research for review. As a result of that review, the Committee chose to take no further action on the bill.[117]

Public Law 105-305: Next Generation Internet Research Act of 1998 [15 U.S.C. 5513(d)]

Shortly after its introduction in the Senate, Congressman James Sensenbrenner (R-WI) offered a House version of S.1609 in H.R.3332, the Next Generation Internet Research Act of 1998. Introduced on 4 March 1998, H.R.3332 amended the High-Performance Computing Act of 1991 by authorizing appropriations for FYs1999 and 2000 for the Next Generation Internet program. It also required the Advisory Committee on High-Performance Computing and Communications, Information Technology, and

the Next Generation Internet to proffer technical advice for the NGI and to report program status annually to the Congress and to the President.[118]

The bill authorized the National Science Foundation, Department of Energy, National Institutes of Health, National Aeronautics and Space Administration, and the National Institute of Standards and Technology to work with America's private sector to develop a new generation of Internet having superior speed, reliability, bandwidth, and security than that available through the current Internet. The bill also authorized the development of an advanced testbed network that would link key Federal laboratories with university research centers around the country. [119]

Following its introduction to the House, H.R. 3332 was referred to the House Committee on Science, where it successfully passed a mark-up session on 13 March 1998. The bill was then ordered reported out of Committee by voice vote on 13 May 1998. Enjoying bipartisan support in the House, the Rules were suspended for H.R. 3332, allowing it to be ordered up before the full House for a voice vote, which it passed easily on 14 September 1998.[120]

On 15 September 1998, the bill was received in the Senate and read twice before being referred to the Senate Committee on Commerce. Enjoying bipartisan support equal in strength in the Senate as it enjoyed in the House, H.R. 3332 was discharged on 8 October 1998 by the Commerce Committee by unanimous consent, and ordered up before the full Senate, where it was passed by unanimous consent and without amendment.[121]

The bill was cleared for the White House on 8 October and was presented to President Clinton on 20 October 1998. The President signed the bill into law (PL 105-305) on 29 October 1998.[122]

Public Law 105-277: Government Paperwork Elimination Act

The Government Paperwork Elimination Act (GPEA), which took effect on 21 October 1998, is an important tool in fulfilling the Clinton Administration vision of improved customer service and government efficiency through the use of Information Technology. This vision, articulated in Vice President Albert Gore's 1997 report, "Access America," involves the widespread use of the Internet by Federal agencies transacting business electronically, i.e., data, electronic forms, and electronic signatures, in the same manner as e-commerce based, commercial enterprises. Delivery of on-line government products and services would nominally save the government tens of millions of dollars in direct costs and an equivalent value in time savings.[123]

GPEA's success as a cornerstone to electronic government would depend on the public's confidence in the security of the Federal Government's electronic information exchange. To be successful, it would be essential for the government to demonstrate that its information infrastructure would remain secure at all times and under any threat scenario. The Office of Management and Budget, in consultation with the Commerce Department, accepted the Executive charter from President Clinton to establish the requisite procedures and standards for agencies to implement GPEA.[124]

CLINTON ADMINISTRATION--1999

Executive Order 13113: President's Information Technology Advisory Committee

On 11 February 1999, President Clinton issued Executive Order 13113, extending the life of the President's Information Technology Advisory Committee (PITAC) and expanding PITAC support functions so that it could carry out the additional responsibilities given to it by the Next Generation Internet Research Act of 1998 (PL 105-305). Under the provisions of this Executive Order, the commission for PITAC was extended until 11 February 2001.[125]

On 24 February 1999, PITAC delivered its final report to President Clinton under the auspices of its original charter and Executive Order 13035. The report entitled, "Information Technology Research: Investing In Our Future," proposed a comprehensive agenda for ensuring America's leadership in the Information Age through the expansion of government investment in long-term, Information Technology R&D.

In articulating the case for major increases in Federal telecommunications and computing R&D investments, PITAC cited the critical role played by the Federal Government in developing the Internet, high-end computing, and other Information Age-enabling technologies. PITAC also stressed the importance of conducting social and economic research on the impacts of information technology on key government policy decisions.[126]

PITAC's recommendation to double the Federal IT R&D budget over a period of five years was used as the basis for the Clinton Administration's FY2000 budget initiative known as IT^{21}, or Information Technology for the Twenty-First Century. The recommendation also spurred complementary congressional proposals for increased Federal IT R&D, including the Networking and Information Technology Research and Development (NITRD) Act.[127]

In support of this R&D initiative, PITAC co-chair Kenneth Kennedy testified before the House Committee on Science, Subcommittee on Basic Research, on 16 March 1999. On 29 June 1999, PITAC offered its strongest endorsement of the NITRD draft legislation in a letter to its sponsor, Congressman James Sensenbrenner. In a follow-up letter to the Congress on 1 September 1999, PITAC expressed its concerns over proposed Information Technology R&D budget cuts, lobbying Congress to, "ensure full funding for proposed increases in information technology IR&D."[128]

In accordance with the Next Generation Internet Research Act of 1998, PITAC conducted a formal review of the NGI program, delivering its findings and recommendations to the President and the Congress on 28 August 1999. In its report, PITAC recommended continuing NGI funding at the proposed levels for basic research activities and for NGI follow-on activities as part of the Administration's IT^{21} initiative. In preparation of its scheduled April 2000, FY2000 review of the NGI program and report to the

Congress, PITAC met with all six NGI agencies to discuss progress and status during October 1999.

Concurrent with its review of the NGI program and at the request of President Clinton, PITAC reviewed the Administration's IT^{21} initiative. In their report to the President on 8 September 1999, PITAC found that the research agenda and agency plans for implementing the IT^{21} initiative were consistent with PITAC's February report and recommendations.[129]

Information Technology for the Twenty-First Century Initiative (IT^{21})

The Information Technology for the Twenty-First Century, or IT^{21}, had its roots in June 1998, during President Clinton's commencement address at MIT. During that address, President Clinton asked his Assistant for Science and Technology, Dr. Neal Lane, to prepare a comprehensive plan for Federal communications and computer research for the new century. Supported by an NSTC interagency working group and drawing heavily on PITAC's interim report of August 1998, a new $366 million, multi-agency initiative known as Information Technology for the Twenty-First Century, or IT^{21} was developed. Vice President Gore unveiled the new initiative in January 1999.

The first publication, outlining the objectives of the new initiative, "Information Technology for the Twenty-First Century: A Bold Investment in America's Future," was published on 24 January 1999 in draft form. On 19 May 1999, advanced Information Technology demonstrations were

presented by the proposed IT[21] participating agencies--DARPA, DOE, NASA, NIST, NOAA, and NSF--to members of Congress and their staffs.[130]

Throughout the remainder of FY 1999, the IT[21] Working Group worked closely with the Subcommittee on Computing, Information and Communications (CIC) R&D to evolve an IT[21] implementation plan and to build Congressional support. In November 1999, the IT[21] Working Group and the Subcommittee on Computing, Information and Communications (CIC) merged to form a separate Interagency Working Group (IWG) for Information Technology Research and Development. The new IWG/ITR&D, reporting directly to the Assistant to the President for Science and Technology and a special group of NSTC agency principals, focused the balance of their CY1999 efforts on meeting its programmatic objectives, while continuing to build Congressional support for increased Federal funding for interagency Information Technology R&D.[131]

Office of Science and Technology Policy: FY2001 Interagency Research and Development Priorities

At the behest of President Clinton, on 3 June 1999, Directors Neal Lane and Jacob Lew of the White House Office of Science and Technology Policy, issued a policy memorandum articulating Clinton Administration interagency R&D priorities for FY2001. Three underlying Clinton Administration science and technology policy themes overarched this policy document.

First, the policy memorandum reiterated the four basic principles of the Clinton Administration science and technology investment strategy: first, sustain and nurture America's world-leading science and technology enterprise through pursuit of specific agency missions and through stewardship of critical R&D; second, strengthen science, math, and engineering education and opportunities for the next generation of American engineers and scientists; third, focus on activities requiring a Federal presence to attain national goals; and fourth, promote international cooperation in science and technology that would strengthen the advancement of science and achievement of Administration priorities.[132]

Second, it reinforced the Administration's practice of identifying specific investment opportunities to be shared across government agencies, each requiring significant levels of interagency coordination among such high-priority Federal investments in science and technology that transcend organizational boundaries. This memorandum directed all Federal Departments and agencies involved in this particular set of National Science and Technology Council (NSTC)-sponsored activities to participate in cross-agency working groups, integrating development and planning of these programs, including full budget disclosure and negotiations, through the NTSC.[133]

For FY2001, two of the eleven priority initiatives involved Information Technology, including the top priority, Information Technology R&D. Protecting Against 21st Century Threats, which focused on the promotion and

coordination of agency research to reduce vulnerabilities in the nation's critical infrastructure, was the Number Five priority identified.[134]

Third, the policy memorandum described the R&D performance measures and accountability standards Clinton Administration Departments and agencies would be expected to comport to. Two, formal, interagency crosscuts, Information Technology R&D and the United States Global Change Research Program (USGCRP), were targeted to promote more uniform management and accounting practices across the Executive Branch. Agency activities contributing to the crosscuts were clearly tied to the overall crosscut goals and performance measures. These goals and performance measures were then internally allocated as measurable agency goals.[135]

Executive Order 13038: Continuance of Certain Federal Advisory Committees

Under the provisions of the Federal Advisory Committee Act, on 30 September 1999, President Clinton issued Executive Order 13038, which continued the President's Committee of Advisors on Science and Technology established by Executive Order 12882, Office of Science and Technology Policy, until 30 September 2001.[136]

Next Generation Internet (NGI) Initiative

By October 1999, the multi-agency, Next Generation Internet (NGI) initiative, a key component to the Clinton Administration's Information Technology program, had prototyped several advanced network technologies

and network applications on testbeds 100 to 1,000 times faster than the current Internet.[137]

CONGRESS--1999

H.R. 2086: Networking and Information Technology Research and Development Act

On 9 June 1999, Congressman James Sensenbrenner (R-WI) introduced H.R. 2086, the Networking and Information Technology Research and Development Act, a bill authorizing funding for information technology research and development for fiscal years 2000 through 2004. The Act would authorize the funding by amending Section 201 (b) of the High-Performance Computing Act of 1991 [15 U.S.C. 5521 (b)].[138]

The total amount of monies allocated for NGI R&D by H.R. 2086 between FY2000 and FY2004 totaled $4.6 billion (see Table 5-1, below).

Agency (figures in $M)	**FY 2000**	**FY 2001**	**FY 2002**	**FY 2003**	**FY 2004**	**Totals**
National Science Foundation	$439.0	$468.6	$493.2	$544.1	$571.3	$2516
NASA	$164.4	$201.0	$208,0	$224.0	$231.0	$1400
Department of Energy	$106.6	$103.5	$107.0	$125.7	$129.4	$ 572
National Institute of Standards and Technology	$ 9.0	$ 9.5	$ 10.5	$ 16.0	$ 17.0	$ 62
National Oceanic and Atmospheric Administration	$ 13.5	$ 13.9	$ 14.3	$ 14.8	$ 15.2	$ 72
Environmental Protection Agency	$ 4,2	$ 4.3	$ 4.5	$ 4.6	$ 4.7	$ 22

Table 5-1: Proposed Funding for the Networking and Information Technology Research and Development Act[139]

After being read twice to the full House, the bill was referred concurrently, on 9 June 1999, to the House Committees on Science and on Ways and Means. On 9 September 1999, the bill was reported out favorably by the Committee on Science, by the unanimous vote of 41-0. Congressman Curt Weldon of Pennsylvania offered this summation in support of the bill:

> Mr. Speaker, we are in the middle of a revolution right now in America, only the second revolution in the history of our country. The first was when America transitioned from an agrarian society to an industrial society. Many of our colleagues and citizens did not want to make that change, but we had no choice because the economy of the world was going to be driven by that nation that could lead the industrial age. We rose to the occasion and we were successful.
>
> The revolution we are going through today is an information revolution. We are changing from an industrial society to an information society. Therefore, we have to change. If we are going to lead the world's economy, we have to lead the information revolution. Therefore, it presents to us a challenge, a challenge to have the best educated, the best equipped, and the best technology available to make sure we are leading the information revolution.[140]

On 16 November 1999, the Committee on Ways and Means requested and was granted an extension for further consideration of the bill to end no later than 29 February 2000.[141]

CLINTON ADMINISTRATION--2000

Office of Science Technology Policy

President Clinton's FY2001 budget request would provide $2.268 billion in Information Technology research and development, a $605 million increase over the FY2000 appropriation approved by Congress and $1 billion

increase over the same figure for FY1999. Table 5-2 depicts the proposed budget allocations by specific Administrative Department and agency, subject to Congressional approval and authorization.

Agency	FY 2000	FY 2001	% Increase
Department of Energy	$ 517,000,000	$ 667,000,000	22%
NASA	$ 158,000,000	$ 233,000,000	32%
HHS/National Institutes of Heath/ Agency for Healthcare Research and Quality	$ 191,000,000	$ 233,000,000	22%
DOC/National Institute of Standards and Technology	$ 36,000,000	$ 44,000,000	22%
National Science Foundation	$ 131,000,000	$ 230,000,000	43%
DOD/National Security Agency	$ 224,000,000	$ 350,000,000	56%
Environmental Protection Agency	$ 4,000,000	$ 4,000,000	0%
Totals:	$1,663,000,000	$2,268,000,000	36%

Table 5-2: Proposed FY2001 IT R&D Funding by the Clinton Administration[142]

In staking a claim to its FY2001 budget request, OSTP, offered the following statistics:

> During the past seven years, computers, high-speed communications systems, and computer software have become more powerful and more useful to people at home and work. Nearly half of all American households now use the Internet, with more than 700 new households being connected every

> hour. More than half of United States classrooms are connected to the Internet today, compared to less than three percent in 1993. IT allows Americans to shop, do homework, and get healthcare advice on-line, and it has enabled businesses of all sizes to join the international economy. Since 1995, more than a third of all United States economic growth has resulted from IT enterprises. Today, more than 13 million Americans hold IT-related jobs, which are being added six times faster than the rate of overall job growth.[143]

Fifth Network Reliability and Interoperability Council (NRIC)

On 6 March 2000, the FCC announced the appointment of *Level 3 Communications* CEO James Q. Crowe as Chairman of a rechartered Fifth Network Reliability and Interoperability Council (NRC). The announced goal of the Fifth Council was to "assure optimal reliability, interoperability and interconnectivity of, and accessibility to, the public telecommunications networks."[144] The new Council's first meeting was held on 20 March 2000 at the FCC offices in Washington, D.C.

CONGRESS--2000

S. 2046: Next Generation Internet 2000 Act

On 2 February 2000, Sen. William Frist (R-TN) introduced S.2046, a bill to reauthorize and continue the funding for the Next Generation Internet project. Entitled the Next Generation Internet 2000 Act, the proposed bill would support a multi-agency research and development program geared toward advancing networking infrastructure and technologies in line with the NGI vision.

Although the bill would continue the research and development funding for the NGI, it would also amend Section 103 of the High-Performance Computing Act of 1991 (15 U.S.C. 5513) to include a 10% set-aside for research into reducing the cost of Internet services in rural areas. It also amends the previous Act by adding a 5% set-aside for Internet support to minority institutions of higher learning.[145]

In formal remarks accompanying the introduction of the bill to the Senate floor, Senator Frist explained how this bill would be different than its predecessor:

> Mr. President, I rise today to introduce the Next Generation Internet 2000 Act, a multi-agency research and development program designed to fund advanced networking infrastructure and technologies. Two and a half years ago, I stood in this exact spot and introduced its predecessor, the Next Generation Internet Research Act of 1998. While scientists throughout the country have made tremendous in-roads since that time, the digital divide makes the truth clear and simple: we are leaving many of our fellow Americans behind. The Next Generation Internet 2000 will attempt to eliminate these geographical barriers, while providing research funding for a faster, more secure and robust network infrastructure for all Americans.[146]

The proposed bill would fund the Next Generation Internet 2000 program for an additional three years. Table 5-3 provides a breakout of the recommended funding levels for each Executive Branch department and agency by fiscal year.

Agency	FY 2000	FY 2001	FY 2002
Department of Energy	$ 32,000,000	$ 33,800,000	$ 35,700,000
NASA	$ 19,500,000	$ 20,600,000	$ 21,700,000
National Institutes of Heath	$ 96,000,000	$101,300,000	$106,300,000
National Institute of Standards and Technology	$ 4,200,000	$ 4,400,000	$ 4,600,000
National Science Foundation	$111,200,000	$117,300,000	$123,800,000
National Security Agency	$ 1,900,000	$ 2,000,000	$ 2,100,000
Agency for Healthcare Research and Quality	$ 7,400,000	$ 7,800,000	$ 8,200,000

Table 5-3: Proposed Funding under Next Generation Internet 2000 Act[147]

On 8 March 2000, the Senate Subcommittee on Science, Technology and Space of the Committee on Commerce, Science, and Transportation held hearings on the merit of S. 2046. The keynote speaker for the Clinton Administration was Dr. Neal Lane, Assistant to the President for Science and Technology. In his testimony, Dr. Lane voiced the Clinton Administration's support of Congress in furthering the nation's Next Generation Internet objectives:

> Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to testify about the important research and development investments proposed by S. 2046, the Next Generation Internet (NGI) 2000 Act. These investments are a vital portion of the Administration's Information Technology (IT) research portfolio that strengthens and expands the important Federal networking research authorized thanks to your sponsorship, by the NGI Act of 1998.

> The Administration has been very encouraged by the active bipartisan support which both chambers of Congress have provided for efforts to strengthen our nation's investments in Information Technology research and development and we look forward to continued support for the exciting new work proposed in the Administration's proposed FY2001 budget. Here in the Senate, your leadership, Mr. Chairman and that of the members of the Subcommittee, has been especially instrumental in helping your colleagues recognize that the advances in Information Technology, which are so vital to the overall success of our nation's scientific and technical expertise, as well as to its economic prosperity, require a foundation of wise, sustained Federal research investments.[148]

Following the hearings on 8 March, the Subcommittee reported S. 2046 favorably out of committee on 13 April 2000, with one amendment, in the nature of a substitute.[149] The Committee on Commerce, Science, and Transportation inserted one amendment in the nature of a substitute to the bill, prepared a report (Senate Report No. 106-310), and announced its favorable findings to the Senate through its Chair, Senator John McCain (R-AZ), on 16 June 2000. On that same day, the Senate placed the bill on the Senate Legislative Calendar under General Orders Calendar No. 607, where it awaits final action.

H. Res. 422: Networking and Information Technology Research and Development Act

On 15 February 2000 and under the direction of the Speaker of the House, J. Dennis Hastert (R-IL), Representative "Doc" Hastings (R-WA) called before the Committee of the Whole House, House Resolution 422, a resolution for the consideration of H.R. 2086, the Networking and Information

Technology Research and Development Act. H.R. 2086, introduced by Representative James Sensenbrenner (R-WI) during the 1st Session of the 106th Congress, would authorize funding for networking and information technology research and development for fiscal years 2000 through 2004.[150]

Congressman Hastings, in presenting H.R. 2086 for immediate consideration by the House, stated:

> Mr. Speaker, the Networking and Information Technology Research and Development Act, H.R. 2086, amends the High-Performance Computing Act of 1991 to authorize funding for networking and information technology research and development programs of the National Science Foundation, National Aeronautics and Space Administration, the Department of Energy, the National Institute of Standards and Technology, the National Oceanic and Atmospheric Administration, and the Environmental Protection Agency for fiscal years 2000 through 2004. The bill was reported favorably by the Committee on Science by unanimous vote 41 to 0.
>
> Mr. Speaker, the Federal Government has an enormous task in maintaining its position as the global leader in the information-technology field. This bill serves to reiterate our commitment to this agenda by emphasizing basic research and information-technology funding levels. This research has played an essential role in fueling the information revolution, advancing national security, and bolstering the United States economy by creating new industries and millions of new jobs. Information-technology now represents one of the fastest growing sectors of our economy, growing at an annual rate of 12 percent between 1993 and 1997 and generating over $300 billion of U.S. revenue in 1998.
>
> In order to maintain the economic growth the United States is currently experiencing, we must maintain our role as a technological leader. Although the private sector provides the bulk of information technology research funding, the Federal Government has a responsibility to support long-term basic research to the private sector, but that is ill-suited to pursue. H.R. 2086 recognizes this by providing adequate funds for such activities.

> Specifically, over the next five years the bill would authorize $2.2 billion for the National Science Foundation, $602 million for the Department of Energy, $1.4 billion for NASA, $73 million for the National Institute of Standards and Technology, $71 million for the National Oceanic and Atmospheric Administration, and $22.3 million for EPA.
>
> Finally, the Congressional Budget Office estimates that appropriating the amounts authorized in H.R. 2086 would result in discretionary spending totaling over $3.7 billion over the five year period. The Committee on Rules was pleased to grant the request of the gentleman from Wisconsin, Chairman Sensenbrenner, for an open rule on H.R. 2086, and accordingly, I encourage my colleagues to support H. Res. 422 and the underlying bill. [151]

Concurrent with the consideration of H.R. 2086 by the full House, on 15 February 2000, President Clinton directed that the Office of Management and Budget (OMB) issue a Statement of Administration Policy in support of the bill, stating:

> The Administration supports several elements of H.R. 2086, but strongly urges that the bill be amended to conform to the authorizations level to those requested in the President's FY2001 Budget. The investment levels in the Budget will support the research needed to underpin advances in Information Technology that are critical to our Nation's current and future prosperity. The goals stated in H.R. 2086 can only be achieved by supporting the diverse research capabilities available in each participating agency.[152]

Following a one-hour general debate on the bill, the Committee of the Whole House entertained amendments to H.R. 2086, in the nature of substitutes to the original bill. A total of ten amendments were considered and approved by voice vote. The ten amendments approved were:

- H. AMDT.573 to H.R. 2086: an amendment, offered by Representative Ralph M. Hall (D-TX), increasing funding for the National Science Foundation, Department of Energy, and Networking and Information Technology Research and Development including an increase in the number of grants authorized;[153]
- H. AMDT.574 to H.R. 2086: an amendment, offered by Representative Nick Smith (R-MI), allowing the United States Geological Survey to participate in the Networking and Information Technology Research and Development Grant Program established by H.R. 2086;[154]
- H. AMDT.575 to H.R. 2086: an amendment, offered by Representative Constance A. Morella (R-MD), authorizing funding for the National Institutes of Health to conduct research directed toward computational techniques and software tools in support of biomedical and behavioral research;[155]
- H. AMDT.576 to H.R. 2086: an amendment, offered by Representative John B. Larson (D-CT), requiring the National science Foundation to study and report to Congress concerning the most effective and economical means of providing all public elementary and secondary schools and libraries with high-speed, large bandwidth capacity access to the Internet;[156]
- H. AMDT.577 to H.R. 2086: an amendment, offered by Representative Joseph M. Hoeffel (D-PA), requiring the National Research Council to

conduct a study on the accessibility to Information Technologies by the elderly and individuals with disabilities;[157]

- H. AMDT.578 to H.R. 2086: an amendment, offered by Representative Robert E. Andrews (D-NJ), granting priority to basic research that, among other issues, addresses security, including privacy and counterinitiatives, and consider the social and economic consequences, including healthcare, of Information Technology; [158]
- H. AMDT.579 to H.R. 2086: an amendment, offered by Representative Sheila Jackson-Lee (D-TX), requiring the Comptroller General to report to Congress analyzing the effects of this bill on lower income families, minorities, and women;[159]
- H. AMDT.580 to H.R. 2086: an amendment, offered by Representative Michael E. Capuano (D-MA), establishing a requirement for a report to Congress on the impact of Information Technology research funded by certain FY2000 appropriations bills;[160]
- H. AMDT.581 to H.R. 2086: an amendment, offered by Representative Michael E. Capuano (D-MA), increasing the funding authorized for the National Science Foundation for fiscal years 2000 through 2004 with offsets from the Department of Energy; and,[161]
- H. AMDT.582 to H.R. 2086: an amendment, offered by Representative James A. Traficant, Jr. (D-OH), expressing the, "sense of the Congress,"

that equipment and products purchased with funds made available under the bill should be American-made.[162]

The bill was approved, as amended, by voice vote on 15 February 2000. H.R. 2086 was received in the Senate on 22 February 2000, where it was read twice on the Senate floor before being referred to the Senate Committee on Commerce, Science, and Transportation chaired by Senator John McCain (R-AZ). Further action on the bill remains pending in Committee.[163]

SUMMARY

Throughout the years of the Clinton Administration, Information Technology was consistently accorded high-level attention as an essential construct of the Clinton Presidency. From Candidate Clinton's vision statements and campaign pledges during the 1991-1992 campaign, to a FY2001 budget request for over $2 billion in Information Technology R&D projects, President Clinton fulfilled his campaign promise to be the "high-tech President."

The Clinton Presidency operated under a set of consistent themes concerning Information Technology. The most overriding of these fundamental themes was that the Internet and its presumed progeny, the Information Superhighway and the National Information Infrastructure, are fundamentally private enterprises. Government's role, as validated by the

evolution of the Internet into the World Wide Web, is one of catalyst and enabler of innovation, but not architect and certainly not builder or banker.

A second Clinton theme was that Information Technology is the key to efficiency in government service provision. The underlying theme throughout the National Performance Review activity was that government cost reductions and improved service delivery are facilitated through the application of Information Technology.

A third theme was that regulation in the telecommunication industry should be limited to standards development and implementation, ensuring universal access, interoperability, and consistency of tools and services, irrespective of service location or user sophistication.

A fourth theme stressed by Clinton was that technology-based change occurs in gradual increments and at an evolutionary, not revolutionary, pace set by a "natural selection" process. The role of government, in such a change dynamic, is to facilitate change and to regulate the pace of change, as necessary; but only consistent with the adaptation of the change agents within the general population.

The case study findings from Chapter Five, Federal Information Technology Policy and Legislative Initiatives During the Clinton Administration (1993-2000), serve as the foundation for the case studies presented in the next two chapters, Chapter Six, Federal Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), and Chapter Seven, Critical Infrastructure Protection Policy Legislative Initiatives

During the Clinton Administration (1993-2000). In Chapter Eight, the PIES Model is applied to the results of the case studies from Chapters Five, Six and Seven, establishing a framework for the systematic analysis of the evolution of Clinton Administration Information Assurance policy between 1993-2000.

[1] Governor William Clinton, "The Economy," campaign speech presented to the Wharton School of Business, University of Pennsylvania, Philadelphia, PA. 16 April 1992.

[2] Clinton, William J., "Technology: The Engine of Economic Growth-A National technology Policy for American," campaign speech presented 18 September 1992, 1.

[3] Ibid., 3.

[4] Ibid., 5.

[5] The White House, Office of the Vice-President, *Reengineering Through Information Technology—Part 1*, Executive Summary. Accompanying Report of the National Performance Review, 1 September 1993.

[6] Ibid., Executive Summary.

[7] The White House, Office of the Vice-President, *Reengineering Through Information Technology--Part3*, Appendix B: Methodology. Accompanying Report of the National Performance Review, 1 September 1993.

[8] Ibid., Appendix B.

[9] David Osborne and Peter Plastrik, *Banishing Bureaucracy* (Reading, MA: Addison-Wesley Publishing Company, Inc., 1997), 39.

[10] Ibid., Executive Summary, 1.

[11] Congress, Senate, Senator Albert Gore, Jr. of Tennessee, "The High-Performance Computing Act of 1991," S.272, 102nd Congress, 1st sess. *Congressional Record* (24 January 1991): S1159.

[12] Statement of Dr. John H. Gibbon,s Director, Office of Science and Technology Policy before the Committee on Science, Space, and Technology U.S. House of Representatives, "Information Infrastructure and H.R.1757, the High Performance Computing and High Speed Networking Applications Act of 1993, 27 April 1993.

[13] Ibid., Gibbon's statement.

[14] Congress, Senate, Senator Albert Gore, Jr. of Tennessee, "Information Infrastructure and Technology Act of 1992," S.2937, 102nd Congress, 2nd sess. *Congressional Record* (1 July 1992), S7261.

[15] Ibid., S7261.

[16] Congress, House, Representative George E. Brown, Jr. of California, "Information Infrastructure and Technology Act of 1992," H.R.5759, 102d Congress, 2d sess. *Congressional Record* (4 August 1992), E2358.

[17] Ibid., E2358.

[18] Ibid. E2358.

[19] The White House, Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," Section III, 15 September 1993, 5.

[20] Executive Order 12864, 15 September 1993.

[21] Op. cit., Tab D (1), 27.

[22] Ibid., Tab D (2), 28.

[23] Ibid., Tab D (3), 28.

[24] The White House, Office of the Vice-President, *Reengineering Through Information Technology—Part1*, Executive Summary, endnotes. Accompanying Report of the National Performance Review, 1 September 1993.

[25] Executive Order 12864, Section 2. Functions (a),15 September 1993, 1.

[26] Ibid., Section 2. (b) (1-10).

[27] Ibid.,Section 2, 1.

[28] Ibid.,Section 2, 1.

[29] The White House, Office of the Press Secretary, "Strategic Planning Document–Information and Communications," 15 January 1994, 1.

[30] Executive Order 12881, Section 1 (23 November 1993),1.

[31] Ibid., 2.

[32] Executive Order 12882, Section 1 (23 November 1993), 1.

[33] Congress, House, Representative Rick Boucher of Virginia, National Information Infrastructure Act of 1993," H.R.1767, 103d Congress,1st sess. *Congressional Record* (21 April 1993), H5084-5094.

[34] Ibid., H5084.

[35] The White House, Office of Science and Technology Policy, "Statement of John H. Gibbons before the Committee on Science, Space, and Technology," United States House of Representatives (27 April 1993), 2-4.

[36] Ibid., H5089.

[37] Ibid., H5089.

[38] Op.cit., H5087-H5093.

[39] Ibid., H5092.

[40] Ibid., H5094.

[41] Ibid., S9540.

[42] Ronald H. Brown, Secretary of Commerce and Chair, IITF, "Putting the Information Infrastructure to Work," Gaithersburg, MD: National Institutes of Standards and Technology, 4 May 1994.

[43] Department of Commerce, Office of Public Relations, "Brown Releases report Highlighting Benefits, Barriers of National Information Highway," 4 May 1994, 1.

[44] Ibid., 1.

[45] Network Reliability and Interoperability Council, "Network Interoperability: The Key to Competitiveness," Final Report of the Third Council (15 July 1997), Section 2, 13.

[46] The White House, Office of Science and Technology Policy, "Global Information Infrastructure," *A White Paper Prepared for the White House Forum on the Role of Science and Technology in Promoting National Security and Global Stability* (30 March 1995), 3.

[47] Ibid., 19.

[48] The White House, Office of Science and Technology Policy, "Global Information Infrastructure," *The Global Information Infrastructure—Summary of Drafting Panel Discussion* (15 April 1995), 2.

[49] Ibid., 3.

[50] The White House, Information Infrastructure Working Group, "Privacy and the National Information Infrastructure," Introduction (6 June 1996), 1-2.

[51] Ibid., Introduction, 1.

[52] Ibid., 2.

[53] Ibid., 4.

[54] Ibid., 11.

[55] PL 104-13 Sec 3501, 4 January 1995.

[56] Ibid., Sec 3501 (1).

[57] Ibid., Sec 3501 (4).

[58] Ibid., Sec 3501 (10).

[59] The White House, Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," Section III, 15 September 1993.

[60] The White House, Information Infrastructure Task Force, "A Nation of Opportunity: Realizing the Promise of the Information Superhighway," Executive Summary, 30 January 1996, 2.

[61] Ibid., The Council's Vision, 5.

[62] Ibid., 13.

[63] Network Reliability and Interoperability Council, "Network Reliability: The Path Forward," Final Report of the Second Council (February 1996), Section 5, 71.

[64] "Network Interoperability: The Key to Competitiveness," 13.

[65] Op.cit, 55-56.

[66] Ibid., 14.

[67] Section 256 of the Telecommunications Act (47 U.S.C § 256).

[68] "Network Interoperability: The Key to Competitiveness," 14.

[69] Ibid., 15.

[70] Ibid., 14.

[71] Executive Order 13010, 15 July 1996, 1.

[72] Ibid., 2.

[73] Ibid., 3. CIO Council membership includes the DOD (includes separate representation from the DOD, DOA, DOAF, and DON), OPM, EPA, DVA, FEMA, CIA, SBA, SSA, NASA, GSA, NRC, the National Science Foundation, a senior representative of the Office of Science and Technology Policy, the Chair of the Government Information Technology Services Board, and the Chair of the Information Technology Resources Board.

[74] Ibid., 4.

[75] Ibid., 4.

[76] Ibid., 1 (d), 1.

[77] Ibid., Section 2 (b) (3), 2.

[78] Capen, 76.

[79] "DOD Approves Information technology Management Plan," *C4I News*, 27 March 1997.

[80] The White House, Office of the Press Secretary, "Background on Clinton-Gore Administration's Next-Generation Internet Initiative," 10 October 1996.

[81] "A Framework for Global Electronic Commerce" (Washington, D.C.: GPO, 1 July 1997), 1.

[82] Ibid., 1.

[83] Ibid., 2.

[84] The White House, Office of the Press Secretary, "Internet Initiative Press Release," 10 October 1996, 1.

[85] Ibid., 1-2.

[86] Ibid., 2.

[87] PL 104-104, codified as 47 U.S.C. 151.

[88] 47 U.S.C. § 256, also known as the Clinger-Cohen Act.

[89] Ibid., Section 256.

[90] Ibid., Section 256.

[91] Ibid., Section 256.

[92] National Security Telecommunications Advisory Committee (NSTAC), *Legislative and Regulatory Group Report*, December 1997, Annex C, 1.

[93] Ibid., 31.

[94] PL 104-106, 10 February 1996.

[95] Ibid., Section 5125(a).

[96] Col. Alan D. Campen, USAF (Ret), "Information Chiefs Join Federal Executive Teams," *SIGNAL*, vol. 51, no. 1 (May 1997), 75.

[97] Ibid., Section S 125(c).

[98] Ibid., Section S 125(c).

[99] Capen, 75.

[100] Also announced on 27 February 1997 to the Advisory Committee on High Performance Computing and Communications, information Technology, and the Next Generation Internet the following individuals as members: Eric A. Benhamou;Vinton Cerf; Ching-chih Chen; David Cooper; Steven D. Dorfman; Robert Ewald; David J. Farber; Serrilynne S. Fuller; Hector Garcia-Molina; Susan Grahm; James N. gray; W. Daniel Hillins; David C. Nagel; Raj Reddy;

Edward H. Shortliffe; Larry Smarr;Leslie Vadasz; Andrew J. Viterbi; and Steven J. Wallach.

[101] The White House, Office of the Press Secretary, "President Clinton Names Co-Chairmen of the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet, 12 February 1997.

[102] President William Clinton, Presidential Directive accompanying the release of "A Framework for Global Electronic Commerce" (Washington, D.C.: GPO, 1 July 1997).

[103] President William J. Clinton, "Presidential Memorandum on Electronic Commerce" (Washington, D.C.: GPO, 1 July 1997), 1.

[104] NSTAC, 1.

[105] "Network Interoperability: The Key to Competitiveness," 11.

[106] Executive Order 13062, Section 1 (g), 29 September 1997, 1.

[107] Executive Order 13062, Section 3 (d), 29 September 1997, 2.

[108] The White House, Office of Science and Technology Policy, "President Clinton Names Robert Elliot Kahn to Serve on Information Technology Advisory Committee," 24 July 1998. 1.

[109] Ibid., 1.

[110] Ibid., 1.

[111] Bill Joy and Ken Kennedy, Co-Chairs, President's Information Technology Advisory Committee, "PITAC-Report to the President: Transmittal Letter," dated 24 February 1999.

[112] Ibid., letter dated 24 February 1999.

[113] Congress, Senate. Senator William Frist of Tennessee, "Next Generation Internet Research Act of 1998," 105th Congress, 2d sess. *Congressional Record* (4 February 1998), S386.

[114] Ibid., S387.

[115] Ibid., S3119.

[116] Ibid., 7289.

[117] Ibid., H11702.

[118] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, Next Generation Internet Research Act of 1998, H.R. 3332, 105th Congress, 2d sess. *Congressional Record* (12 November 1998), D1203-1204.

[119] The White House, Office of the Press Secretary, "Statement by the President on the Next Generation Internet Research Act of 1998," 28 October 1998.

[120] Op.cit., D1203-1204.

[121] Ibid., D1204.

[122] Ibid., D1204.

[123] The White House, Office of Management and Budget, "Proposed Implementation of the Government Paperwork Elimination Act," *Federal Register* (5 March 1999).

[124] Ibid.,

[125] Executive Order 13113, Section 3, Section 4 (b), 1

[126] Ibid., 30.

[127] Ibid., 30.

[128] Ibid., 31.

[129] Ibid., 31.

[130] Ibid., 31.

[131] Ibid., 31.

[132] The White House, Office of Science and Technology Policy, "FY2001 Interagency Research and Development Priorities," *Memorandum for the Heads of Executive Departments and Agencies* (3 June 1999), 2.

[133] Ibid., 3.

[134] Ibid., 4-5.

[135] Ibid., 7-9.

[136] Executive Order 13038, 30 September 1999.

[137] Ibid., 29.

[138] United States Congress, House, Representative F. James Sensenbrenner of Wisconsin, "Network and Information Technology Research and Development Act," H.R. 2086, 106th Congress, 1st sess., *Congressional Record* (9 June 1999), E1186.

[139] United States Congress, House, Representative F. James Sensenbrenner of Wisconsin, "Network and Information Technology Research and Development Act," H.R. 2086, Sec.3.Authorzation of Appropriations (a-f), 22 February 2000.

[140] United States Congress, House, Representative Curt Weldon of Pennsylvania, debate on HR 2086, "Network and Information Technology Research and Development Act, *Congressional Record* (15 February 2000), H393.

[141] Ibid., H.R. 2086, H12106.

[142] The White House, Office of Science and Technology Policy, *Information Technology Research and Development: Information Technology for the 21st Century* (21 January 2000), 1.

[143] Ibid., 1-2.

[144] Donald Draper Campbell, *Network Reliability and Interoperability Council (NRIC),* homepage @http://www.nric.org, 15 March 2000.

[145] United States Congress, Senate, Senator William Frist of Tennessee, "The Next Generation Internet 2000 Act," S. 2046, referred to the Committee on Commerce, Science, and Technology, 106th Congress, 2nd sess., *Congressional Record, Daily Digest* (9 February 2000), D370.

[146] United States Congress, Senate, Senator William Frist of Tennessee, "The Next Generation Internet 2000 Act," S. 2046,106th Congress, 2nd sess., *Congressional Record* (9 February 2000), S546.

[147] Op. Cit., D370

[148] The White House, Office of Science and Technology Policy, "Testimony of The Honorable Neal Lane, Assistant to the President for Science and Technology before the Subcommittee on Science, Technology and Space, Committee on Commerce, Science, and Transportation, United States Senate, 1 March 2000, 1.

[149] United States Congress, Senate, S.2406, 106th, 2nd sess., *Congressional Record, Daily Digest* (13 April 2000), D375.

[150] United States Congress, House, Representative Doc Hastings of Washington, "Networking and Information Technology Research and Development Act," H. Res. 422, 106th Congress, 2nd sess., *Congressional Record* (15 February 2000), H389.

[151] Ibid., H400.

[152] The White House, Office of Management and Budget, *H.R. 2086 – Networking and Information Technology Research and Development Act* (15 February 2000), 1.

[153] Ibid., H401.

[154] Ibid., H402.

[155] Ibid., H402.

[156] Ibid., H403.

[157] Ibid., H404-405.

[158] Ibid., H405.

[159] Ibid., H405-406.

[160] Ibid., H406.

[161] Ibid., H406.

[162] Ibid., H407.

[163] Ibid., H407.

CHAPTER SIX

ENCRYPTION POLICY AND LEGISLATIVE INITIATIVES DURING THE CLINTON ADMINISTRATION (1993-2000)

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

The purpose of Chapter Six is to chronicle the specific actions and activities by the Federal Government in support of United States' Federal Encryption policy during the eight years of the Clinton Administration. This case study provides a chronological ordering of the policy-specific activities and associated impacts of Federal Encryption policy decision makers operating within the three branches of the Federal Government between the years 1993 and 2000.

The chapter is organized by calendar year. For each calendar year, significant Federal Encryption policy activities undertaken by the Clinton Administration, Congress, and the Federal Judiciary are chronicled. For the purposes of this study, a "significant Federal Encryption policy activity" is defined as: an administrative action, e.g., the publication of an Executive Order, formation of a Federal Advisory Commission, issuance of a report or formal policy statement by the White House; activity on a related bill by Congress; or a hearing or judgement rendered on a related case brought before a Federal court. In years where no significant Federal Encryption

policy activity was manifest, no annotation in the chapter chronicle was made.

BACKGROUND--SETTING THE STAGE

Several organizations have responsibility for establishing computer security controls and standards for the various agencies and departments of the Federal Government. The Office of Management and Budget (OMB) holds overall responsibility for computer security policy. The General Services Administration (GSA) is also empowered to issue regulations for physical security of computer facilities and for ensuring that security hardware and software meet certain technological and fiscal specifications.

Within the Department of Defense, the National Security Agency (NSA) bears responsibility for the security of all classified information, including all electronic information processed by and electronically stored within computer systems. NSA is also responsible for establishing and maintaining technical standards for secure, or trusted, computer systems. NSA accomplishes this through its administration of the Department of Defense's (DOD) National Computer Security Center (NCSC).

NSA also provides expertise to the private sector on data security standards and practices, working in a voluntary--not regulatory--advisory role with industry, through the National Computer Security Center, to develop security standards and applications for private sector use. However, NSA's role and its actions are severely restricted by the 1987 Computer Security

Act, which limits the agency's role in all but Federal computer systems which use, manage, or store classified information. The Computer Security Act assigns the role of protecting Federal-only computer systems which use, manage, or store unclassified to sensitive data to the Department of Commerce (DOC) and its National Institute of Standards and Technology (NIST).[1]

NIST's Institute of Computer Science and Technology (ICST) is the Federal agency responsible for developing computer security and information processing standards, such as the Data Encryption Standard (DES), discussed in detail later in this Chapter. The Federal Information Processing Standards (FIPS), developed by the ICST, provide specific codes, language, procedures, and techniques for Federal and private sector information systems managers. Also at the DOC, the National Telecommunications and Information Administration (NTIA) is responsible for analyzing, developing, implementing and applying executive branch policy for all telecommunications infrastructure employed within the Federal Government.

Under the auspices and policy direction of the Executive Branch, and operating within the legal guidelines provided by statute enacted by the Legislative Branch, these organizations create and execute national computer security standards and policy for the United States Government. This Chapter examines their origins, their organizational authority and

processes, and the recent history of their combined actions that have served to shape Information Assurance policy and practice for the United States.

National Security Council Intelligence Directive No. 9

On 24 October 1952, President Harry S. Truman issued National Security Council Intelligence Directive (NSCID) No.9, establishing the National Security Agency (NSA) under the Department of Defense. The NSA mission is to collect, process, evaluate, and disseminate foreign intelligence information gleaned from foreign-source electronic signals collected by national intelligence means, i.e., satellite collectors, cable taps, microwave intercept terminals, etc. NSA's primary focus in its information collection and processing role is national foreign intelligence and counterintelligence, as well as strategic and tactical support to military operations.[2] NSA is forbidden by law from any domestic use of its electronic surveillance resources within the United States.

Presidential Directive: Establishment of the Central Security Services

On 5 May 1972, President Richard Nixon issued a Presidential Directive establishing the Central Security Service (CSS) within the National Security Agency. As established by the Nixon Presidential Directive, the primary function of CSS is to provide a unified cryptologic authority and centralized encryption/de-encryption capability primarily for the Department of Defense (DOD) and across the Federal spectrum. The Director of NSA also serves as the Chief of the CSS.[3]

Public Law 100-235: The Computer Security Act of 1987

By 1986, the United States Federal Government operated over 17,000 medium- and large-scale computers. The Department of Defense alone had more computer users than any other organization in the world, employing some 2.1 million computers and accessing 10,000 networks on an average workday. In 1986, the Federal Government was easily the largest single user of computers in the world, with an investment in Information Technology systems that accounted for 1.6 percent of the 1986 Federal budget, or more than $15 billion in 1986 dollars.[4]

As the data processing and information dissemination roles of the Federal Government became broader, the need for data automation systems and a corresponding need to secure data, also grew. As a consequence, both the Congress and the Executive Departments and agencies began directing more of their attention to the operation of Federal computer systems in a number of areas, to include a focus on their internal data integrity and automated system security. Both Section 111(f) of the Federal Property and Administrative Service Act of 1949 (as amended by the Brooks Act of 1965) and the Paperwork Reduction Act, represented attempts by Congress to address the issues of automating information in Federal agencies and creating an efficient method of storing and disseminating that information.

In October 1984, Congress passed the first Federal computer crime legislation, the Counterfeit Access Device and Computer Fraud Act of 1984,

PL 98-473, which was amended by the Computer Fraud and Abuse Act of 1986, PL 99-474. The latter law prohibits "unauthorized access" into "Federal interest computers" affecting national security data, financial data, and other data stored in those computers. In addition, penalties were established for pirated "bulletin boards" containing information, which might subsequently lead to the fraud or abuse of data stored within a Federal computer.

This mixture of laws, regulations, and agency responsibilities began to raise concerns that Federal computer security policy was lacking direction and forcefulness in some areas, yet had created overlapping and duplicative effort in several other areas. This gave rise to the establishment of a host of Federal regulations and directives, along with the introduction of a number of pieces of Congressional legislation targeting the duplication of effort and lack of coordination among the Federal agencies.

On March 15, 1985, OMB issued a draft circular intended, "to provide a general framework of management for information resources." This circular combined and updated previous OMB circulars, including OMB Circular A-71 (originally issued in July 1978). The new OMB Circular, A130, was issued on 12 December 1985. Appendix III of the circular addressed Federal Government computer security requirements. Those agencies identified as being responsible for the implementation of this circular included the Department of Commerce, Department of Defense, General Services Administration, and the Office of Personnel Management, in addition to OMB.

On 17 September 1984, the Executive Branch issued National Security Decision Directive 145 (NSDD-145), "National Policy on Telecommunications and Automated Information Systems Security." This directive was aimed at safeguarding automated information systems, with a special focus on protecting those Federal systems accessed via (and dependent on) network communications. NSDD-145 created a National Telecommunications and Information Systems Security Committee (NTISSC), a panel of 22 voting representatives from 12 defense/intelligence agencies and 10 civilian agencies. An Assistant Secretary of Defense would chair the NTISSC, and the Director of the National Security Agency would act as the National Manager for implementing policy under NSDD-145. The NTISSC would be empowered to issue operating policies to assure the security of telecommunications and automated information systems that process and communicate both classified national security information and other sensitive data.

H.R. 2889: The Computer Security and Training Act of 1985

On 27 June 1985, Representative Dan Glickman, Chairman of the Subcommittee on Transportation, Aviation and Materials, and the House Committee on Science and Technology, introduced H.R. 2889, the Computer Security and Training Act of 1985. The intent of this legislation was to establish NBS as the focal point for developing training guidelines for Federal employees involved in the management, operation, and use of automated

information processing systems. This legislation was based in part on the results of hearings conducted by the Subcommittee in 1983, and a 1984 Subcommittee report, which recommended increasing ADP training and awareness in Federal agencies.

The Subcommittee on Transportation, Aviation and Materials conducted hearings on H.R. 2889 on 24 September 1984, 17 June 1985, and 29 October 1985 and again, jointly, with the Subcommittee on Science, Research and Technology on 30 October 1985. At the end of the 99th Congress and under House procedures, the bill was brought up for consideration under suspension of rules, but it failed to garner the necessary two-thirds vote required for advancement and went no further.

On 29 October 1986, National Security Adviser John Poindexter issued National Telecommunications Information Systems and Security (NTISS) policy Directive No. 2. This directive would have added a new "sensitive but unclassified" category of Federal information, setting new classification criteria for information formerly unclassified. It would not only have affected managers, users, and programmers of information systems within the Federal Government, but there was concern that it could have been extended to private sector contractors of the Federal Government as well, potentially restricting the type of information and data that could be released to the general public. However, on 16 March 1987, National Security Adviser Frank Carlucci rescinded NTISS Directive No. 2, following

negotiations with Congressional committees having jurisdiction over a new bill before the House, H.R. 145.

H.R. 145: The Computer Security Act of 1987

On 6 January 1987, Representative Dan Glickman introduced H.R. 145, the Computer Security Act of 1987. This legislation, based in part on H.R. 2889 introduced during the 99th Congress, assigned to the National Bureau of Standards responsibility for developing standards and guidelines for the security of Federal computer systems. It directed NBS to draw upon technical guidelines developed by the National Security Agency whenever such guidelines were consistent with the requirements for protecting sensitive information.

H.R. 145 also provided for a Computer Systems Advisory Board to identify emerging Federal computer security and privacy issues, advise NBS on these issues, and to report significant findings to the Office of Management and Budget (OMB), NSA, and to the Congress. The bill also amended the Brooks Act of 1965, by updating the definition of the term "computer" to reflect a more technically precise description of an evolved technology. It required the establishment of security plans by all operators of Federal computer systems containing sensitive information and required mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems containing sensitive information.

On 26 February and during the 100th Congress, the Subcommittee on Transportation, Aviation, and Materials, and the Subcommittee on Science, Research and Technology of the House Science, Space, and Technology Committee held hearings on H.R. 145. On 19 May 1987, the Subcommittee on Transportation, Aviation, and Materials held an additional hearing before voting to forward the bill for final consideration by the full House Science, Space and Technology Committee.

These two hearings touched upon four major issues: (1) the current state of computer security in the Federal Government; (2) the role of the National Security Agency (NSA) in setting Federal computer security; (3) the issue of privacy and security, particularly with a new "sensitive but unclassified" criteria; and (4) the role of the Federal Government in adequately training Federal employees and heightening awareness of computer security. Congress declared that improving the security and privacy of sensitive information in Federal computer systems was in the public interest and with passage of this Act, created a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.[5]

Specifically, the Computer Security Act of 1987 amended the Act of 3 March 1901 (15 U.S.C. 271-278h) by assigning to the then National Bureau of Standards, now the National Institute of Science and Technology, or NIST, responsibility for developing standards and guidelines for Federal computer

systems. Most particularly, NIST was to assume responsibility for developing standards and guidelines to assure the security and privacy of sensitive information in all Federal computer systems. To accomplish this mandate, NIST was to draw upon the technical advice and assistance (including products) of the National Security Agency. The principle target of the Act was controlling the loss and unauthorized modification or disclosure of sensitive information in federal computer systems and to prevent computer-related fraud and misuse [6]

In addition to security standards and guidelines, the Act also charged NIST with the responsibility for overseeing security planning for all Federal computer systems and for providing mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems containing sensitive information.[7]

Data Encryption Standard (DES-USDoC 1977)

By 1975, the National Security Agency (NSA) and the National Bureau of Standards (NBS) jointly recognized that the Privacy Act of 1974, and other Federal legislation, coupled with a growing use of computers and computer networks in both the public and private sectors, would soon create a demand for data protection and products that the Federal Government and/or the commercial sector would be compelled to meet.

The United States Federal Government, though adamantly opposed to any loss of NSA's monopoly and control of data security through its

cryptographic capabilities, was understandably reluctant to provide any of its products for general government or commercial use for two, very good reasons. The first reason was that commercial or even wide-spread United States Government use of NSA encryption products would complicate the task of real-time decoding of intercepted electronic messages, impacting both international and national law enforcement efforts, as well as national security practices. The second was that in providing encryption products to a larger clientele that might well include some perhaps inclined to "reverse engineer" NSA products in an effort to learn how they function, NSA could easily compromise its own, most closely guarded cryptographic methods and tools.[8]

In recognition of these conflicting needs, the Federal Government opted to openly solicit ideas for a new encryption system with the potential for widespread use. A 128-bit encryption algorithm--the key mathematical formula that underpins the encryption, or data scrambling process--developed by a team from IBM, was submitted for evaluation to the National Bureau of Standards (now NIST). For help in determining the strength and applicability of the algorithm, NBS forwarded "Lucifer," as the software was named, to the National Security Agency (NSA) for evaluation and possible certification as a commercial data encryption standard.[9]

In many ways, Lucifer was a revolutionary product. Lucifer was a digital shift-register system.[10] A digital shift register is an electronic device

made up of a number of cells or stages, each of which holds a single bit of information. As the shift register operates, the data is literally shifted, or moved, one or more cells along the register for every increment of time that passes, usually measured in seconds or fractions of seconds. In addition to moving to the left or right along the register, some of the bits are further modified by being combined with other bits. In nonlinear shift register systems, the value of the bits is table driven and then used to interchange the value of still other bits, all under the control of a key. This process is repeated over and over again, until every bit has changed in a way that is a complex function of every other bit of the key. Any single bit of input that is thus modified results in approximately fifty percent of the outputs bits being modified.[11]

IBM's Lucifer so impressed the agency that not only did NSA evaluate the algorithm, it felt compelled, according to some rumors, to dissect and tinker with its functionality before returning it to IBM. These reputed "modifications" spawned speculation that NSA installed its own "backdoor" into Lucifer, effectively permitting NSA to decrypt Lucifer-encrypted messages into plain text in real-time. This has never been substantiated. In fact, the final report from hearings held in 1978 before the Senate Intelligence Committee investigating this matter completely exonerated NSA of the algorithm tampering charge.[12]

What NSA did do was to shorten the Lucifer encryption key length from 128 bits to 56 bits. Other changes were made to the critically-important S-boxes, which are components of the algorithm that control the repeated substitution of letters and numbers or groupings of letters and numbers during the coding sequence.[13]

The number of bits in the key is also highly significant. Each bit (i.e., either a 1 or 0; each bit represents a binary, or two position switch--"0" for "off" and "1" for "on") used in creating a cryptographic key--in this case, 56-bit versus 128-bit--increases the strength of the algorithm exponentially. For every bit added to the key length, the complexity of the algorithm doubles. Therefore, for every bit added to the code, the effort required to decipher, or "crack" that code doubles, i.e., exponential versus linear progression.[14]

IBM re-tested and certified that the NSA "modified" product worked as originally intended. Both NIST and NSA were suitably impressed with the capabilities of even a modified Lucifer that, on 23 November 1977, it became the basis for an encryption system that became the United States Data Encryption Standard, or DES (USDoC 1977).[15]

From a commercial perspective, this 56-bit key DES was a significant leap forward in useable data security technology. In the greater world of encrytion and information assurance, DES was a poor "country cousin" to the much more sophisticated NSA cryptography of the day. By 1978, NSA had developed 1,024-bit cryptographic algorithms and had approved at least one

of them for use in commercial banking in support of high-dollar value, electronic funds transfers (EFTs). But in exchange for this industrial-strength encryption, NSA insisted on retaining, or "escrowing" the algorithmic cipher keys, thus enabling instantaneous government recovery and decryption of all electronic data transactions.

The 56-bit Lucifer-based DES continued in widespread use as the most advanced NSA-approved cryptographic product available for general commercial use and limited export for over two decades. However, an understanding of Moore's law reveals a fatal flaw in DES (see Chapter Four's discussion of Moore's Law). Following the trend of Moore's law over the past thirty years, the average desktop personal computer will have the computational power to break any 56-bit DES cipher within forty-five seconds by the year 2008. The current United States Data Encryption Standard still uses a 56-bit key, thus falling within easy range of the computing power of the next generation of home computers. Since the DES standard is used extensively throughout the commercial world and particularly by the banking industry to transact trillions of dollars of electronic funds transfers each day, the Moore's Law imperative was seen as a serious threat to the integrity of DES.[16]

In a study made public in December 1997, Trusted Information Systems reported that DES could be found in 281 foreign and 466 domestic encryption products, accounting for between one third and one half of the

market.[17] The inadequacy of the 56-bit standard was apparent. Because NIST had yet to issue a replacement standard, Triple-DES, a block cipher employing DES in three block rows, each having a separate key, arose as a de facto upgrade to DES. Triple-DES has since been accepted as a standard by the Banking Standards Committee (ANSI X9F) of the American National Standards Institute (ANSI).[18]

DES was revolutionary in one very significant, additional aspect. NSA assumed that DES would be used as an embedded, hard-wired software component within a hardware encryption device. When NBS/NIST published the new standard, NSA was surprised to learn that the entire algorithm had been published within the standard, providing computer programmers world-wide a first-time opportunity to study the complexities of an encryption algorithm certified by NSA. For the first time, software developers outside the Federal Government were privy to an essential blueprint for the development of virtual software encryptors based upon DES. NSA acknowledged that had they known that the details of the algorithm were to be released, NSA would never have approved release of the algorithm as a commercial standard.[19]

Although once considered prohibitively costly and nearly technically impossible for all but the most sophisticated government-sponsored cryptologic organizations, 56-bit DES encryption algorythms have been deciphered.[20] On 19 January 1999, the Electronic Frontier Foundation's (EFF) DES Cracker, a specially designed PC-based, virtual supercomputer,

linking together 100,000 PCs through the Internet, deciphered a 56-bit encoded message in 22 hours, 15 minutes.[21]

RSA's original DES Challenge was launched in January 1997 with the aim of demonstrating that DES offers only marginal protection against a committed, cyber intruder. This was confirmed when a team led by Rocke Verser of Loveland, Colorado recovered the secret key in 96 days, winning the DES Challenge I. In February 1998, Distributed.Net won RSA's DES Challenge II-1, with a 41 day effort, followed by EFF's 56 hour code breaking accomplishment five months later, on 13-15 July 1998.[22]

In a letter to EFF's President Barry Steinhardt, dated 10 August 1998 and issued after the July 1998 contest, Deputy Assistant Director of the FBI Edward Allen expressed the Bureau's interest, but lack of concern in the Distributed.Net/ EFF accomplishments, saying:

> You must realize that law enforcement, in the most critical, often life threatening investigations, requires immediate, lawful access to information. This obviously includes the "plain text" of encrypted data, both stored and in-transit (communicated). The reports claim that 56 bit DES can be broken in 56 hours, which falls far short of legitimate and lawful law enforcement needs.[23]

A similar sentiment was expressed in a 26 August 1998 letter received by Steinhardt from Undersecretary of Commerce for Export Administration, William Reinsch, in which Reinsch said:

> With respect to your comments about breaking DES, ...I would only observe that "breaking" is a bit of an elastic term. Spending 56 hours breaking a single message in a situation where those making the attempt knew where the message was

and, presumably, knew it was in English, is not analogous to the real-time problems facing law enforcement.[24]

Public-Key Encryption

With all of the attention focused on the Lucifer-based DES, little notice was paid outside cryptographic circles to an announcement in 1976 of a new kind of cryptography, called public-key encryption (PKE). Public-key encryption works by the sender and the receiver of a message each having a private and a public encryption algorithm, or key. Each individual's public key is available to anyone, but only the individual who generated it knows the corresponding private key, which unlocks the public key. The sender encrypts the message using the receiver's public key. The message can only be deciphered by the receiver's private key.

Public-key cryptography, also known as asymmetric-key cryptography, is based upon a mathematical discovery made during the 1974-1975 academic year by a pair of Stanford University graduate students, Whitfield Diffie and Martin Hellman.[25] What Diffie and Hellman discovered is that there are pairs of numbers, such that data encrypted with one member of a unique pair of such numbers can only be decrypted by the other member of the pair and by no other means. If the numbers are large enough, it is extremely difficult, even knowing one member of a pair, to deduce the other member. This provides sufficient assurance that the owner of the key pair may distribute the public key widely, with little fear that the private key can be

determined. Anyone who has access to the public key can encrypt data, but only the holder of the private key can decrypt it. [26]

The major disadvantage of asymmetric-key cryptography is that it is considerably slower to execute than symmetric-key cryptography, and is therefore impractical for use in encoding large data sets. However, it can be combined with symmetric-key cryptography to form a very secure and agile cryptographic solution. The hybrid solution works by encrypting the plaintext using a symmetric encryption key, then implanting the key in the header block of the transmitted data and encrypting the header block using the public key for the asymmetric encryption algorithm. If the data is concurrently sent to more than one user, each recipient would have a different header block, since each recipient has a unique private key.[27]

Asymmetric-key cryptography may also be used to provide authentication. Authentication serves as the guarantor of the identity of the originator of the message and also prevents the originator from denying authorship after the fact. Asymmetric-key cryptography provides an integrity, or authentication service, "guaranteeing" that a message has not been modified since it was digitally "signed" and electronically transmitted by the original sender.[28]

By early 1991, the team of computer scientists, Ron Rivest, Adi Shamir, and Leonard Adelman, had created RSA, the first cryptosystem to use the PKE algorithm system. In June 1991, Philip Zimmerman, a computer

scientist in Boulder, Colorado, used the RSA algorithms to create an extremely strong and robust encryption program he named PGP, for Pretty Good Privacy. When it appeared as freeware on the Internet for public consumption, the security services of the United States went into apoplexy.[29]

Clearly, commercial industry and market demand for strong encryption products, much as nature itself, could not be artificially constrained nor denied indefinitely. Eventually, the explosive growth of the Internet and electronic commerce, coupled with a lightening-fast evolution of advanced programming languages and tools, became too much of an irresistible force to be contained. The Information Age demand for new and better products to protect the intellectual property and privacy rights of individual users on the Information Superhighway, became undeniable. The private sector met that demand by creating RSA, PGP, and other new and enabling products that fell squarely into the Federal Government's regulatory lap. A new approach to the nation's Federal policies on encryption, encryption products, and their export was needed. This was one of the Information Assurance challenges facing the Clinton Administration as it took office in January 1993.

CLINTON ADMINISTRATION--1993

To control the public proliferation of encryption software, the Clinton Administration devised a two-step strategy. First, it resorted to a law, the Arms Export Control Act (22 U.S.C. 2571-2794), designed to control the export of arms and munitions. The Clinton Administration declared that all

encryption software beyond a certain strength--in this case forty bits--"qualified" as a munition under the Act, and was therefore illegal to export.[30]

The second step of the Clinton Administration's control strategy was to create a government-sponsored, public-key alternative to the new, commercially-based encryption products employing public-key technologies. The first of these key escrow or "spare key" programs was the Clipper Program, which made the term "Clipper" virtually synonymous with key escrow. The program made its much-heralded public debut on 13 April 1993, with multiple press releases from the White House and other Federal Government institutions, along with Clinton Administration-orchestrated front-page news releases in the *Washington Post* and *New York Times.*[31]

The centerpiece of the announced policy was the adoption of a new Federal standard for protecting electronic communications. It called for the use of an advanced cryptographic system; one embodying a software "backdoor" that would allow the United States Government, and the government only, to decipher messages encrypted by the new system for law enforcement and national security purposes.

Key recovery, which refers to access to encryption key materials, allows individuals to retain the critical information necessary for a third party to reconstruct a key to the encryption code. Key escrow involves having a third party, such as the Federal Government, hold the cipher key to an encryption product. Holding the cipher key is akin to having an extra set of

keys to the neighbor's house while the neighbor is on vacation. In concept, it is intended to promote security for the neighbor's property, when the arrangement works as expected. However, nothing, save honesty and neighborly good, will restricts the key holder from unlocking the residence at will and randomly browsing through the most intimate of the owner's personal property. The ramifications of such a policy are significantly compounded, when the keys were held by that third party in perpetuity--thus the vehement objections from 1st and 4th Amendment advocates to government-controlled key escrow schemes.

Subsequently adopted by the Clinton Administration over the unanimous opposition from civil libertarians and the computer and telecommunications industries, the Escrowed Encryption Standard (ESS) proved itself a very unpopular standard. As a result, software developed by American commercial companies largely ignored provisions for serious data access protection, making most of the world's commercial-off-the-shelf (COTS) software extremely vulnerable to fairly simple cyberintrusion techniques and tools.[32]

CONGRESS--1993

H.R. 3627: Legislation to Amend the Export Control Act of 1979

On 22 November 1993, a bill to amend the Export Administration Act of 1979, with respect to the control of computers and related software and equipment, was introduced by Congresswoman Maria Cantrell (D-WA).

Formally known as the Legislation to Amend the Export Control Act of 1979, this bill sought to amend the 1979 Act's export controls on computer software with encryption capabilities.

In introducing this bill, Representative Cantrell sought to target the debilitating impact that software encryption export restrictions were having on United States software vendors. Ms. Cantrell's Washington Congressional District included Redmond, WA, home of the Microsoft Corporation. In her introductory remarks, Congresswoman Cantrell stated:

> Mr. Speaker, I am today introducing legislation to amend the Export Control Act of 1979, to liberalize export controls on software with encryption capabilities. A vital American industry is directly threatened by unilateral United States Government export controls which prevent our companies from meeting worldwide user demand for software that includes encryption capabilities to protect computer data against unauthorized disclosure, theft, or alteration. The legislation I am introducing today is needed to ensure that American companies do not lose critical international markets to foreign competitors that operate without significant export restrictions. Without this legislation, American software companies, some of America's star economic performers, have estimated they stand to lose between $6 and $9 billion in revenue each year. American hardware companies are already losing hundreds of millions of dollars in lost computer sales, because increasingly sales are dependent on the ability of an U.S. firm to offer encryption as a feature of an integrated customer solution involving hardware, software, and services.[33]

Section I of the proposed bill (Section 2 provides definitions only) would amend the Export Administration Act by adding a new subsection with three specific provisions to address the export of encryption technology. The first provision would grant the Secretary of Commerce exclusive authority

over the export of all computer programs and products, except those specifically designed for military use or for deciphering encrypted information. The second provision would prohibit the Federal Government from requiring an export license for the export of generally commercially available computer hardware and software, including encryption products. The third provision would require the Secretary of Commerce to grant validated export licenses for the export of software to commercial users in any country to which exports of that software is approved for use by foreign financial institutions.[34]

H. R. 3627 specifically would not require the Secretary of Commerce to grant export licenses for the export of computer security products, especially software, to foreign commercial users in any country for which substantial evidence exists suggesting that the products would be diverted or modified for military or terrorists end-use, or used or re-export purposes.[35]

Following its initial reading on the floor of the House, H.R. 3627 was referred to the House Committee on Foreign Affairs on 22 November 1993. On 6 December 1993, the House Committee on Foreign Affairs referred the bill to its Subcommittee on Economic Policy, Trade and Environment. No further action was taken on the bill.

CLINTON ADMINISTRATION--1994

The White House: Changes to Computer Export Policy

On 1 April 1994, President Clinton announced changes to U.S. computer export controls, liberalizing licensing requirements on the export of

nearly all commercial telecommunications equipment and computers operating at up to 1,000 million theoretical transactions per second (MTOPS). This liberalization of the export licensing requirements effected the sale of computers to civil end-users in all computer export controlled countries, except those in North Korea.[36]

Executive Order 12924: Declaration of National Emergency Under the International Emergency Economic Powers Act (IEEPA)

On 19 August 1994 and in response to the refusal of the Congress to extend the statutory life of the Export Administration Act of 1979, President Clinton declared a national state of emergency with respect to the lapse of the Export Administration Act and the system of export controls maintained under that Act. As part of that declaration, President Clinton invoked the presidential authorities available to him under the International Emergency Economic Powers Act (IEEPA) to continue the functions of EEA under emergency conditions.[37]

EO 12924 conferred upon the Secretary of Commerce a continuance of the export control authority granted by the Export Administration Act. The Executive Order charged the Secretary of Commerce with the responsibility of approving the issuance of all export licenses and for establishing the requirements, reviews, and approval process for documentation and other forms of information supporting applications for export licenses. The Order prohibited the export of any goods, technology, or service without appropriate

licensing, subject to the Secretary's export jurisdiction and authority. Licensing the export of sensitive technologies, such as computers and encryption products, could only be made in consultation with the Secretaries of State and Defense.[38]

The National Institute of Standards and Technology/National Security Agency: Establishment of a National Digital Security Standard (DSS)

By 1994, RSA's proprietary public-key algorithm was the most widely employed, asymmetric-key encryption algorithm in commercial use. The patented RSA algorithm, the only commercially-available, asymmetric-key algorithm capable of providing both a digital signature and encryption service from the same mathematical formula, was a preferred product of the United States Government, as well. However, the algorithm's patent created a barrier to its more widespread use within government (i.e, RSA charged a royalty for every public/private key pair generated by the patented algorithm).[39]

In response, in October 1994, the National Institute for Standards and Technology (NIST) created a Digital Signature Standard (DSS) for the United States Government. DSS was based upon the Digital Signature Algorithm (DSA) previously developed by the National Security Agency (NSA). DSS, would however, only provide a digital signature service, not an encryption service. To circumvent the RSA patent, the Federal Government adopted the Diffie-Hellman encryption algorithm for use in tandem with DSS. The Diffie-

Hellman algorithm was developed in the 1970s by Whitfield Diffie and Martin Hellman, co-inventors of asymmetric-key cryptography.[40]

CONGRESS--1994

H.R. 3937: The Export Administration Act of 1994

On 2 March 1994, Representative Samuel Gejdenson (D-CN) introduced H.R. 3937, The Export Administration Act of 1994, to the full House of Representatives. Known also as the Omnibus Export Administration Act of 1994 and the Nuclear Proliferation Prevention Act of 1994, the goal of Title I of H.R. 3937 would stem the proliferation of materials and technologies used in the manufacture of weapons of mass destruction through aggressive export controls. The bill would also specify export goals and relax export restrictions on computers and encryption hardware and software, counteracting the existing, restrictive Information Technology trade policies of the Clinton Administration.[41]

Section 105 of Title I would require the Secretary of State to periodically review and remove export controls on computer equipment, computer communications and networking equipment, computer software, and related technology that had become obsolete. Section 105 would also require the Secretary of State to establish a goal to eliminate export controls on mass-market, commercial-based computer equipment in instances of United States export policy, where such controls exist. Finally, Section 105 would direct the Secretary of State to enter into an arrangement with the

National Academy of Sciences and the National Academy of Engineering to study and report to the President and the Congress on the extent to which exports of computers could be controlled, as well as the methods for maintaining such controls.[42]

Section 117 of Title II of the Act would require the President to prepare and submit a report to the Congress, assessing the international market for computer encryption software and the impact of United States encryption export controls on the international competitiveness of the United States computer software industry.[43]

Following its introduction to the House floor, H.R. 3937 was referred to the House Committee on Foreign Affairs on 2 March 1994. The Foreign Affairs Committee, in considering the bill, held a Mark-up Session, amending the bill on 18 May 1994. The Committee reported the amended bill to the House through House Report 103-531, Part I.[44]

On 25 March 1994, the bill was referred jointly and sequentially to the House Committee on Armed Services, the House Committee on Judiciary, the House Committee on Way and Means, and the House Committee on Intelligence, for a period of time not to exceed 17 June 1994, for consideration of those measures within the bill falling within each of the Committees' jurisdictions. On 15 June 1994, each of the Committees met to consider the bill. Each of the Committees amended the bill during its respective Mark-up Sessions; each approved the amended bill by voice vote.

The bill was reported out favorably to the full House on 17 June 1994 through House Report No. 103-531, Parts I-IV (each part corresponding to each of the four Committees which reviewed the bill).[45]

On 17 June 1994, the bill was placed on the Union Calendar No. 304. On 12 July 1994, the Rules Committee passed House Resolution 474, allowing H.R. 3937 to be called up and considered by the full House under suspension of the House rules.[46]

H. Res. 474: Providing for Consideration of H.R. 3937, Export Administration Act of 1994

Acting under direction from the House Committee on Rules, Congressman Bart Gordon (D-TN) called up H.R. 3937 under House Resolution 474, asking for immediate consideration of the bill before the full House. The floor debate revealed a fractured House, split on the merits of an imperfect bill versus having no export administration control legislation at all. Congressman Gerald R. Soloman (R-NY) summed the debate up best in his statement for the record:

> I hope that Members will not oppose this rule, because it represents the best that could be done under the difficult circumstances that surround the bill. Mr. Speaker, The Export Administration Act has always presented difficulties on the floor of the House because it is an extraordinarily important statute which happens also to be highly technical in nature and something that does not lend itself to superficial analysis or debate.[47]
>
> The Export Administration Act sets forth the policies, procedures, and institutional oversight concerning the export of so-called dual-use items—civilian products, commodities, or

technologies that have potential for military applications. In controlling the export of such dual use items, an appropriate balance must be struck between the absolute imperative of protecting the security of the country and the legitimate needs of the United States business community to remain competitive in international markets.[48]

The single most important element of this bill is the establishment of a statutory relationship or integration between United States policies on the export of dual-use items and the policies maintained by the multilateral export control regimes of which the United States is a member. In other words, from here on out, our Government will be relying almost exclusively on a multilateral approach for the establishment and enforcement of export control policies. [49]

This causes me great concern, Mr. Speaker, especially when I observe the performance of an administration that seems to view multilateral organizations as a substitute for United States leadership--instead of places where America must lead. Many of the provisions in this bill will have to be subject to further multilateral negotiations before they can be implemented, and they will have to be reinforced constantly and consistently in order to be effective thereafter. Is the Clinton Administration up to this kind of challenge? Frankly, I doubt it.[50]

Then there is the whole issue I mentioned earlier: The question of which Federal department should be the lead agency in this new process. This bill would give the Commerce Department almost exclusive control and that really alarms me. During the 1980s, I found the Export Licensing Office at Commerce to be a shoestring operation more suited for a Charles Dickens story than for keeping up with the analytical demands imposed by modern technology and the multitude of dangerous places to which such technology can be diverted.[51]

Does the Commerce Department have the qualified personnel, the database, the technical infrastructure, and, most importantly, the commitment to undertake these new responsibilities? Frankly, I doubt it. In short, Mr. Speaker, I seriously question whether our government presently has either the political will or the administrative know-how to make good on the multilateral approach to export controls that this bill sets up. Our country has already fought one war against a

> dictatorship that managed to arm itself with military aid and dual-use technology from western sources. And unless the Members think the United States can afford to conduct another operation Desert Storm any time soon, they had better take another look at this bill.[52]

Following the debate, the bill was passed on a roll-call vote of 188 in favor, to 157 opposed. There were 90 abstentions. The vote reflected the fractured nature of the debate. Of the 188 yeas cast, Republicans cast 72 and Democrats cast 116. Of the nays cast, Republicans cast 67 and Democrats cast 89. The abstentions reflected a similar split: 39 Republican and 51 Democrat.[53]

H.R. 4922: Communications Assistance for Law Enforcement Act (Public Law 103-414)

On 9 August 1994, Representative William D. "Don" Edwards (D-CA) introduced H.R. 4922 to the Congress. The bill, entitled the Communications Assistance for Law Enforcement Act, amended Title 18 of the United States Code, clarifying the legal responsibilities and duties of telecommunications carriers in cooperating in the interception of certain electronic communications at the request of law enforcement and national defense agencies. Title I, Interception of Digital and Other Communications, would require that pursuant to a court order or other lawful authorization:

- carriers be able to isolate and enable government intercepts of all subject subscribers' electronic communications over the carriers' equipment;

- that carriers be able to isolate the physical locations for the subject transmissions through call identification information (CII) technologies and provide that information upon request;
- that carriers deliver those intercepted transmissions and CII data to law enforcement authorities, as directed; and,
- that carriers do so unobtrusively and in a manner that protects the privacy and security of those communications not subject to court ordered search and seizure.[54]

The bill specifically prohibited a carrier from being responsible for decrypting or ensuring government's ability to decrypt any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possessed the information to decrypt the encrypted communications.[55]

On 9 August 1994, H.R. 4922 was read on the floor of the House of Representatives and then referred to the House Committee on Judiciary for review. The House Committee on Judiciary referred it to its Subcommittee on Civil and Constitutional Rights the following day, 10 August 1994. On 11 August 1994, the House Subcommittee on Civil and Constitutional Rights and the Senate Committee on Judiciary, Subcommittee on Technology and the Law held joint hearings on the bill. On 17 August 1994, the House Subcommittee on Civil and Constitutional Rights held a successful Consideration and Mark-up Session, then forwarded the bill to the full House

Committee on Judiciary for its consideration. On 4 October 1994, the bill was reported to the House (amended) by the House Committee on Judiciary, through House Report 103-827, Part I.[56]

On 4 October 1994, H.R. 4922 was called before the full House under a motion to suspend the rules. The bill was sequentially referred to the House Committee on Energy and Commerce, in consideration of provisions of the bill falling within the jurisdiction of that committee, pursuant to Clause 1 (h), Rule X off the House Rules. On 5 October 1994, the bill was again brought before the full House, this time for consideration as unfinished business. The bill passed the full House, as amended, by a voice vote.[57]

H.R. 4922 was referred to the Senate on 6 October 1994. On 7 October 1994, the bill passed the Senate by voice vote and without amendment and was cleared for the White House by Executive Branch action later that same day. On Oct 12, 1994, the official message on the Senate action on H.R. 4922 was sent to the House of Representatives. The enrolled measure was signed by the House and Senate on 17 October 1994 and presented to President Clinton for his signature on 18 October 1994.[58]

H.R. 4922 was placed before and subsequently signed into law by President William Clinton, becoming Public Law 103-414 on 25 October 1994.[59]

S. 2375: Communications Assistance for Law Enforcement Act

On 9 August 1994, Senator Patrick Leahy (D-CN) introduced to the floor of the Senate a companion bill to H.R. 4922 entitled, the Communications Assistance for Law Enforcement Act. S. 2375 was a near-verbatim copy of the House bill introduced on 9 August 1994 by Representative William D. "Don" Edwards (D-CA). Upon its introduction, it was immediately referred to the Senate Committee on Commerce for consideration.[60]

On 25 August 1994, the Senate Committee on Commerce completed its review of the bill and reported it favorably out of committee without amendment. The bill was reported out to the full Senate by the Committee on Commerce Chair, Senator Earnest Hollings (D-SC), without recommendations or amendments. The bill was placed on the Senate Legislative Calendar under General Orders Calendar No. 603. At the same time, the bill was referred to the Senate Committee on Judiciary.[61]

On 19 September 1994, Judiciary Committee Chairman, Senator Joseph Biden (D-DE) referred S. 2375 to the Subcommittee on Technology and the Law, which, due to favorable scheduling, had already held joint hearings on the bill with the House Subcommittee on Civil and Constitutional Rights on 11 August 1994. The Subcommittee on Technology and the Law approved the bill for full committee consideration with a single amendment by nature of a substitute clause, in keeping with the House version of the bill. On

28 September 1994, Chairman Biden and the Judiciary Committee approved the bill, as amended by the subcommittee. The bill was placed on the Senate Legislative Calendar under General Orders Calendar No. 684.[62]

On 6 October, Senator Biden filed Report No. 103-402 from the Senate Judiciary Committee, clearing the bill for action by the full Senate. On 7 October, the bill passed the Senate on a voice vote. This action was reported to the House later on 7 October 1994.[63] S.2375 was then merged into H.R. 4922. President Clinton signed the bill into law, becoming Public Law 103-414 on 25 October 1994.

H.R. 5199: Encryption Standards and Procedures Act of 1994

On 6 October 1994, Representative George Brown (D-CA) introduced H.R. 5199, the Encryption Standards and Procedures Act of 1994. H.R. 5199 was designed to amend the National Institute of Standards and Technology Act to provide for the establishment and management of voluntary encryption standards to protect the privacy and security of private sector and commercial electronic information. The bill would establish an Encryption Standards and Procedures Program to promote the development of an information infrastructure consistent with the needs for national security and public welfare, balanced against the needs for privacy and protection of individual data and intellectual property rights. The bill would promote the development and use of encryption standards and technologies and establish new Federal encryption policies and standards.[64]

The bill was short-lived. On 6 October 1994, H.R. 5199 was referred to the House Committee on Science, Space and Technology, where it was tabled in Committee.[65]

CLINTON ADMINISTRATION--1995

Executive Order 12981: Administration of Export Controls

On 6 December 1995, President William Clinton signed Executive Order 12981, Administration of Export Controls. This Executive Order reaffirmed the, "power, authority, and discretion conferred upon the Secretary of Commerce by the Export Administration Act," and continued them under the auspices of the Executive Order. The Executive Order established a ninety-day maximum for the resolution of any export licensing issues before their automatic referral to the President for final disposition. In addition, the Executive Order granted export license review authority to the Departments of State, Defense, and Energy and the Arms Control and Disarmament Agency.[66]

EO 12981 also established an Export Administration Review Board, chaired by the Secretary of Commerce and consisting of the Secretaries of State, Defense, Energy, and the Director of the Arms Control and Disarmament Agency, whose purpose would be resolving agency disputes arising over the export licensing process.[67]

CLINTON ADMINISTRATION--1996

Executive Order 13026: Administration of Export Controls on Encryption Products

On 15 November 1996, President Clinton issued Executive Order 13026, the Administration of Export Controls of Encryption Products. This placed additional restrictions on the export of encryption products, including those products for which equivalent foreign products were available:

> I have determined that the export of encryption products could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States, and that facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure of judicial review without revealing or implicating classified information that could harm the United States national security or foreign policy interest.[68]

The Executive Order conferred on the Secretary of Commerce the authority, "at his discretion," to consider the foreign availability of comparable encryption products in determining whether to issue export licenses or to remove controls on the export of certain encryption products. However, the Executive Order did not require the Secretary of Commerce to issue licenses or remove export controls on products based on such consideration.[69]

CONGRESS--1996

H.R. 9011: The Security and Freedom Through Encryption Act of 1996

In response to privacy concerns expressed by civil libertarians over the Federal Government's key escrow policy decision, Congressman Robert

Goodlatte introduced H.R. 9011, the Security and Freedom Through Encryption (SAFE) Act, on 5 March 1996. The intent of H.R. 9011 was to amend Title 18 of the United States Code, to affirm the rights of United States citizens to use and sell encryption and encryption products and to relax controls on their export. The bill was also intended to amend the United States criminal code to permit any person within the United States, and any United States citizen in a foreign country, to use any encryption regardless of the encryption algorithm used, encryption key length selected, or implementation technique employed. The sole prohibition would be the unlawful use of encryption to further criminal activity. [70]

The SAFE Act of 1996 specified that no person in lawful possession of a key to encrypted information could be compelled by Federal or State law to relinquish that key to any other person, save for legal access for law enforcement purposes. It also would amend the Export Administration Act of 1979, by granting to the Secretary of Commerce exclusive authority to control the export of encryption and encryption products, an authority previously vested jointly in the Departments of State and Defense. Finally, the SAFE Act of 1996 authorized the Secretary of Commerce to permit the export of encryption products and capabilities for non-military use to any country to which exports of similar software were permitted for use in the financial industry, even if the institution was not subject to control by the United States.[71]

On 25 March 1996, the SAFE Act was referred to both the House Committee on Judiciary and the House Committee on International Relations for consideration of provisions of the Act that fell within their individual purviews. The bill was subsequently referred to the Subcommittee on International Economic Policy and Trade, who endorsed it and returned it to the Committee on Judiciary. The Committee on the Judiciary held a Committee hearing on the bill on 25 September 1996. No floor actions resulted from the committee hearings and the bill was permanently tabled.[72]

S.1726: Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996

On 2 May 1996, Senator Conrad Burns (R-MT) introduced The Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996. The intent of the bill was to prohibit the Secretary of Commerce from promulgating or enforcing regulations, adopting standards, or carrying out policies that would result in the adoption of computer system encryption standards intended for use by anyone other than the Federal Government. Pro-Code would also prohibit the government from taking any action that would have the effect of imposing government-designed encryption standards on the private sector, i.e., by restricting the export of computer hardware and computer software with commercially-based encryption capabilities.[73]

Pro-CODE was designed to prohibit the Federal and state governments from restricting or regulating the interstate sale of any product with encryption capabilities, or requiring, as a condition of such a sale, that a decryption key--key escrow--be given to any other party, including a Federal agency or a private entity certified or approved by the Federal Government.[74]

Pro-CODE was designed to eliminate the need for export licensing (with limited exceptions) in the export or re-export of any commercially-available computer or computer software, including that with encryption capabilities, designed for installation by the purchaser, or in the public domain, including on the Internet. It would grant the Secretary of Commerce exclusive authority to control exports of all computer hardware, software, and technology with encryption capabilities, except those products specifically designed or modified for military use, including command, control, and intelligence applications.[75]

Finally, the bill would require the Secretary of Commerce to authorize the export or re-export of computer software with encryption capabilities under a general license for nonmilitary end-uses in any country to which exports of software or hardware of similar capability were permitted for use by financial institutions, including those not controlled by U.S. citizens.[76]

After being twice read on the Senate floor, Pro-CODE was referred to the Senate's Committee on Commerce, Chaired by Senator John McCain (R-AZ), on 2 May 1996. On 12 June 1996, the Subcommittee on Science,

Technology, and Space held hearings on the bill. The bill was returned to the full Committee, which held its own hearings on 25 July 1996. The Committee voted not to forward the bill to the full Senate for its consideration.[77]

JUDICIARY--1996

At least two plaintiffs challenged Clinton Administration polices on data encryption products and their export. Both suits were filed in 1996, the first in the United States District Court for the District of Columbia, the second in the United States District Court for the Northern District of California.

***Karn v. Department of State*, 925 Federal Supplement 1 (D.D.C. 1996)**

In *Karn v. Department of State*, Plaintiff Karn sued the Federal Government in a challenge to its practice of labeling encryption software as a "munition," thus legitimizing their falling under the control of the Arms Export Control Act (AECA, 22 U.S.C. Sec 2751 et seq.) and its accompanying International Trafficking in Arms Regulations (ITAR, 22 C.F.R. 120 et. seq.). The United States District Court for the District of Columbia ruled that the Federal Government's decision to designate an encryption product as a munition, and therefore restrict its export, was not subject to judicial review. The Court further held that the Federal Government's export restrictions on data encryption products was content neutral and narrowly tailored, and, therefore not in violation of the First Amendment.[78]

***Bernstein v. Department of State*, 945 Federal Supplement 1279 (N.D. Cal. 1996)**

In 1990, New York University undergraduate student Daniel Bernstein developed a program called Snuffle. Snuffle was a mapping and conversion program, which facilitated the transformation of non-encrypted software into an encrypted version. Bernstein was concerned that the Federal Government, in permitting the export of this class of non-encrypted software, would be exporting products easily transmuted into prohibited encrypted software.[79]

In 1992, as a Berkeley graduate student, Bernstein decided to test his theory and sought the Federal Government's approval to publish Snuffle as freeware on the Internet. His request was rejected by both the State Department and by NSA, and he was informed that his product could only be officially sanctioned by the Federal Government for sale or other public distribution as a registered munition under Category XIII of the United States Munitions List, which at that time was regulated by the Department of State under the Arms Export Control Act (22 U.S.C. 2778 et seq.).[80]

Bernstein and supporters John Gilmore, of the Electronic Frontier Foundation, and Cindy Cohn, a young free-speech lawyer from San Mateo, CA, filed suit in 1995 with U.S. District Judge Marilyn Patel. At the heart of their case was the contention that computer source code was a constitutionally protected form of speech, not subject to restrictions by Federal Government administrative or departmental regulations. The Federal

Government argued that encryption products must be subject to regulation on national security grounds. But Judge Patel ruled in favor of the Plaintiff, Bernstein, affirming that the export restrictions on encryption products were unconstitutional prior restraints on free speech because of inadequate procedural safeguards.[81]

CLINTON ADMINISTRATION--1997

Department of Commerce/NIST: Plans to Develop an Advanced Encryption Standard

On 2 January 1997, the National Institute of Standards and Technology announced plans to establish a new Federal Advanced Encryption Standard (AES). Based upon a hybrid asymmetric/symmetric algorithm combination, the new Federal standard would be chosen from algorithms and products solicited from the private sector. NIST announced that the new standard would be in place by 1 January 2002.[82]

Department of Commerce/NIST: Plans to Develop a New Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange

On 13 May 1997, the National Institute of Standards and Technology announced plans to develop a new Federal Information Processing Standard (FIPS) for public-key based cryptographic key agreements and exchange. The standard would be used to design and implement public-key based key agreements and exchange systems operated by Federal agencies and departments. The notice specifically identified the RSA, Diffie-Hillman, and

Elliptic Curve algorithms and encryption techniques as examples of acceptable approaches to address the Federal need, stating that more than one algorithm could be specified in the standard, consistent with sound security practices.[83]

The announcement further stipulated that the new cryptographic standard support key recovery and key escrow under current Clinton Administration encryption policy:

> The Administration policy is that cryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable through an agency or third-party process and that keys used for digital signature (i.e., for integrity and authentication of information) shall not be recoverable. Agencies must be able to ensure that signature keys cannot be used for encryption. Any algorithms proposed for digital signature must be able to be implemented such that they do not support encryption unless keys used for encryption are distinct from those used for signature and are recoverable.[84]

President's Commission on Critical Infrastructure Protection (PCCIP)

On 13 October 1997, General Thomas Marsh (USA, Ret.) delivered the final report of the President's Commission on Critical Infrastructure Protection (PCCIP) to President Clinton. In the letter accompanying the report, General Marsh reported that the United States' increasing dependence on networked information and communications systems was a "source of rising vulnerabilities":

> We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find

> widespread capability to exploit infrastructure vulnerabilities. The capability to do harm--particularly through information networks--is real; it is growing at an alarming rate; and we have little defense against it.[85]

While acknowledging that the majority of the nation's telecommunications assets and networks were owned by the private sector, Marsh stipulated that, for electronic commerce to flourish, the nation's information infrastructure must be made secure and reliable. And that, Marsh concluded, would only be practical as a joint government-private sector partnership:

> Protection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure information infrastructure requires the following:
>
> - Secure and reliable telecommunications networks;
> - Effective means for protecting the information systems attached to those networks;
> - Effective means for authenticating communications of trading partners, assuring the integrity of data and non-repudiation of transactions;
> - Effective means of protecting data against unauthorized use or disclosure;
> - Well-trained users who understand how to protect their systems and data.
>
> Strong encryption is an essential element for the security of the information on which critical infrastructure depends.[86]

The Commission's report recommended the establishment of key management infrastructures (KMIs) as the "only" way to enable encryption on

a national scale. Those KMIs must, the report concluded, include the development of appropriate standards for interoperability on a global scale and a key-escrow and recovery component needed to provide business and law enforcement access to data in the event encryption keys are lost or compromised.[87]

The Commission, acknowledging the public's reticence to trust government-escrowed, key-recovery programs, found that public confidence in key recovery would only be possible if stored encryption keys received the same legal protections and individual rights of redress when access is abused as other forms of protected communications (i.e., mail, telephone, wire transfers). This, the report summated, "should also be defined in law."[88]

CONGRESS--1997

S. 376: The Encrypted Communications Privacy Act of 1997

On 27 February 1997, Senator Patrick Leahy (D-VT) introduced S. 376, the Encrypted Communications Privacy Act (ECPA) to the Senate. S.376, which was co-sponsored by Senator Conrad Burns (R-MT), would ban government-mandated, key-recovery or key-escrow encryption policies of the Federal Government, ensuring that all computer users were free to choose any encryption method desired to protect the privacy of their own on-line transmissions and computer files.[89]

Following its introduction by Senator Leahy, ECPA was referred to the Subcommittee on Technology, Terrorism, and Government on 19 March

1997 and from there to the Senate Judiciary Committee on 9 July 1997. However, no further action was taken on the bill.

S. 377: The Promotion of Commerce On-Line in the Digital Era Act

In coordination with the introduction of ECPA, Senator Conrad Burns (R-MT) re-introduced the Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act. Co-sponsored by Senator Leahy of Vermont, Pro-CODE would restrict the Department of Commerce (NIST) from imposing government encryption standards intended for use by the private sector. Further, it would restrict the DOC from promulgating de facto standards through the use of export controls.[90]

In his remarks introducing S.377, Senator Burns pointedly reminded the Clinton Administration that the production and use of encryption products were not reserved for the United States alone:

> This legislation was drafted to not only address the concerns raised by industry but also to encourage law enforcement and national security officials to prepare themselves to do their job in an environment where strong encryption is everywhere. To date, the FBI/NSA/CIA have devoted heir efforts in this area to maintaining the status quo and hoping that strong encryption does not become worldwide. The evidence from the Commerce Department study conducted over a year ago, indicates that this has already taken place--the study identified 497-foreign made products that were capable of offering encryption in excess of that which domestic companies could export under the present export restrictions in 28 foreign countries.[91]

On 19 March 1997, Pro-CODE was referred to the Senate Commerce, Science, and Transportation Committee chaired by Senator John McCain (R-AZ). Subsequent to the referral, no further action was taken on the bill.

H.R.1903: The Computer Security Enhancement Act of 1997

In the House of Representatives on 17 June 1997, Congressman James Sensenbrenner (R-WI) introduced H.R.1903, the Computer Security Enhancement Act of 1997. The Act would update the Computer Security Act of 1987 (P.L. 100-235) and amend the National Institute of Standards and Technology Act, enhancing the ability of NIST to improve Federal computer security and to ensure that, "appropriate attention and effort is concentrated on securing [the] Federal Information Technology infrastructure."[92]

The bill would clarify that NIST standards and guidelines, used for the acquisition of computer security technologies, could not be used as de facto regulations to control the production or use of encryption technologies or products by the private sector. The bill would also enhance the role of the Independent Computer System Security and Privacy Advisory Board in NIST's decision-making process, by requiring the Board to make formal recommendations regarding proposed security standards and to provide guidance to NIST on emerging computer security issues.[93]

The bill was referred to the House Committee on Science on 17 June 1997 and placed with the Subcommittee on Technology on 23 June 1997. The Subcommittee held a hearing on the bill that same day and followed the

Subcommittee hearing with a Mark-up Session on 28 July 1997. The amended bill was returned to the House Committee on Science on 28 July 1997.

On 29 July 1997, the full Committee took up the bill for consideration. A second Mark-up Session was held that same day. The Committee then voted to order the bill, with one minor amendment, to be reported out to the House floor. On 3 September 1997, the House placed the bill on the Union Calendar (Calendar No. 139) and on 16 September 1997, the bill passed the House, as amended, by voice vote. On 17 September 1997, the Computer Security Enhancement Act of 1997 was referred to the Senate for consideration. The Senate chose to delay action on the bill during the balance of the 1997 term, deferring any action until 1998.

JUDICIARY--1997

***Bernstein v. Department of State*, 945 Federal Supplement 1279**

In the case of *Bernstein v. Department of State*, discussed earlier, the Clinton Administration was handed its second legal set back in its on-going battle to maintain tight export controls on data encryption software. In a motion for reconsideration and dismissal of an unfavorable 1996 ruling by the United States District Court for the Northern District of California in *Bernstein v. Department of State,* the Federal Government had argued that the release of encryption software could be regulated under existing export law.[94]

In the review of her original findings, District Court Judge Marilyn Patel, who had presided in the 1996 case, agreed with the government's contention that the regulation of software is not prohibited by law and that the First Amendment does not remove encryption technology entirely from all government regulation. However, Judge Patel further ruled that software code could be considered a form of speech and she again found in favor of Plaintiff Bernstein, affirming his right to publish scientific papers, algorithms, or computer program including those having to do with data encryption.

CLINTON ADMINISTRATION--1998

The Department of Defense: Establishment of PKI for DOD Supplier Base

In an effort to protect the integrity of information exchanges between the public and private sectors and to jump-start the development of a public-key recovery system, on 14 May 1998, the DOD announced its intention of requiring all its commercial supplier base to adopt a public-key recovery system for all transactions with the DOD. Because of its enormous procurement leverage, the DOD placed itself in the position of jump-starting Federal Government efforts to build and use strong PKI encryption. "Agencies cannot wait for the Government and industry to settle on a national policy," stated Deputy Defense Secretary John Hamre.[95]

In a major policy reversal, Hamre announced that the DOD was willing to cede the management of the keys and let an outside, third party serve as

the Certificate Authority, or key holder. But Hanre also called the on-going debate over encryption a "fraud." Key recovery, he said, would give the Federal Government no greater access to documents than it had presently. Hamre said industry must take the lead in implementing key-recovery systems, because the Federal Government could not, or would not, set the system requirements. The designs, he said, should be based on commercial applications.[96]

The White House: Changes to Encryption Export Policy

On September 14, 1998, the Clinton Administration amended its encryption policy by streamlining the export licensing approval process for computer products employing the 56-bit Data Encryption Standard (DES). The change allowed multinational companies to begin passing relatively secure information across the Internet or via company-internal, private intranets using standards-based, 56-bit algorythms.[97]

The policy change also permitted the export of unlimited strength encryption products, such as those based upon 128-bit algorythms, which had yet to be broken, to:

- Subsidiaries of United States firms, worldwide (except those doing business in the seven Tier IV terrorist nations);
- Insurance companies to the same 45 countries recently approved for exports to banks and financial institutions;
- Health and medical organizations (including civilian government health agencies) in the same 45 countries.

Does not include biochemical/pharmaceutical manufacturers;

- On-line merchants for client-server applications, in the same 45 countries, with the purpose of securing electronic transactions between merchants and their customers. Does not include manufacturers and distributors of items controlled on the U.S. munitions list.[98]

The new policy eliminated any requirement for key-recovery planning entirely.[99]

In reflecting on the recent Clinton Encryption Export policy changes, on 16 September 1998, Vice President Al Gore, citing the difficulties in balancing national security and law enforcement needs with the rights of the individual, made the following observations during a press briefing at the White House:

> Some of you who have followed this issue know that it is probably one of the most difficult and complex issues that you can possibly imagine. But we've made progress, and we're here this morning to announce an important new action that will protect our national security and our safety, and advance our economic interests and safeguard our basic rights and values in this new Information Age.[100]
>
> Balancing these needs is no simple task, to say the least. That is why, in taking the next step toward meeting these complex goals, we worked very closely with members of Congress from both parties, House and Senate; with industry; with our law enforcement community and with our national security community. And as we move forward we want to keep working closely with all who share a stake in this issue--especially law enforcement--to constantly assess and reassess the effectiveness of our actions in this fast changing medium.[101]
>
> Beginning today, American companies will be able to use encryption programs of unlimited strength when communicating between most countries. Health, medical, and insurance

> companies will be able to use far stronger electronic protection for personal records and information. Law enforcement will still have access to criminally related information under strict and appropriate legal procedures. And we will maintain our full ability to fight terrorism and monitor terrorist activity that poses a grave danger to American citizens.[102]
>
> With this new announcement, we will protect the privacy of average Americans, because privacy is a basic value in the Information Age, indeed in any age. We will give industry the full protection that it needs to enable electronic commerce to grow and to thrive. And we will give law enforcement the ability to fight 21st century crime with 21st century technology, so our families and businesses are safe, such as privacy and safety.[103]

NIST Encryption Product Certification Under FIPS 140-1

On 26 October 1998, NIST announced the first certification of commercial hardware and software encryption products compliant with Federal Information Processing Standard 140-1. The FIPS 140-1 standard specified requirements that cryptographic modules must meet for handling unclassified information. Under FIPS 140-1, Federal agencies must use certified products on networks that encrypt information unless they obtain a waiver from NIST.[104]

The nFast Cryptographic Accelerator from nVipher Inc. of Andover, MA gained its initial certification in September 1998 ; the SmartGate virtual private network client from V-One Corp. of Germantown, MD received its certificate in October 1998.[105]

CONGRESS--1998

Computer Security Enhancement Act of 1997--Senate Action

In the Senate, the Computer Security Enhancement Act of 1997 was referred to the Committee on Commerce, Science, and Transportation chaired by Senator John McCain (R-AZ). A Science, Technology, and Space Subcommittee hearing, Chaired by Senator William Frist (R-TN), was held on 10 February 1998. On 1 October, the full Committee met in open executive session and by voice vote, ordered H.R. 1903 to be reported out of Committee without amendment[106].

In a letter dated 8 October 1998, Congressional Budget Office Director June E. O'Neill reported to Senator McCain that the anticipated cost to NIST of implementing the mandatory provisions of H.R.1903 would be $13 million over the bill's five-year life (1999 to 2003). On 13 October 1998, Senator McCain reported the bill out of Committee to the full Senate under written report No. 105-412. The bill was subsequently placed on the Senate Legislative Calendar (Calendar No. 718) under General Orders of 13 October 1998. No further action was taken on the bill.[107]

CLINTON ADMINISTRATION--1999

Preserving America's Privacy and Security in the Next Century: A Strategy For America in Cyberspace

On 16 September 1999, the seminal event of the Clinton Administration's seven year battle over encryption policy occurred with the

publication of, "Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace." Co-signed by Secretary of Defense William Cohen, Attorney General Janet Reno, Secretary of Commerce William Daley, and OMB Director Jacob Lew, this document reversed four decades of United States Government encryption policy by removing virtually all prohibitions on the use, sale, or export of encryption products. In explanation, the preamble of the document set the stage in the following manner:

> The Federal Government has sought to maintain a balance between privacy and commercial interest on the one hand and public safety and national security concerns on the other by limiting the export of strong encryption software. Preserving the balance has become increasingly difficult with the clear need for strong encryption for electronic commerce, growing sophistication of foreign encryption products and the proliferation of software vendors, and expanded distribution mechanisms. In the process, all parties have become less satisfied with the inevitable compromises that have had to be struck. United States companies believe their markets are increasingly threatened by foreign manufacturers in a global economy where businesses, consumers, and individuals demand that strong encryption be integrated into computer systems, networks, and applications. National security organizations worry that the uncontrolled export of encryption will result in diversion of powerful tools to end users of concern. Law enforcement organizations see criminals increasingly adopting tools that put them beyond the reach of lawful surveillance.[108]

With this introduction, the national policy paper proposed a "new paradigm" to address the national security and privacy interests of the United States based upon, "three pillars--information security and privacy; a new framework for export controls; and updated tools for law enforcement."[109]

In the areas of data security and information privacy, the new Clinton Administration policy would be a radical departure from previous encryption policy positions:

> In updating enduring constitutional values for the computer age, we need to ensure that our citizens' personal data and communications are appropriately protected. Businesses need to privately communicate with their employees and manufacturing partners without risk that their proprietary information will be compromised through unauthorized access. Encryption is one of the necessary tools that can be used in this technological environment to secure information. Therefore, we encourage the use of strong encryption by American citizens and businesses to protect their personal and commercial information from unauthorized and unlawful access.[110]

On the subject of encryption exports, the new policy was again a significant departure from the "absolutes" established previously as policy underpinnings by the Clinton Administration:

> Encryption products and services are needed around the world to provide confidence and security for electronic commerce and business. With the growing demand for security, encryption products are increasingly sold on the commodity market, and encryption features are embedded into everyday operating systems, spreadsheets, word processors, and cell phones. Encryption has become a vital component of the emerging global information infrastructure and digital economy. In this new economy, innovation and imagination are the engines, and it is economic achievement that underpins America's status in the world and provides the foundation for our national security. We recognize that United States information technology companies lead the world in product quality and innovation, and it is an integral part of the Administration's policy of balance to see that they retain their competitive edge in the international marketplace.[111]
>
> Accordingly, the Administration has revised its approach to encryption export controls by emphasizing three simple

> principles that protect important national security interests: a meaningful technical review of encryption products in advance of sale, a streamlined post-export reporting system that provides us an understanding of where encryption is being exported but is aligned with industry's business and distribution models, and a license process that preserves the right of government to review and, if necessary, deny the sale of strong encryption products to foreign government and military organizations and to nations of concern.[112]

In addressing the third of the three pillars of the new policy, the Clinton Administration called upon Congress to support necessary changes in the law to ensure:

> That law enforcement maintains its ability to access decryption information stored with third parties, but only pursuant to rules that ensure appropriate privacy protections are in place. The Administration and Congress must develop legislation to create a legal framework that enhances privacy over current law and permits decryption information to be safely stored with third parties, but allows for law enforcement access when permitted by court order or some other appropriate legal authority.[113]

In addition, in announcing its new encryption policy, the Clinton Administration served notice on Congress that these policy concessions would come at a price:

> Since criminals will not always store keys with third party recovery agents, we must ensure that law enforcement has the personnel, equipment, and tools necessary to investigate crime in an encrypted world. This requires that the Congress fund the Technical Support Center as proposed by the Administration to ensure that the confidentiality of the sources and methods developed by the Technical Support Center can be maintained.[114]

Finally, the Clinton Administration looked to the private sector to fulfill the last condition for change to the long-standing encryption policy:

> It is well recognized that industry is designing, deploying, and maintaining the information infrastructure, as well as providing encryption products for general use. Industry has always expressed support, both in word and in action, for law enforcement, and has itself worked hard to ensure the safety of the public. Clearly, industry must continue to do so, and firms must be in a position to share proprietary information with the government without fear of that information's disclosure or that they will be subject to liabilities. Therefore, the law must provide protection for industry and its trade secrets as it works with law enforcement to support public safety and national security. The law must assure that sensitive investigative techniques remain useful in current and future investigations by protecting them from unnecessary disclosure.[115]

White House: Update to Computer Export Policy

In concert with the radical changes announced to long-standing United States Encryption Export policy, on 26 November 1999, the Clinton Administration announced a major revision to United States export policy for general purpose microprocessors. The decision would raise the export limit for multipurpose computers from 1900 MTOPS and 3500 MTOPS. The Administration's decision was predicated on reaching a general agreement among the United States export community, i.e., the Departments of State, Commerce Defense, Energy, and the Arms Control Agency, that "mass market" microprocessors were not controllable due to their wide-spread use in virtually all consumer and business computers; that they are highly portable; and that they are sold in very large quantities through multiple distribution channels. The change was made in recognition of the rapid increases in microprocessor technology and computational power.[116]

S. 798: Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act

On 14 April 1999, Senator John McCain (R-AZ), Chairman of the Senate Commerce, Science, and Transportation Committee and long-time proponent of export controls on encryption products, joined with Senators Patrick Leahy (D-VT), Ronald Wyden (D-OR), and Conrad Burns (R-MT) in sponsoring S. 798, the Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act. S. 798 would promote electronic commerce by encouraging and facilitating the use of encryption in the transaction of interstate commerce, consistent with the preservation of national security protections. In announcing his support for the bill, Senator McCain said:

> This bill protects our national security and law enforcement interests while maintaining the U.S. leadership role in information technology. The PROTECT Act would establish a credible procedure for making encryption export decisions, while providing a national security backstop to make certain that advanced encryption products do not fall into the wrong hands.[117]

Senator Burns, a long-time Senate champion and advocate of the rights of the private sector to develop and employ strong encryption in support of electronic commerce on the Internet, rose in support of Senator McCain's bill, stating:

> Mr. President, as the Members of the Senate know, for several years I have advocated the enactment of legislation that would facilitate the use of strong encryption. Beginning in the 104th

Congress, I have introduced legislation that would ensure that the private sector continues to take the lead in developing innovative products to protect the security and confidentiality of our electronic information including the ability to export such American products.

I am pleased to rise today to introduce with my Chairman, Senator McCain, the PROTECT Act of 1999. The bill reflects a number of discussions we have had this year about the importance of encryption in the digital age to promote electronic commerce, secure our confidential business and sensitive personal information, prevent crime and protect our national security by protecting the commercial information systems and electronic networks upon which America's critical infrastructures increasingly rely. I am extremely pleased to join him in introducing this important legislation.

While this bill differs in important respects from the PRO-CODE legislation I introduced in the previous Congress, I do think it accomplishes a number of very important objectives. Specifically, the bill:

- Prohibits domestic controls on encryption products and their use;

- Guarantees that American industry will continue to be able to come up with innovative products;

- Permits the immediate exportability of 128-bit encryption in recoverable encryption products and in all encryption products to a broad group of legitimate and responsible commercial users to users in allied countries;

- Recognizes the futility of unilateral export controls on mass market products and where there are foreign alternatives and so permits the immediate exportability of strong encryption products whenever a public-private advisory board and the Secretary of Commerce determines that they are generally available, publicly available, or available from foreign suppliers;

- Directs NIST to complete establishment of the Advanced Encryption Standard with 128 bit key lengths (the DES

successor) by 1 January 2002 (and ensures that it is led by the private sector and open to public comment;

- Decontrols thereafter products incorporating the AES or its equivalent.[118]

The bill would permit the export of products based on 64-bit encryption technology, a modest enhancement of the 56-bit limitation currently allowed under Clinton Administration export rules. The bill would also prohibit the Federal Government from establishing any conditions or standards requiring that decryption keys, access to keys, key recovery information, or any other plain text access capability be built into commercial software as a condition for licensing, selling, or exporting the software commercially.[119]

The bill would not prohibit law enforcement or the intelligence community, from gaining access to the encrypted communications or information under existing security statutes.[120] The bill would also prohibit the Secretary of Commerce from establishing or enforcing any regulations that would indirectly impose Federal Government-designed encryption standards on the private sector by restricting the export of encryption products.[121] It would also limit the Federal authority to those products used by computer systems operated by the Federal Government, but would require that those products be interoperable with other commercially available encryption products.[122]

An amendment to the bill, offered by Senator John Kerry (D-MA) and approved in conjunction with the McCain bill by the Senate Commerce,

Science, and Transportation Committee, would establish an Encryption Export Advisory Board that would oversight and continuously review encryption export limits.[123] The 12-member board would be composed of representatives from industry, the Secretary of Commerce, the National Security Agency, the Federal Bureau of Investigation, and the Central Intelligence Agency.[124]

The bill would also require NIST to complete its evaluation and selection of one or more private-sector developed, Advanced Encryption Standard (AES) products, no later than 1 January 2002. NIST had initiated the AES search and selection process on 2 January 1997.[125]

S.798 was referred to the Committee on Commerce on 14 April 1999. On 10 June 1999, the Committee held hearings on the proposed bill. In testimony before the Committee, Justice Department officials reported that DOJ advocacy remained with the promotion of recoverable encryption products:

> Given both the benefits and the risks posed by encryption, the Department of Justice believes that encouraging the use of recoverable products is an important part of the Administration's balanced encryption policy.[126]

By "encouraging," the Committee inferred that the DOJ meant requiring the use of specified recoverable products for private citizens and businesses to interoperate with government computers and networks. To Congress, this effectively represented a "backdoor" Federal mandate, compelling the private sector to use only those encryption products for which

the government could escrow the keys. The effect of such a mandate would be to dramatically skew the marketplace and to impose substantial cost impacts on the private sector for those individuals and commercial businesses required to reconfigure their existing systems to comply with the Federal edict.[127]

In response, the Committee ordered the review of the findings of a 1996 report on encryption, authored by Kenneth W. Dan and Herber S. Lin of the National Research Council (NRC), which stated, in part:

> If encryption can protect trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States. [128]

The Committee also reviewed data extracted from the 1995 Annual Report on Foreign Economic Collection and Industrial Espionage prepared by the National Counterintelligence Center (NCC). The NCC findings were summarized in the following exert from the Annual Report:

> Industrial espionage poses a critical problem in a global marketplace. The National Counterintelligence Center has concluded that 'special technical operations (including computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses) account for the largest portion of economic and industrial information lost by United States corporations.[129]

Finally, the Committee elicited testimony from a number of encryption experts representing the private sector. One such expert was David Aucsmith, Chief Security Architect for the Intel Corporation, who testified:

> Information security is critical to the integrity, stability and health of individuals, corporations, and government. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime and sabotage through these networks. The security of any network, however, is only as good as its weakest link. America's infrastructure cannot be protected if they are networked with foreign infrastructures using weak encryption.[130]

The bill was reported out of Committee on 5 August 1999 (Report. No.106-142). It was placed on the Senate Legislative Calendar under General Orders Calendar No. 263. No further action was taken on this bill.[131]

H.R. 850: Security and Freedom Through Encryption (SAFE) Act

On 25 February 1999, Representative Robert Goodlatte (R-VA) introduced H.R. 850, the House version of S.798. H.R. 850, the Security and Freedom through Encryption (SAFE) Act, would amend the federal criminal code to permit any person within any state and any United States citizen in a foreign country to use and sell any encryption product regardless of the algorithm selected, key length chosen, or implementation technique-to-medium used. The bill would direct the President to control the export of dual-use encryption products and to deny any export that is found to be contrary to United States security interests. Like S.798, H.R.850 would also

direct the National Institute of Standards and Technology to have an advanced encryption standard selected and in place by January 1, 2002.[132]

H.R.850 was referred to the House Judiciary Committee, Subcommittee on Courts and Intellectual Property, on 3 March 1999. A Subcommittee hearing on the bill has held the following day, 4 March 1999, in Room 2226 of the Rayburn House Office Building. Government witnesses included the Honorable William Reinsch, Undersecretary of Commerce for Export Administration, United States Department of Commerce; the Honorable Ronald D. Lee, Associate Deputy Attorney General, United States Department of Justice; and the Honorable Barbara McNamara, Deputy Director, National Security Agency.[133]

Secretary Reinsch testified first. He observed that the policy issue had progressively evolved since he last testified to the Congress on the subject in September 1997. He reiterated existing Clinton Administration policy, saying:

> Developing a new encryption policy has been complicated because we do not want to hinder its legitimate use--particularly for electronic commerce; yet at the same time we want to protect our vital national security, foreign policy, and law enforcement interests. We have concluded that the best way to accomplish this was to continue a balanced approach: to promote the development of strong encryption products that would allow lawful government access under carefully defined circumstances; to promote the legitimate uses of strong encryption to protect confidentiality; and continue looking for additional ways to protect law enforcement and national security interests.[134]

Associate Deputy Attorney General Lee testified that the DOJ continued to be concerned with the implications of strong encryption on the

ability of the law enforcement community to prevent the commission of crimes:

> We have the responsibility for preventing, investigating, and prosecuting serious criminal and terrorist acts when they are directed against the United States. We are gravely concerned that the proliferation and use of non-recoverable encryption by criminal elements would seriously undermine these duties to protect American people, even while we favor the spread of strong encryption products that permit timely and legal law enforcement access and decryption.[135]

NSA Deputy Director McNamara's testimony strongly echoed that of her Clinton Administration colleagues. In explaining how her agency intercepts encrypted communications signals from foreign adversaries, unscrambles them and prepares intelligence reports for United States decision makers and military commanders, McNamara stated:

> Very often, time is of the essence. Intelligence is perishable; it is worthless if we cannot provide it in time to make a difference in rendering vital decisions... While our mission is to provide intelligence to help protect the country's security, we also recognize that there must be a balanced approach to the encryption issue. The interests of industry and privacy groups, as well as the government, must be taken into account. Encryption is a technology that will allow our citizens to fully participate in the 21st Century world of electronic commerce. It will enhance the economic competitiveness of United States industry. It will combat unauthorized access to private information and it will deny adversaries from gaining access to United States information wherever it may be in the world.[136]
>
> The SAFE Act will harm national security by making NSA's job of providing vital intelligence to our leaders and military commanders, difficult, if not impossible, thus putting our nation's security at risk. Our nation cannot have an effective decision-making process, or a strong fighting force, or a responsive law enforcement community unless the intelligence information required to support them is available in time to

> make a difference. The nation needs a balanced encryption policy that allows United States industry to continue to be the world's technology leader, but that policy must also protect our national security interests.[137]

Following the testimony of the three Administration witnesses, Chairman Hyde empanelled seven private sector-experts to testify. They included Thomas Parenty, Director, Data and Communications Security, Sybase, Inc.; Craig McLaughlin, Chief Technology Officer, Privada; Grover Norquist, President, Americans for Tax Reform; Dorothy E. Denning, Professor, Computer Science Department, Georgetown University; Alan Davidson, Staff Counsel, Center for Democracy and Technology; and Ed Gillespie, Executive Director, American for Computer Privacy.[138]

Craig McLaughlin, summarizing testimony from the other industry panelists, said:

> The current policy of restricting encryption exports is, I respectfully submit, outdated and counterproductive. The Administration's approach to encryption exports, like others before it, has sought to balance the needs of law enforcement and national security with the needs of Internet users, but instead has only created a situation in which United States industry is at a competitive disadvantage to its foreign counterparts, where online communications and transactions may remain vulnerable, where users do not have robust tools to protect their privacy and that ultimately threatens to undermine our technological leadership in this critical area.[139]

On 11 March 1999 and again on 24 March 1999, the Subcommittee on Courts and Intellectual Property met in open session to discuss H.R. 850. Successful Subcommittee mark-up sessions on 11 and 24 March 1999 resulted in the bill being forwarded to the full Committee on Government

Reform and Oversight by virtue of majority voice vote on 24 March 1999. While the bill was in Committee, Committee Chairman Henry Hyde (R-IL) requested that the Congressional Budget Office prepare a cost estimate for H.R.850's implementation. In his response dated 21 April 1999, CBO Director Dan Crippen reported that H.R.850 would cost the DOJ up to $3-5 million annually to fund the additional "administration of justice" functions mandated by the bill.[140]

Upon receipt of the CBO estimate, a full Committee mark-up session was conducted and the bill was reported out of Committee on 24 March 1999. On 27 April 1999, the bill was referred concurrently to four separate committees, each having partial jurisdiction over portions of the bill: the House International Relations Committee, the House Armed Services Committee, the House Commerce Committee, and the House Committee on Intelligence. The House International Relations Committee referred the bill to the Subcommittee on International Economic Policy and Trade for hearings on 19 May 1999. A Subcommittee mark-up session on 19 May 1999 was followed by a full Committee mark-up session and vote on 13 July 1999. The bill was ordered favorably reported out of Committee on a 33-5 vote.[141]

The House Committee on Armed Services requested Executive Comment on the bill from the Defense Department on 1 June 1999 and held two Committee hearings on the bill on 1 and 12 July respectively, before reporting it favorably out of Committee on a 47-6 vote.[142]

The House Committee on Commerce referred the bill to its Subcommittee on Telecommunications, Trade, and Consumer Protection on 5 May 1999, where hearing were held on 16 June 1999. Following a mark-up session on that same day, the bill was forwarded to the full Committee on 16 June 1999 by virtue of a voice vote. The House Commerce Committee conducted its own mark-up session on 23 June 1999, during which the bill was amended and then approved by the Committee, also on a voice vote.[143]

On 27 April 1999, the House Select Committee on Intelligence requested and was granted an extension for further consideration of the bill until 2 July 1999. A subsequent request for additional time for consideration of the bill was requested on 2 July 1999 and granted until 23 July 1999. During this extension, the Committee failed to hold hearings on the bill. Hoever, the Committee did act on the bill, reporting it out of Committee, as amended, on 23 July 1999 (House Rept. 106-117, Part V). The bill was placed on the House Union Calendar (Calendar No. 149) on 23 July 1999.

While both H.R.850 and S.798 would permit the exportation of encryption products, they differed on key recovery and key escrow issues, which S.798 favored and H.R. 850 opposed. For commercial software companies, mandating the escrowing of encryption keys continued to be an extremely onerous point of contention. Congressman Goodlatte observed:

> I thought the administration had finally begun to realize that American citizens and businesses would not tolerate Big Brother holding the keys to their private and proprietary information. These new draft regulations indicate just the

> opposite. Mandatory key escrow is a digital dog that just won't hunt. Software companies must have the freedom to develop products with strong security features to meet customer demands and privacy concerns in the United States and abroad.[144]

S. 854: The Electronic Rights for the 21st Century Act

Concurrent with the introduction of S.798, Senator Patrick Leahy (D-VT) introduced S.854, the Electronic Rights for the 21st Century Act, on 21 April 1999. The bill was designed to afford protection from the unwarranted interception and decryption--including by the Federal Government--of encrypted or otherwise electronically protected data and messaging, authored or exchanged by United States citizens via electronic media. The bill would also affirm the rights of United States citizens to employ and sell encryption products as a tool for securing personal on-line privacy, and for other purposes. Section 201, Freedom to Use Encryption, of the proposed bill states:

> It shall be *lawful* for any person within the United States, and for the United States person in a foreign country, to use, develop, manufacture, sell, distribute, or import any encryption product, regardless of the encryption algorithm selected, encryption key length chosen, existence of key recovery or other plaintext access capability, or implementation or medium used.[145]

The bill was read twice on the Senate floor, then was referred to the Senate Judiciary Committee. As of 21 April 1999, no further action was taken to advance the bill out of Committee.

H.R. 2413: The Computer Security Enhancement Act of 1999

On 1 July 1999, Congressman F. James Sensenbrenner, Jr. (R-WI) introduced H.R. 2413, the Computer Security Enhancement Act of 1999. The bill would amend the National Institute of Standards and Technology Act by directing NIST to coordinate efforts with the private sector in establishing voluntary interoperable standards for the establishment of non-Federal, public-key infrastructures (PKI). The PKI established could then be certified for use in communicating with and conducting business with the Federal Government.[146]

In his remarks introducing H.R. 2413 to the House floor, Congressman Sensenbrenner outlined the seven key features of the bill:

> Mr. Speaker, I am pleased to introduce, H.R. 2413, the Computer security Enhancement Act of 1999, a bipartisan bill to address our government's computer security needs. The bill amends and updates the Computer Security Act of 1987 which gave the National Institute of Standards and Technology (NIST) the lead responsibility for developing security standards and technical guidelines for civilian government agencies' computer security. Specifically, the bill:
>
> - Reduces the cost and improves the availability of computer security technologies for Federal agencies by requiring NIST to promote Federal use of off-the-shelf products for meeting civilian agency computer security needs;
>
> - Enhances the role of the independent Computer System Security and Privacy Advisory Board in NIST's decision-making process. The board, which is made up of representatives from industry, Federal agencies, and other outside experts, should assist NIST in its development of standards and guidelines for Federal systems;

- Requires NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products. Through such tests and procedures, NIST, with assistance from the private sector, will be able to judge the relative strength of foreign encryption, thereby defusing some of the concerns associated with the export of domestic encryption products;

- Clarifies that NIST standards and guidelines are to be used for the acquisition of security technologies for the Federal Government and are not intended as restrictions on the production or use of encryption by the private sector;

- Requires the National Research Council to conduct a study to assess the desirability of creating public-key infrastructures. The study will also address advances in technology required for public key in technology required for public-key infrastructure;

- Establishes a national panel for the purpose of exploring all relevant factors associated with the development of a national digital signature infrastructure based on uniform standards and of developing model practices and standards associated with certification authorities (CAs).[147]

The bill would direct and require NIST to evaluate and test commercially available security products, including foreign encryption products. The bill would also require the Under Secretary of Commerce for Technology to promote the widespread use of cryptography applications as a means of enhancing the security of the nation's critical information infrastructures. The bill would also establish a centralized Federal clearinghouse for the collection and dissemination to the public of information to promote awareness of information security threats. The bill would also promote the development of a national standards-based infrastructure needed to support commercial and private uses of encryption technologies

for confidentiality and authentication. At the same time, the bill would prohibit NIST from promulgating or adopting standards or engaging in security practices that would create a de facto Federal encryption standard, that would then be required for use in computer systems other than Federal Government computer systems.[148]

The bill was originally referred to the House Committee on Science, which in turn referred it to the Subcommittee on Technology for consideration on 30 September 1999. Hearings on the bill were conducted by the Subcommittee on Technology on 14 October 1999. On 20 October 1999, the Subcommittee on Technology conducted a Mark-up Session before returning the bill to the full Committee (amended), where it was approved by a voice vote. No further action was taken on the bill.[149]

H.R. 2616: Encryption for the National Interest Act

On 27 July 1999, Representative Porter J. Goss (R-FL) introduced H.R. 2616, the Encryption for the National Interest Act. H.R. 2616 would make it lawful for any person within the United States and any United States citizen to use any encryption product, regardless of the encryption algorithm utilized in the product, the encryption bit length employed, or the implementation technique or medium used.[150]

H.R. 2616 would make it unlawful for any person to intentionally use decrypted information, or break the encryption code of another person without legal authorization, or to impersonate another person for the purpose

of obtaining decryption information belonging to that individual (again, without legal authority). The bill would also make it a violation of Federal law for an individual to facilitate the encryption of data, knowing that the data would be used in the furtherance of a crime, or to disclose decryption information in violation of law.[151]

On 27 July 1999, H.R. 2616 was referred simultaneously to the Committees on the Judiciary, on International Relations, and on Government Reform for consideration of those provisions falling within the jurisdiction of each of the three committees. The House Judiciary Committee referred the bill to its Subcommittee on Courts and Intellectual Property on 30 July 1999. The House Committee on International Relations referred the bill to its Subcommittee on International Economic Trade Policy and Trade on 1 September 1999. The House Government Reform Committee referred the bill to its Subcommittee on Government Management, Information and Technology on 23 August 1999. None of the committees reported the bill out, effectively killing it.[152]

H.R. 2617: Tax Relief for Responsible Encryption Act of 1999

On 27 July 1999, Representative Porter J. Goss (R-FL) also introduced H.R 2617, the Tax Relief for Responsible Encryption Act of 1999, a bill to amend the Internal Review Code of 1986 and allow a tax credit for the development cost of encryption products having an automated plain text encryption/de-encryption capability. The development of such a security

product would enable a user to send and receive plain text data that could be encrypted and de-encrypted automatically, without user intervention. The bill would provide the developer a tax credit equal to fifteen percent of the developer's encrypted product-plain text development costs during the development tax year.[153]

H.R. 2617 was referred to the House Ways and Means Committee for review. No further action was taken on the bill.[154]

JUDICIARY--1999

***Bernstein v. Department of State*, US Ninth Circuit Court of Appeals, San Francisco, California**

In the third in a series of legal set backs for the Clinton Administration's Encryption Export policy, a three-judge panel of the United States Ninth Circuit Court of Appeals in San Francisco, California, ruled against the Federal Government in its appeal of a 1997 District Court judgment in the case of *Bernstein v. Department of State*. On 6, May 1999, the United States Ninth Circuit Court of Appeals upheld the ruling of United States District Court Judge Marilyn Patel of the Northern District of California. In a 2-1 majority decision, the Court of Appeals affirmed that government efforts to block the export of data-scrambling encryption software was an unconstitutional restraint of free trade. Writing for the majority, Judge Betty Fletcher stated:

> Cryptography should not merely be a state secret, but also a protector of the people's privacy. Government attempts to

> control encryption may well implicate not only First Amendment rights of cryptographers, but also the constitutional rights of each of us as potential recipients of encryption's bounty.[155]

CLINTON ADMINISTRATION--2000

The White House: Update to Computer Export Policy

In July 1999, President William Clinton directed his Administration to conduct a review of United States computer export controls, taking into account advancements in computing technology since mid-1999, United States national security interests, and the need to evolve a policy that would remain in effect for at least six months.[156]

On 1 February 2000, President Clinton announced yet another update in a series of Clinton Administration computer export policy revisions. The revised controls maintained the four country groups (Tier I-IV) announced in 1995, but amended the countries in and control levels for the four groups as follows:

- Tier I (Western Europe, Japan, Canada, Mexico, Australia, New Zealand, Hungary, Poland, the Czech Republic and Brazil): Exports without an individual license are permitted for all computers (i.e., there is no prior government review);

- Tier II (South and Central America, South Korea, ASEAN, Slovenia, most of Africa): Exports without an individual license are permitted up to 20,000 MTOPS with record-keeping and reporting as directed; individual licenses (requiring prior government review) are needed above 20,000 MTOPS;

- Tier III (India, Pakistan, all Middle East/Maghreb, the former Soviet Union, China, Vietnam, Central Europe): Based on President Clinton's July 1999 decision, exports are

permitted without and individual license up to 6,500 MTOPS, and require individual licenses for military end-uses and end-users above that figure. Exports without an individual license are permitted for civil end-users between 6,500 MTOPS and 12,300 MTOPS, with exporter record keeping and reporting as directed. Individual licenses are required for all end-users above 12,300 MTOPS;

- Tier IV (Iraq, Iran, Libya, North Korea, Cuba, Sudan, and Syria): There are no planned changes for Tier IV. Current policies remain in effect (i.e., the United States will maintain a virtual embargo on computer exports).[157]

The 1 February 2000 decision raised the Tier II individual licensing level from 20,000 MTOPS to 33,000 MTOPS. Further, the President's decision promoted Romania from a Tier III country to a Tier II country. It would also maintained a separate two-tier system for civilian and military/proliferation end-users. The President's decision raised the individual licensing levels from 6,500 to 12,500 MTOPS for military end-users and from 12,300 to 20,000 MTOPS for civilian end-users.[158]

President Clinton, in announcing his decision to amend the export controls on United States high-performance computers (HPCs), said:

> Today, based on the recommendations I have received from agencies as a result of their review, I am announcing additional reforms to United States export controls on HPCs. This decision reflects my commitment to a control system that will enhance United States national security by implementing controls on computer exports that are effective and enforceable.

> I have decided to raise the licensing threshold for HPC exports to Tier II countries. I have decided also to raise the licensing threshold for Tier III countries and the threshold above which proposed exports to Tier III countries must be notified to United States Government export control agencies, and to adjust the Tier III country grouping. The Administration will continue its policy of maintaining a lower threshold for military end-users than civilian end-users. Export control agencies will examine the benefits of maintaining a civilian/military differential in the course of their next review of HPC levels. Due to the ever-increasing rate of technological change, agencies will review control levels by April 2000 to determine if further changes are warranted.[159]

Critical Information Assurance Office (CIAO): *Practices for Securing Critical Information Assets*

In January 2000, the Critical Information Assurance Office published, *Practices for Securing Critical Information Assets.* The guide was created by the Clinton Administration to aid and assist Federal Government personnel in the development and implementation of information security policy. Information security policy, as defined in the document, refers to the set of rules and practices used to manage and protect organizational information resources. This definition of the term "policy" is consistent with the definition found in the December 1998 NIST publication, *Guide for Developing Security Plans for Information Technology Systems:*

> In discussions of computer security, the term policy has more than one meaning. Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to specific security rules for particular systems. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting and organization's email privacy policy or fax security policy.[160]

Practices for Securing Critical Information Assets defines program policy development and promulgation as the, "responsibility of senior management under the direction of the agency head or senior administration official responsible for the agency." For critical information security policy, *Practices for Securing Critical Information Assets* points to the Computer Security Act of 1987 (P.L. 100-235); OMB Circular A-130, *Management of Federal Resources* (8 February 1996), and PDD-63, *Protecting America's Critical Infrastructures* (22 May 1998). The *Guide* defines system-specific policy development as, "platform by platform rules for securing access to critical information." Issue-specific policy is defined as "the set of guidelines that govern access, use, and common sense protection of agency computer information assets."[161]

To establish a framework for specifying security requirements for agency computer systems and Information Technology products and for their evaluation in practice, CIAO's *Practices for Securing Critical Information Assets* offers a Common Criteria Standard. The Common Criteria Standard is an international standard developed by the National Information Assurance Partnership (NIAP), a 1999 joint venture of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The standard provides a framework by which commercial companies can have security product tested by a third party and, if desired, obtain a certificate of validation by the NIAP.[162]

Chapter III, of *Practices for Securing Critical Information Assets*, entitled, "Tools and Practices for Critical Information Asset Protection," is devoted to physical and information security tools and practices. Physical security, defined by *Practices for Securing Critical Information Assets* as, "guns, gates, and guards," is identified as the first line of defense against unauthorized computer system access:

> The measures discussed may seem simple and obvious, but they are essential. If you must choose, make the investments needed to physically secure your site before buying high-cost information security tools. Shortchanging physical security is like equipping your car with state-of-the-art technology—then walking away and leaving your keys in the ignition and the doors unlocked.[163]

Information security is identified by *Practices for Securing Critical Information Assets* as those technology measures employed to ensure computer system information assurance:

> Information security measures are intended to protect data and software against nonphysical threats, including unauthorized access, compromise of data integrity, and denial or disruption of service (for example, an attack via the Internet). They include software and electronic tools installed at various points in the client-server architecture (firewalls, intrusion detection systems, and antivirus software), sound access control practices (password requirements, limiting access to sensitive information, and the like), and *encryption*.[164]

Cryptography, the science of transforming or encrypting plaintext data in a manner that makes the data interpretable by authorized persons only, is accomplished through the application of complex mathematical formulae, or algorithms, to the data. The algorithm creates a pattern by which each plain

text letter or number is substituted with a series of randomly generated characters. The transformed, encrypted plaintext is only decipherable by someone who knows the algorithmic key. [165]

Symmetric-key cryptography employs a single mathematical key to encrypt and decrypt plaintext data. Asymmetric, or public-key cryptography, employs the use of unique number pairs such that data encrypted by one member of the pair can only be decrypted by the other member of the pair, and no other number. If the numbers are large enough, it is extremely difficult to derive one of the numbers, even by a supercomputer and even when the other number of the pair is known. But asymmetric encryption is too slow for practical use with large sets of data. However, a hybrid system, employing symmetric encryption for encoding the data set, and asymmetric encryption to encode the symmetric encryption key and embed it as a component of the asymmetrically-encrypted message header, is the basis for modern cryptography.[166]

The most popular symmetric-key encryption algorithm in use today is a variant of the Data Encryption Standard (DES) adopted by NIST as the Federal standard in 1976 and by the American National Standards Institute (ANSI) as the commercial standard in 1981. The DES variant, known as Triple-DES, operates on a block of data three times with two separate keys: first, with the first key, then the second, and then again with the first key. Triple-DES will be replaced by a next-generation, symmetric-key encryption

standard, or Advanced Encryption Standard (AES) by NIST within the next several years.[167]

Until 2000, the most widely used, asymmetric-key encryption algorithm in use was proprietary to RSA, a commercial software security company. RSA's patented algorithm was one of very few asymmetric-key algorithms capable of providing both a digital signature and encryption service from the same mathematical formula. The patent issue created a barrier to more widespread use of the RSA algorithm (i.e, RSA could charge a royalty for every public/private key pair generated by the patented algorithm). However, the patent expired in 2000, creating a flood of orders for RSA's product from the Federal Government.[168]

Appendix D of *Practices for Securing Critical Information Assets*, entitled Cryptographic Technology Deployment Issues, provides guidelines for addressing the twin issues of trusted Certification Authorities (CAs), and the evolution of de facto Public-Key Cryptography Standards, both necessary for universal applicability of the Federal Government's public-key encryption approach.[169]

The establishment of a Certification Authority (CA) is necessary to support the widespread propagation of asymmetric-key based or public-key infrastructures (PKIs). The Certification Authority issues the certificate that binds an encryption user's identity to a public key. The CA also serves as the escrow, or key holder, for all certified private key owners. Both public and

private keys are necessary to decipher data encrypted using asymmetric cryptography. The CA publishes the procedures through which user's identities have been authenticated by the Certifying Authority. The procedures and certifications attest that the CA has verified, or authenticated, that the public keys issued have been issued to the correct users.[170]

Once a certificate has been issued, it must be published either by the key owner or by the CA to be of use to the owner and the user community at large. The lightweight Directory Access Protocol (LDAP), a scaled down version of the Directory Access Protocol previously developed by the International Telecommunications Union (ITU), has become the de facto standard for publishing and accessing public key certificates from a certificate repository.[171]

The CA process has been complicated by the complete failure by the Federal Government in establishing a centralized, public-key Certifying Authority in the United States (e.g., the Clipper Chip fiasco). The emergence of independent government agency and commercial Certifying Authorities for public-key certifications, a genuine reluctance outside the Federal Government to trust Federal CAs for private key escrow purposes, and the absence of an agreed-upon, hierarchical structure for CAs or universal PKI policies and standards, have contributed to the lack of a national PKE system for the United States.[172]

CONGRESS--2000

H.R. 4246: Cyber Security Information Act

On 12 April 2000, Representative Thomas M. Davis (R-VA) introduced H.R. 4246, the Cyber Security Information Act, designed to encourage the secure disclosure and protected exchange of information concerning cyber security problems, solutions, test practices and results. Following its reading on the House floor, the bill was referred concurrently to the House Committees on Government Reform and on the Judiciary, for consideration of provisions of the bill falling within the jurisdiction of each committee.[173]

On 8 May 2000, the House Government Reform Committee referred the bill to its Subcommittee on Government Management, Information and Technology for consideration. On 22 June 2000, the Committee held formal hearings on the bill. No further action was taken to advance the bill out of the Committee.[174]

SUMMARY

The issues surrounding the sale and use of encryption products were at the core of the debate concerning Information Assurance well before the eight years of consideration by Clinton Administration. Once the exclusive purview of the NSA and the Defense establishment, encryption has come to symbolize a sort of security panacea for the Information Age and the National Information Infrastructure.

While true that strong or even moderately strong encryption is a powerful security tool, encryption cannot solve all of the security issues surrounding use of microprocessors, computer systems, and the Internet. The key is not data security but rather data access security. Data access security can only be achieved through the application of robust, user authentication technologies, coupled to a meaningful but minimal set of adequate, user security practices. Social engineering remains the single greatest threat to computer system security. It takes but a single instance of lax personal security to allow an intruder access to the system from which to exact untold damage depending on the intruder's individual skills and motivation.

Over a nearly eight-year period, the Clinton Administration expended considerable resources and energy to defend an encryption policy that, by all standards, was overtaken by events before the Clinton Administration ever took office. Finally, on 16 September 1999, President Clinton himself reversed years of government stonewalling by edicting an end to long-standing government prohibitions on the use, sale, and export of encryption products.

In speculating as to the cause for this significant policy change, Admiral William O. Studeman, USN (Ret.), formerly head of NSA, DIA, ONI, Acting Director of Central Intelligence under President George Bush and

easily one of the most knowledgeable experts on encryption in the world today, said:

> It's a tough policy issue, perhaps the toughest in government (makes your head hurt). United States industry wanted no constraints on their market competitiveness in this area, and competitiveness is a more important consideration than national security. In fairness, global secure commercial competitors were headed in this direction anyway (i.e., witness the focus on PKI/CA technology and other security product layers which are enabled by PKI), and it was stated that the United States could have been left behind as others provide the technology which was already out there in places like the Internet. Perhaps the voices of law enforcement and national security were silenced by the combination of Executive Branch and Congressional policies. A lot of this stems from the obvious fact that the United States has not been able to find a techno-policy approach which simultaneously facilitates the proliferation of adequate information protection on the one hand, and preserves some level of transparency on the other. I don't think we (the law enforcement and defense community) tried hard enough and hold the current Administration at fault for this.[175]

In retrospect, could the encryption policy issues have been handled in a more "enlightened" fashion? Unquestionably. But without an adequate framework to piece together the myriad of constituent interdependencies of such a complex policy, even the United States Executive Branch can find itself hopelessly mired in the technical complexities and political nuances of such a policy issue.

The case study findings in Chapter Six, Federal Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), along with the results from the preceding Chapter Five, Federal Information Technology Policy and Legislative Initiatives During the Clinton

Administration (1993-2000), serve as the foundation for the case study analysis in Chapter Seven, Critical Infrastructure Protection Policy and Legislative Initiatives During the Clinton Administration (1993-2000). In Chapter Eight, Analyzing the Government's Information Technology/ Information Assurance Policy Initiatives (1993-2000), the PIES Model will be applied to the results of these case study results from Chapters Five, Six and Seven, establishing a framework for the systematic analysis of the evolution of Clinton Administration Information Assurance policy between 1993-2000.

[1] Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington, D.C.: Department of Defense, Office of the Undersecretary of Defense for Acquisition Technology, October 1994), 36.

[2] Harry S. Truman, President of the United States, National Security Council Intelligence Directive No. 9, 24 October 1952.

[3] Richard M. Nixon, President of the United States, Presidential Directive: Establishment of the Central Security Services (CSS) within NSA, 5 May 1972.

[4] William Cohen, William Daley, Jacob Lew, and Janet Reno, "Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace," *A Report to the President of the United States,* 16 September 1999, 6.

[5] P.L. 100-235, Section 1 (a).

[6] Ibid., Section 2 (b) (1).

[7] Ibid., Section 2 (b) (2).

[8] Whitfield Diffie and Susan Landau, *Privacy on the Line* (Cambridge, MA:The MIT Press, 1998), 59.

[9] James Adams, *The Next World War* (New York, NY: Simon and Schuster, 1998), 215-216.

[10] Diffie, 23-24.

[11] Ibid., 25.

[12] Discussion with Admiral William O. Studeman, USN (Ret.), Former Director, National Security Agency, dated 4 March 1998.

[13] Adams, 215.

[14] Ibid., 215.

[15] Ibid., 215.

[16] Ibid., 219.

[17] Electronic Frontier Foundation, "'EFF DES Cracker' Machine Brings Honesty to Crypto Debate," *EFF DES Cracker Press Release* (17 July 1998), 2.

[18] Diffie, 28.

[19] Adams, 216.

[20] William Melton, "Electronic Cash Transfers," *Proceedings from the Conference on National Security in the Information Age*, ed. General James P. McCarthy, USAF [Ret], (United States Air Force Academy, February 28-March 1, 1996), 301.

[21] Electronic Frontier Foundation, "RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation," in Press Release from RSA Data Security Conference (San Jose, CA: 19 January 1999), 1.

[22] Ibid., 2.

[23] Edward L. Allen, Deputy Assistant Director, Information Resources Division, Federal Bureau of Investigation, in letter to Barry Steinhardt, 10 August 1998.

[24] William A. Reinsch, Undersecretary of Commerce for Export Administration, U.S. Department of Commerce, in letter to Barry Steinhardt, 26 August 1998.

[25] Whitfield Diffie and Susan Landau, *Privacy on the Line* (Cambridge, MA: The MIT Press, 1998), 60-61.

[26] Critical Information Assurance Office, "Practices for Securing Critical Information Assets," Chapter III (Washington, D.C., January 2000), 44.

[27] Ibid., 44.

[28] Ibid., 44.

[29] Adams, 217.

[30] Diffie, 106 and Adams, 217.

[31] Office of the Press Secretary, The White House, "Statement by the Press Secretary," 16 April 1993, 1-2.

[32] Diffie, 7-12.

[33] Congress, House, Representative Maria Cantrell of Washington, "Legislation to Amend the Export Control Act of 1979," H.R. 3627, 103rd Congress, 1st sess., *Congressional Record* (24 November 1993), E3110.

[34] Ibid., E3112.

[35] Ibid., E3112.

[36] The White House, Office of the Press Secretary, "Statement by the Press Secretary on Export Control Reform, 30 March 1994, 1.

[37] Executive Order 12924, 1.

[38] Ibid., 2.

[39] Critical Information Assurance Office, *Practices for Securing Critical Information Assets* (Washington, D.C.: CIAO, January 2000), D-2.

[40] Ibid., D-2.

[41] Congress, House, Representative Samuel Gejdenson of Connecticut, "The Export Administration Act of 1994," H.R. 3937, 103rd Congress, 1st sess., *Congressional Record* (25 May 1994), H4089.

[42] Ibid., H4089.

[43] Ibid., H4090.

[44] Congress, House, Representative Samuel Gejdenson of Connecticut, "The Export Administration Act of 1994," H.R. 3937, 103rd Congress, 1st sess., *Bill Summary and Status for the 103rd Congress* (2 March 1994), 1-2.

[45] Ibid., 2.

[46] Ibid., 3.

[47] Congress, House, Representative Bart Gordon of Tennessee, "Providing for Consideration of H.R. 3937, Export Administration Act of 1994," *Congressional Record* (14 July 1994), H5732.

[48] Ibid., H5732.

[49] Ibid., H5732.

[50] Ibid., H5732.

[51] Ibid., H5732.

[52] Ibid., H5732.

[53] Ibid., H5733.

[54] Congress, House, Representative William D. "Don" Edwards of California, "Communications Assistance for Law Enforcement Act," H.R. 4922, 103th Congress, 1st sess., *Congressional Record* (4 October 1994), H10726.

[55] Ibid., H10726.

[56] Ibid., H10773-10783.

[57] Ibid., H10917.

[58] Ibid., 29 November 1994, H11563.

[59] Ibid., 29 November, 1994, D1259.

[60] Congress, Senate, Senator Patrick Leahy of Vermont, S. 2375, 103th Congress, 1st sess., *Congressional Record* (9 August 1994), S11055-11062.

[61] Ibid., S12619.

[62] Ibid., S14478.

[63] Ibid., S14666.

[64] Congress, House, Representative George E. Brown, Jr. of California, "Encryption Standards and Procedures Act of 1994," H.R. 5199, 103rd Congress, 1st sess., *Bill Summary and Status for the 103rd Congress* (6 October 1994), 1.

[65] Ibid., 1.

[66] Executive Order 12981: Administration of Export Controls, 1.

[67] Ibid., 3-5.

[68] Executive Order 13026: Administration of Export Controls on Encryption Products, 1.

[69] Ibid., 2.

[70] Congress, House, Representative Robert Goodlattee of Virginia, "Security and Freedom Through Encryption (SAFE) Act," H.R. 3011, 104th Congress, 2d sess., *Congressional Record* (5 March 1996), E276-277.

[71] Ibid., E277.

[72] Ibid., E277.

[73] Congress, Senate, Senator Conrad Burns of Montana, "Promotion of On-Line in the Digital Era (Pro-CODE) Act of 1996, S.1726, 104th Congress, 2nd sess., *Congressional Record* (2 May 1996), S4624.

[74] Ibid., S4624.

[75] Ibid., S4625.

[76] Ibid., S4625.

[77] Ibid., S2624

[78] Karn v. Department of State, 925 F. Supp. 1 (D.D.C. 1996).

[79] Steven Levy, "Courting a Crypto Win," *Newsweek*, vol. CXXXIII, no. 20 (17 May 1999), 85.

[80] Ibid., 85.

[81] *Bernstein v. Department of State*, 945 F. Supp. 1279 (N.D. Cal. 1996).

[82] Frank Tiboni, "In Turnabout, McCain Sponsors Bill to Ease Crypto Export Limits," *Government Computer News*, Vol. 18, No. 11 (26 April 1999), 6.

[83] Department of Commerce, National Institute of Standards and Technology, " Announcing Plans to Develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange," *Federal Register,* Vol. 62, No. 92 (13 May 1997), 26294.

[84] Ibid., 26294.

[85] The White House, President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, i.

[86] The White House, The President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, 74.

[87] Ibid., 74.

[88] Ibid., 75.

[89] Congress, Senate, Senator Frank Leahy of Vermont, "The Encrypted Communication Privacy Act of 1997(ECPA) Act of 1997, S.376, 105th Congress, 1st sess., *Congressional Record* (27 February 1997), S1749.

[90] Congress, Senate, Senator Conrad Burns of Montana, "Promotion of On-Line in the Digital Era (Pro-CODE) Act of 1997, S.377, 105th Congress, 1st sess., *Congressional Record* (27 February 1997), S1756.

[91] Ibid., S1756.

[92] Ibid., E1231.

[93] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 1997," H.R. 1903, 105th Congress, 1st sess., *Congressional Record* (17 June 1997), E1231.

[94] Levy, 85

[95] Christopher J. Dorobek, "Defense Wants PKI Now," Government Computer News, vol. 17, no. 12 (4 May 1998), 1.

[96] Ibid., 60.

[97] Sharon Gaudin, "Feds Allow 56-bit Encryption," *Computerworld*, Vol. 32, No. 38 (21 September 1998): 6.

[98] White House, Office of the Press Secretary, "Administration Updates Encryption Policy," 16 September 1998, 1.

[99] Ibid., 1.

[100] The White House, Office of the Press Secretary, "Press Briefing By: The Vice President, Deputy Chief of Staff John Podesta, Principal Associate Deputy Attorney General Robert Litt, Assistant Director of the FBI Carolyn Morris, Under Secretary of Commerce William Reinsch, Deputy Secretary of Defense John Hamre, and Deputy National Security Advisor Jim Steinberg ," 16 September 1998, 1.

[101] Ibid., 1-2.

[102] Ibid., 2.

[103] Ibid., 2.

[104] William Jackson, "NIST OKs Crypto Products," *Government Computer News,* vol. 17, no. 36 (26 October 1998), 3.

[105] Ibid., 3.

[106] Ibid. H7293-7294.

[107] Congress, Senate, "Computer Security Enhancement Act of 1997," H.R. 1903, 105th Congress, 1st sess., *Congressional Record* (17 September 1997), S9514.

[108] William Cohen, Janet Reno, William Daley, and Jacob Lew, *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace,* 16 September 1999, 5.

[109] Ibid., 5.

[110] Ibid., 5.

[111] Ibid., 7.

[112] Ibid., 8.

[113] Ibid., 9.

[114] Ibid., 9.

[115] Ibid., 9.

[116] The White House, Office of the Press Secretary, "Export Controls on Computers," 1 February 2000, 3.

[117] Tiboni, 6.

[118] Congress, Senate, Senator McCain of Arizona, *Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999,* S.B. 798, Title I, SEC. 103., 106th Congress, 2d sess., *Congressional Record* (14 April 1997), S3695.

[119] Ibid., S3705-3706.

[120] Ibid., Title 1, SEC. 103. (b).

[121] Ibid., Title III, SEC. 302.

[122] Ibid., Title II.

[123] Ibid., Title V, SEC. 505. (b).

[124] Tiboni, 6.

[125] PROTECT ACT, Title III.

[126] United States Congress, Senate, Committee on Commerce, Science and Transportation, Hearing on Encryption, "Testimony, Department of Justice," *Congressional Record*, 10 June 1999, S10388.

[127] United States Congress, Senate, Committee on Commerce, Science and Transportation, Hearing on Encryption, *Congressional Record,* 10 June 1999.

[128] Kenneth W. Dam and Herber S. Lin, "Cryptography's Role in Securing the Information Society," National Research Council, 1996. *Congressional Record,* 10 June 1999, S10388.

[129] National Counterintelligence Center, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 1995. *Congressional Record,* 10 June 1999, S10388.

[130] Testimony, Hearing on Encryption, David Aucsmith, Chief Security Architect, Intel Corporation, *Congressional Record,* 10 June 1999, S10388.

[131] United States Congress, Senate, Committee on Commerce, Science, and Transportation, Senator John McCain of Arizona, "Report from the Committee on Commerce, Science, and Transportation, S. 798," Rept. No. 106-142, 106th Congress, 2d sess., *Congressional Record* (5 August 1997), S10388.

[132] Reports of Committees, S.798. *Congressional Record* (5 August 1999), S10388.

[133] United States Congress, House, Representative Henry Hyde of Illinois, Legislative Hearing on H.R.850, "Security and Freedom Through Encryption (SAFE) Act, " 4 March 1999, http://www.house.gov/judiciary/106-19.htm.

[134] Ibid., http://www.house.gov/judiciary/106-19.htm., testimony of the Honorable William Reinsch, Undersecretary of Commerce for Export Administration, United States Department of Commerce, before the House Judiciary Subcommittee on Courts and Intellectual Property, 4 March 1999.

[135] Ibid., http://www.house.gov/judiciary/106-19.htm., testimony of the Honorable Ronald D. Lee, Associate Deputy Attorney General, United States Department of Justice, before the House Judiciary Subcommittee on Courts and Intellectual Property, 4 March 1999.

[136] Ibid., http://www.house.gov/judiciary/106-19.htm., testimony of the Honorable Barbara McNamara, Deputy Director, National Security Agency, United States Department of Defense, before the House Judiciary Subcommittee on Courts and Intellectual Property, 4 March 1999.

[137] Ibid., http://www.house.gov/judiciary/106-19.htm.

[138] Ibid., http://www.house.gov/judiciary/106-19.htm.

[139] Ibid., http://www.house.gov/judiciary/106-19.htm., testimony of Craig McLaughlin before the House Judiciary Subcommittee on Courts and Intellectual Property, 4 March 1999.

[140] United States Congress, House, Representative Henry Hyde, "Letter to Chairman Hyde from CBO Director Dan Crippen," 21 April 1999.

[141] Congress, House, Representative Robert Goodlattee of Virginia, "Security and Freedom Through Encryption (SAFE) Act," H.R.850, 106th Congress, 1st sess., *Congressional Record*, House Report 106-117, Part III (19 July 1999), H5838.

[142] Ibid., House Report 106-117, Part IV, H6423.

[143] Ibid., House Report 106-117, Part II, H6423.

[144] Lawlor, 67.

[145] United States Congress, Senate, Senator Patrick Leahy of Vermont, "Electronic Rights for the 21st Century Act," S.854, 106th Congress, 1st sess., *Congressional Record* (21 April 1999), S4042-4047.

[146] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 1999," H.R. 2413, 106th Congress, 1st sess., *Congressional Record* (1 July 1999), E1491.

[147] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 1999," H.R. 2413, 106th Congress, 1st sess., *Congressional Record* (1 July 1999), E1491-1492.

[148] Ibid., E1491-1492.

[149] Shruti Date, "Security Issue Ignites Debate: Congress, GAO Want to See Better Security Planning," *Government Computer News,* vol. 19, no. 6 (20 March 2000), 1 & 52.

[150] Congress, House, Representative Porter J. Goss of Florida, "Encryption for the National Interest Act," H.R. 2616, 106th Congress, 1st sess., *Bill Summary and Status for the 106th Congress* (27 July 1999), 3.

[151] Ibid., 3.

[152] Ibid., 1-2.

[153] Congress, House, Representative Porter J. Goss of Florida, "Tax Relief for Responsible Encryption Act of 1999," H.R. 2617, 106th Congress, 1st sess., *Congressional Record* (27 July 1999), H6581.

[154] Ibid., H6581.

[155] Ibid., 85.

[156] The White House, Office of the Press Secretary, "Export Controls on Computers," 1 February 2000.

[157] Ibid., 2-3.

[158] Ibid., 2.

[159] The White House, office of the Press Secretary, "Statement by the President," 1 February 2000.

[160] U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Developing Security Plans for Information Technology Systems,* NIST Special Publication 800-18 (Washington, D.C.: December 1998), 33.

[161] Critical Information Assurance Office, *Practices for Securing Critical Information Assets* (Washington, D.C.: CIAO, January 2000), 3-5.

[162] Ibid., 30.

[163] Ibid., 27.

[164] Ibid., 29.

[165] Ibid., 43.

[166] Ibid., 44-45.

[167] Ibid., D-2.

[168] Ibid., D-2.

[169] Ibid., D-1.

[170] Ibid., D-1.

[171] Ibid., D-1.

[172] Ibid., D-1.

[173] Congress, House, Representative Thomas M. Davis of Virginia, "Cyber Security Information Act," H.R. 4246, 106th Congress, 2nd sess., *Bill Summary and Status for the 106th Congress* (12 April 2000), 1.

[174] Ibid., 1.

[175] Email to the author from Admiral William O. Studeman, USN (Ret.), Former Chief of Naval Intelligence; Director, Defense Intelligence Agency; Director, National Security Agency; Acting Director, Central Intelligence Agency. Vice-President and Deputy General Manager, TRW Systems Integration and Technology Group, dated 4 April 2000.

Assessing United States Information Assurance Policy

Response to Computer-Based Threats to National Security

Continued

by

John Frederick Stickman

A Dissertation Presented to the
FACULTY OF THE SCHOOL OF POLICY, PLANNING,
AND DEVELOPMENT
UNIVERSITY OF SOUTHERN CALIFORNIA
In Partial Fulfillment of the
Requirements for the Degree
DOCTOR OF PUBLIC ADMINISTRATION

May 2001

CHAPTER SEVEN

CRITICAL INFRASTRUCTURE PROTECTION POLICY AND LEGISLATIVE INITIATIVES DURING THE CLINTON ADMINISTRATION (1993-2000)

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

The purpose of Chapter Seven is to chronicle the specific actions and activities by the Federal Government in support of United States' Critical Infrastructure Protection policy during the eight years of the Clinton Administration. This case study provides a chronological ordering of the policy-specific activities and associated impacts of Critical Infrastructure Protection policy decision makers operating within the three branches of the Federal Government between the years 1993 and 2000.

The chapter is organized by calendar year. For each calendar year, significant Critical Infrastructure Protection policy activities undertaken by the Clinton Administration, Congress, and the Federal Judiciary are chronicled. For the purposes of this study, a "significant Critical Infrastructure Protection policy activity" is defined as: an administrative action, e.g., the publication of an Executive Order, formation of a Federal Advisory Commission, issuance of a report or formal policy statement by the White House; activity on a related bill by Congress; or a hearing or judgement rendered on a related case brought before a Federal court. In years where no significant Critical

Infrastructure Protection activity was manifest, no annotation in the chapter chronicle was made.

BACKGROUND--SETTING THE STAGE

On 7 January 2000, President William Clinton issued *Defending America's Cyberspace: National Plan for Information Systems Protection.*[1] In his message accompanying the release of the Plan, President Clinton summarized the Administration's position on Information Assurance:

> For this Plan to succeed, government and the private sector must work together in a partnership unlike any we have seen before. This effort will only succeed if our Nation as a whole rises to this challenge. Therefore, I have asked the members of my Cabinet to work closely with representatives of the private sector industries and public services that operate our critical infrastructures. We cannot mandate our goals through government regulation. Each sector must decide for itself what practices, procedures, and standards are necessary for it to protect its key systems.[2]

Defending America's Cyberspace: National Plan for Information Systems Protection represents the culmination of over six years attention by the Clinton Administration to the Information Assurance policy arena. A descriptive chronology of the major administrative, legislative, and judicial actions leading to this Version 1.0 document are instructive in the understanding of its formulation as the foundation for United States policy for Information Assurance and Critical Infrastructure Protection.

Critical Infrastructure Protection

Prior to the advent of the Internet, the telecommunications component of the nation's critical infrastructure consisted of the loosely confederated government-owned telephone and teletype networks and the Public Switch Network (PSN) owned by Bell Telephone. After the Cuban Missile Crisis in October 1962, a great concern was raised over the integrity of the nation's emergency telecommunications infrastructure. Due to the central relevance of the telecommunications foundation to this chronology, a brief background summary is supplied.

Presidential Memorandum on the National Communications System

Protecting the nation's critical infrastructure has long been a subject of government concern. Dams, bridges, tunnels, power plants, and other important physical structures have been specially protected over the past 50 years. Protection of the Nation's telecommunications infrastructure has only been of major governmental concern since October 1962 and the Cuban Missile Crisis. During that 12-day period, between 16 and 28 October 1962, the United States and the former Soviet Union hovered on the brink of nuclear war, precipitated by the introduction of Soviet offensive nuclear missiles into Cuba.[3] Difficulties in maintaining secure communications between the leaders of the United States, Soviet Union, NATO, and other foreign heads of state had threatened to complicate the crisis further.

Immediately after the crisis, in November 1962, President John F. Kennedy ordered a comprehensive investigation of United States national security communications. The National Security Council (NSC) formed an interdepartmental committee to examine the existing communication networks and to institute changes as deemed necessary.[4] As a result of the committee's findings, it recommended the formation of a single, unified communications system to serve the President, DOD, diplomatic and intelligence activities, and the civilian leadership.[5]

Consequently, and in order to provide better communications support to critical governmental functions during an emergency, President Kennedy established the National Communications System (NCS) by Presidential Memorandum on 21 August 1963. The mission of the NCS was to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of Management and Budget in establishing and implementing policy and provisions for national security and emergency preparedness communications for the Federal Government. This capability would be provided primarily through the owned and leased telecommunications facilities and services of the United States Government. The NCS' mandate included linking, improving, and extending the communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability under national emergency situations, principally nuclear war.[6]

Executive Order 12382: President's National Security Telecommunications Advisory Committee (NSTAC)

In September 1982, President Ronald Reagan established a civilian telecommunications advisory committee to provide analysis and advice to the Executive Branch on national security and emergency communications issues. The President's National Security Telecommunications Advisory Committee (NSTAC) was created in September 1982 by Presidential Executive Order 12382, amending Section 706 of the Communications Act of 1934.[7]

NSTAC was created to provide a forum for industry-based analyses and council to the President of the United States on a wide range of policy and technical issues associated with national security and emergency preparedness (NS/EP) telecommunications. Its membership, comprised of up to 30 industry CEOs appointed by the President, represent a national cross-section of the leading information technology, telecommunications, aerospace, banking and manufacturing companies.[8]

The telecommunications industry/government partnering embodied in the NSTAC charter and bylaws adopted 20 July 1983 and amended twice since, on 8 June 1989 and again on 12 January 1995, are intended to facilitate the information exchange between the public and private sectors as the national telecommunications infrastructure evolves. The specific work of the NSTAC is performed by its subordinate task forces and working groups.[9]

Executive Order 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions

On 3 April 1984, President Ronald Reagan signed Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecom-munications Functions.[10] Executive Order 12472 considerably broadened the National Security and Emergency Preparedness (NS/EP) telecommunications responsibilities of the National Communications System (NCS). Under President Reagan's order, the NCS would be responsible for developing a revolutionary NS/EP telecommunications architecture, preparing program plans that would identify NS/EP telecommunications requirements and enhancements that would take advantage of new technologies and foster interoperability with other public and private components of the NCS, and for implementing and administrating funded plans and programs associated with the NCS.[11]

The NCS administrative structure consists of the Secretary of Defense as Executive Agent, an NCS Committee of Principals (COP), an NCS Manager, and an administrative structure to govern NCS-designated communication assets.[12] The NCS Manager chairs the COP. In recent years, the NCS Manager has also been the Director of the Defense Information Systems Agency. As of 1 November 1999, LTG David J. Kelley, USA, held that dual assignment.[13]

Department of Defense Directives 8000.1 and 3600.1: Defense Information Systems Agency's Vulnerability Analysis and Assessment Program

During the 1991 Gulf War, the Department of Defense relied extensively on the Internet to support its global communications, to exchange data with its coalition allies, and to gather and disseminate intelligence and counter-intelligence information concerning Iraqi intentions. This increasing Defense reliance on the Internet global communications backbone would come at a price: increased opportunity for unauthorized, Internet-based cyber intrusions into Defense computer systems and networks.

Generally, classified information such as war planning data or highly classified weapons systems research and development information is protected from outside cyber intrusion through its hosting on isolated or stand-alone computers, encryption of the data, or limiting its transmission over dedicated, secure circuits. However, extensive and growing DOD use of the Internet to exchange unclassified, but sensitive information trafficked through DOD automated information systems, places military readiness and operations at risk to cyber-based exploitation of Defense computer security weaknesses. These exploitable weaknesses would offer an Information Technology-enabled adversary essential keys for the cyber-based disruption of the United States' critical information infrastructures in some future Strategic Information Warfare (SIW).

In recognition of these severe weaknesses in Defense computer security and the emerging cyber threats emanating from Interneted sources,

the Department of Defense issued two directives, 8000.1 and 3600.1. Department of Defense Directive (DODD) 8000.1, entitled *Defense Information Management Program*, was issued on 27 October 1992 and charges the Defense Information Systems Agency (DISA) and the military services with the responsibility to provide the necessary technologies and services to ensure the availability, reliability, maintainability, integrity, and security of Defense information.[14]

DODD 8000.1 was followed in December 1992 with DODD 3600.1, entitled *Information Operations*. This directive broadly states that measures will be taken as part of a program to, "protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within those systems."[15] DISA, in cooperation with the military services and Defense agencies, is responsible for implementing the information security program called out in DODD 3600.1.

In December 1992, and in response to DODDs 8000.1 and 3600.1, DISA created a program to assess the vulnerabilities and exploitable security holes in the over 2.1 million computers, 10,000 local area networks, 100 long-distance networks, 200 command centers, and 16 central computer processing centers operated by the Department of Defense. Under this initiative, dubbed the Vulnerability Analysis and Assessment Program (VAAP), DISA would attempt to penetrate selected Defense information

systems using techniques both widely known and available to hackers, cyber terrorists, and adversary nations via the Internet.[16]

The focus of DISA personnel in their probative attacks on DOD systems would be limited to known computer-system vulnerabilities previously publicized by DISA in their alerts to the military services and Defense agencies. Assessments are performed at the request of the targeted Defense agency or installation. Upon completion of the assessment, DISA personnel meet with the targeted systems and security personnel to discuss the results of the assessment and to jointly develop a detailed action plan to strengthen the targeted organization's cyber defenses, intrusion detection capabilities, and system security administrator training.[17]

Despite the implied mandates of DODD 8000.1 and DODD 3600.1, DOD to date has not initiated DOD-wide policy requirements for correcting identified computer system or computer network deficiencies and vulnerabilities. Vulnerabilities and deficiencies that are identified are immediately broadcast to Defense network administrators, along with suggested fixes. However, the lack of specific policy requirements or resultant directives for correcting identified vulnerabilities has led to little or no corrective actions on the part of many Defense organizations operating critical infrastructure components and installations.[18]

CLINTON ADMINISTRATION--1994

Department of Defense and Central Intelligence Agency: Joint Security Commission

In Fall 1993, a Joint Security Commission was established by the Secretary of Defense and the Director of Central Intelligence to study the state of Defense computer security. On 28 February 1994, the Commission, chaired by Deputy Attorney General Jamie Gorelick, issued its final report entitled, *Redefining Security.* In the report, the Commission identifies computer networks as "the battlefields of the future" and that the "at cyber risk" was not limited to just military systems. Most significantly, the Commission reported that if an enemy were to launch a cyber attack on the United States' unprotected civilian infrastructure, e.g., the public switched telephone network, the economic and societal results could be disastrous:

> The Commission considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century, and believes there is insufficient awareness of the grave risks we face in this arena. We have neither come to grips with the enormity of the problem nor devoted the resources necessary to understand it fully, much less rise to the challenge.[19]

Despite the growing concern for hackers, cyber terrorists, and other outsider threats to Defense systems, the Joint Security Commission found that the greatest risk to the compromise of secure Defense systems is through insiders:

> The great majority of past compromises have involved insiders, cleared persons with authorized access who could circumvent

physical security barriers, not outsiders breaking into secure areas.[20]

The Commission found that personal security lies at the heart of DOD security systems and the trustworthiness of those who deal with sensitive and classified information must be ensured.[21]

However, the Commission also found DOD computer security policies to be severely outdated, having been developed in an era of physically and electronically isolated computer systems, and therefore unsuited for the modern, network-dependent, Internet environment. The Commission found contemporary DOD computer security policy to be overly based on a philosophy of risk avoidance. The Commission recommended a more realistic risk management approach predicated on gradual risk reduction through incremental steps, coupled with increased investment in DOD information security equal to 5-10% of the total information systems infrastructure cost--including operations and maintenance. In addition to an incremental risk step down approach, the Commission recommended adopting a risk management approach focused on reducing overall DOD information security costs and increasing across the board implementation of DOD-wide physical and information security (INFOSEC). In addition, the Commission found that Defense policy was fragmented among a profusion of computer security policy-making authorities within the Department. This, the Commission concluded, led to policies evolving in relative vacuum, creating

inefficiencies and implementation problems as systems proliferate and network across organizational boundaries.[22]

The Commission report particularly criticized DOD's lack of a comprehensive training program for information systems security personnel. Citing the lack of adequately trained personnel necessary to wage combat effectively in the new cyber dimension, the report noted:

> Because of a lack of qualified personnel and a failure to provide adequate resources, many information systems security tasks are not performed adequately. Too often, critical security responsibilities are assigned as additional or ancillary duties.

The report concluded that despite the critical importance of computer security awareness, training, and education programs, these same programs tend to be frequent and ready targets for budget cuts.[23]

Defense Science Board Summer Study Task Force: Information Architecture for the Battlefield

Shortly after the Joint Security Commission submitted its final report, the Under Secretary of Defense for Acquisition and Technology directed that a Defense Science Board Task Force be established to study mechanisms for expanding the use of information in modern warfare and to define an information architecture to support combat operations on the battlefield. Co-chaired by Dr. Craig I. Fields and General James P. McCarthy, USAF (ret.), the Task Force completed its work in the fall of 1994. Its final report, dated 20 October 1994 and entitled, *Information Architecture for the Battlefield,* focuses on the role of the warfighter as the principal customer for battlefield

information and the warfighter's need for flexible information systems that can be readily adapted to accomplish a variety of different missions.[24]

In summarizing its recommendations for a proposed framework for a warfighter-centric, battlefield information architecture, the Task Force concluded that:

> The timing is right for a major push to improve the effectiveness of information systems to support the warfighters. The Task Force sees significant opportunities for DOD in the use of information in warfare as well as vulnerabilities in today's information systems. The Department has not come to grips with the leverage of information as a tool for use by the warfighter. There is a need for change throughout the Department regarding the way information systems are developed and employed. This Task Force underscores the importance of such changes to achieving information dominance on the battlefield. Unfortunately, the business practices of the Department are hindering DOD's ability to exploit the best systems and technologies available in the commercial sector. Further, DOD needs to place high priority on military-unique science and technology areas in its information technology investments.[25]

In summarizing the review of United States battlefield information systems, the Task Force concluded that the DOD had built a system of systems that collectively could not adequately support the warfighter, especially in joint or multi-service operations.[26]

In conducting its investigation, the Task Force found itself drawn to a second major aspect of the use of information in warfare. What began as a study of the use of information **in** warfare also became a study of aspects of information **as** warfare. Information warfare, termed the "next revolutionary technology" by the Task Force, became an equally central theme.[27]

During this phase of the study, Defense systems vulnerabilities to strategic and tactical information warfare became a dominant concern of the Task Force. Though the Task Force found the information systems of potential adversaries equally vulnerable to the affects of information warfare, it concluded that the level of vertical and horizontal digital information integration within the United States military, economy, and society to be unique. Despite this fact, the Task Force found that, "**No one** (Task Force's bold/underline) is responsible for protecting the commercial, public and private systems upon which national viability now depends. This must be addressed in a national policy review."[28]

Despite the strength of this declaration, identifying a specific information warfare threat to those, "commercial, public and private systems upon which the national vitality now depends," proved elusive for the Task Force:

> Vulnerabilities of the national information infrastructure (NII) are easily described; however, the actual threat is more difficult to pin down. Nevertheless, there is mounting evidence that there is a threat that goes beyond hackers and criminal elements. This threat arises from terrorists groups or nation states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. The threat causes concern over the specter of military readiness problems caused by attacks on DOD computer systems, but it goes well beyond DOD. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected. This is especially so for those tied to the NII. As the United States military enters a new world order where regional conflicts and economic competition take center stage, more and more potential adversaries will see Information

> Warfare as an inexpensive (and even surgical) means of damaging an adversary's national interests.[29]

Key recommendations of the Task Force include DOD and Administration recognition that Information in Warfare is a critical element of warfighting success, necessitating the establishment of a Battlefield Information Task Force to define warfighter information systems needs and vision for the future. The Task Force reinforced the need for DOD to "gear up" for both offensive and defensive information warfare by conducting an overall assessment to determine the impact of information warfare on the DOD and by providing strong DOD inputs to the formulation of a coordinated national policy on information warfare. Finally, the Task Force recommended an expanded exploitation of commercial research and development to address DOD information warfare needs.[30]

CLINTON ADMINISTRATION--1995

President's National Security Telecommunications Advisory Committee (NSTAC)

In part as a result of the Joint Security Commission study and the Defense Science Task Force on the Information Architecture for the Battlefield, President Clinton requested that the National Security Telecommunications Advisory Committee (NSTAC) formally addresses Information Assurance and critical information infrastructure protection issues beginning in 1995. At the NSTAC XVLL meeting on 16 January 1995, Vice Admiral Mike McConnell, Director of the National Security Agency (NSA)

briefed the 17th meeting of the NSTAC principals on threats to U.S. information systems and the need to improve the security of critical national infrastructures.[31]

On 20 March 1995 and in response to the Admiral McConnell's briefing, NSTAC Chair Mr. William T. Esprey, CEO of the Sprint Corporation, wrote a letter to President William Clinton, stating that:

> [The] integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack...[and] other national infrastructures...[such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems and could be at risk.[32]

On 7 July 1995, President Clinton responded, stating that he would:

> Welcome NSTAC's continuing efforts to work with the Administration to counter threats to our Nation's information and telecommunications systems...the President further asked...the NSTAC principals, with input from the full range of NII users, to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information infrastructure.[33]

In the spring of 1995, NSTAC's Issues Group held a series of panel discussion to address concerns related to Information Warfare (IW) and Information Assurance (IA). As a result of these meetings, the Issues Group determined that it would be appropriate for the NSTAC to address Information Assurance matters as they related to critical national infrastructures. The Issues Group recommended that an Information Assurance Task Force (IATF) be established as the focal point for NSTAC activities.[34]

On 15 May 1995, the NSTAC's Industry Executive Advisory Subcommittee (IES) established the Information Assurance Task Force (IATF) to cooperate with the United States Government to identify critical national infrastructures and to determine their importance to the national interest and to schedule independent assessments of elements of the critical information infrastructure. Working with representatives from the national security community, law enforcement, civil departments and agencies, and the private sector, the task force narrowed an initial study list of national services critically dependent on the nation's information infrastructures to three: electric power, financial services, and transportation. These three infrastructures were selected on the basis of their strong interdependencies and their reliance on telecommunications and information systems networks to perform key functions.[35]

At the NSTAC XIX Executive Session, Attorney General Janet Reno expressed her concerns about cyber security and issues surrounding cyber crime, stating that government could not solve the associated Information Assurance problems without first establishing a strong partnership with industry. In response, the IIG established a Cyber Crime Subgroup to explore the need for a more cooperative approach to Information Assurance between industry and government. A point paper was developed to frame the issues to be discussed in a

proposed future meeting between NSTAC and Attorney General Reno at NSTAC XX.[36]

Following NSTAC XIX, the Industry Executive Subcommittee (IES) restructured its organization to streamline its work to prevent any duplications of effort within the NSTAC working committee structure. As a result, the IATF and its Information Assurance responsibilities were incorporated into the activities of the Information Infrastructure Group (IIG) and its four subgroups. Two of these subgroups, the Cyber Crime Subgroup and the Information Assurance Policy Subgroup, were focused specifically on threats to the nation's information networks and computer system infrastructures.[37]

Defense Science Board: Task Force on Improved Application of Intelligence to the Battlefield

In a follow on to the October 1994 Defense Science Board Task Force study on Information Architectures for the Battlefield, the Under Secretary of Defense for Acquisition and Technology directed that the Defense Science Board establish a Task Force to study mechanisms for improving the application of information intelligence to the battlefield. The Task Force members met between May and July 1995 under the leadership of Chairman Charles Gandy and Vice Chairman General James P. McCarthy, USAF (ret.).[38]

The Task Force was chartered to assess the use of advanced information systems to extend and enhance the value of real-time battlefield

intelligence to the warfighter. The Task Force was also asked to make recommendations for future DOD investments in high-bandwidth, digital global telecommunications technologies and integrated in-theater satellite communications equipment best suited for satisfying the real-time information needs of deployed United States and NATO forces. The Task Force test case was the peacekeeping operation in Bosnia-Herzegovina. The Task Force was asked to assess the efficacy of the Bosnian Command and Control Augmentation (BC2A) initiative, an ad hoc, satellite-based, in-theater direct broadcast system developed and fielded under the direction of Colonel Edward C. Mahen, United States Air Force. The BC2A was designed to employ both MILNET and SIPRNET communications channels, providing bi-directional, broadband communications for United States secret and sensitive data between forces on the ground in Bosnia, the National Command Authority in Washington, D.C., and the in-theater commanders-in-chief (CINCs).[39]

The Task Force conducted extensive meetings in the continental United States (CONUS) and in the field, paying particular attention to the needs of the warfighter at lower echelon levels (battalion and below). The Task Force determined that the BC2A initiative was already significantly contributing to improving the flow of information and the subsequent effectiveness of military operations on a small-scale basis, but that more could be accomplished by expanding the high-bandwidth, BC2A

communications infrastructure to additional sites. The Task Force also found that expansion of the BC2A communications infrastructure would demand improvements in the information management tools and techniques used to manage and route the increased data flow. The Task Force concluded that experimentation under the realistic conditions of the Bosnian operations were "invaluable" in providing a realistic proving ground for evaluating information based warfighting concepts and approaches.[40]

Critical Infrastructure Working Group (CIWG)

A series of physical and cyber terrorists events perpetrated against the United States in the early 1990s and culminating in the 1995 bombing of the Murrah Federal Building in Oklahoma City, coupled with the results of this series of government and industry task force and commission studies, served to underscore the serious deficiencies in government and private sector preparedness in addressing new threats and vulnerabilities to the nation's critical infrastructures.

In response to the Oklahoma City tragedy, in the fall of 1995, the Clinton Administration created an interagency working group chartered to examine the nature of these new terrorist threats, the nation's vulnerabilities to them, and possible long-term solutions for addressing this aspect of United States national security.[41]

Chaired by then Deputy Attorney General Jamie Gorelick and including representatives from the Departments of Defense, State, and

Justice, the Central Intelligence Agency, and the National Security Agency, the Working Group compiled an extensive list of threats and vulnerabilities. In April 1996, the Committee delivered a white paper to the White House, in which it identified its list of physical and cyber threats. Most importantly, it recommended the formation of a Presidential Commission to more thoroughly address these growing concerns. In response to the CIWG recommendation, President Clinton signed Executive Order 13010 in July 1996, creating the President's Commission on Critical Infrastructure Protection (PCCIP).[42]

Defense Science Board: Task Force on Information Warfare (Defense)

In parallel with the formation of the CIWG, a Defense Science Board Task Force on Information Warfare (Defense) was established at the direction of the Under Secretary of Defense for Acquisition and Technology (USD/A&T). Under USD (A&T) Memorandum for the Chairman, Defense Science Board, dated October 4, 1995, the Task Force was directed to "focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability in several areas, including deterrence."[43]

Specifically, the Task Force was directed to accomplish five taskings:

- Identify the information users of national interest who can be attacked through the shared elements of the National Information infrastructure (NII);

- Determine the scope of national information interests to be defended by information warfare defense and deterrence capabilities;

- Identify the indications and warning, tactical warning, and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the National Information Infrastructure (NII) and/or attacks on the information users of national interest;
- Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national information warfare-defense capability;

- Provide specific guidelines for implementation of the Task Force's recommendation.[44]

In a letter written to Dr. Craig Fields, Chairman of the Defense Science Board, on November 21, 1996, Mr. Duane Andrews, Chairman of the Defense Science Board Task Force on Information Warfare (Defense) wrote:

> We conclude that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States which would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions. We have observed an increasing dependency on the Defense Information Infrastructure and increasing doctrinal assumptions regarding the continued availability of that infrastructure. This dependency and these assumptions are ingredients for a national security disaster.[45]

Andrew's Task Force made 16 specific recommendations and identified 50 specific actions directed at the Department of Defense to be undertaken in preparation for defending the United States' vital information infrastructure in the event of either physical or cyberattack. These actions

were to be taken over a period of five years and at an estimated cost of some $3 billion.[46]

David Leavy, a spokesman for the National Security Council, said the Government, "needs to have a more organized response," to the critical infrastructure terrorist threat, noting that with the appointment of a national anti-terrorism director, the Clinton Administration had taken steps to centralize and consolidate the oversight of United States counter-terror activity. The assignment of a military commander to oversee and coordinate the domestic antiterrorism program won general support from a Congressionally mandated study committee, the National Defense Panel, whose December 1997 recommendations included the consolidation of the Pentagon's multiple anti-terrorist initiatives into one program under a single military authority. [47]

Critics would contend that implementing this proposal would violate the federal Posse Comitatus Statute of 1878. This law severely limits the involvement of the military in civilian law enforcement matters to special duties and only upon the specific request and authorization of the President of the United States.

CONGRESS--1995

S. 982: The National Infrastructure Protection Act of 1995

Contemporary with the Joint Security Commission and Defense Science Board studies, Congress also began wrestling with the complex

issues of critical infrastructure protection. On 29 June 1995, Senator Jon Kyle (R-AZ) sponsored S. 982, the National Infrastructure Protection Act of 1995 during the 1st Session of the 104th Congress. The proposed bill was intended to revise Federal criminal code provisions regarding fraud and related activity in connection with computers. The measure would establish penalties for anyone who intentionally accessed a Federal computer without authorization or exceeding authorized access, obtains specified restricted information or data and willfully transmits or delivers it to any person not entitled to receive it.[48]

The bill was read twice on the Senate floor, then referred to the Committee on the Judiciary on 29 June 1995. The Committee subsequently tabled the bill; no further action was taken by the Senate on the bill.

CLINTON ADMINISTRATION--1996

General Accounting Office: Information Security--Computer Attacks at Department of Defense Pose Increasing Risks

On 22 May 1996, Jack L. Brock, Jr., Director, Defense Information and Financial Management Systems, General Accounting Office presented the findings of a GAO study on Department of Defense information security to select committees of Congress. Accompanying the report was a letter of transmittal, authored by Director Brock, and addressed to Senator John Glenn (D-OH), Ranking Minority Member of the Senate Committee on Governmental Affairs; Senator Sam Nunn (D-GA), Ranking Minority Member

of the Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs; and to Congressman William H. Zeliff (R-NH), Jr., Chairman of the House Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight. In his letter, Director Brock stated:

> In view of the increasing threat of unauthorized intrusions into Department of Defense computer systems, you asked us to report on the extent to which Defense computer systems are being attacked, the actual and potential damage to its information and systems, and the challenges Defense is facing in securing sensitive information. This report identifies opportunities and makes recommendations to the Secretary of Defense to improve Defense's efforts to counter attacks on its computer systems.[49]

Summarizing statistical data compiled by the Defense Information Systems Agency (DISA), the GAO reported that, in the year 1995, the DOD experienced as many as 250,000 cyber attacks against its 2.1 million computers, 10,000 local area networks, and 100 long distance networks. The exact number remains unknown, the report states, since only 1 in 150 of the estimated attacks was actually detected and reported.[50]

Based upon event data complied for the year 1995, DISA concluded that, of the estimated 250,000 DOD cyber intrusions, 65% were assumed to have been successful based upon statistical information compiled through DISA's Vulnerability Analysis and Assessment Program (VAAP). Since VAAP's inception in 1992, DISA had conducted over 38,000 cyber attacks on Defense computer systems, assessing both DOD cyber vulnerabilities and

DOD's ability to detect and report unauthorized cyber intrusions. Of DISA's successful probes, only 4%, or 988, were detected either by the targeted systems or host organizations. Of the 988 attacks detected, only 267, or approximately 27%, were reported to DISA, as required by DOD regulation.[51]

The GAO report found that DOD's increasing communications and information sharing dependence on the Internet and its reliance on public switched telephone and privately owned and operated telecommunications networks, places DOD secure communications increasingly at risk to Internet-based cyber attack. This is due to the fact that Defense systems connected to the Internet traffic in data that, while not classified, are deemed sensitive and warranting protection due to the role that data plays in worldwide Defense missions.[52]

Although classified Defense information systems are "firewalled" from non-secure Defense systems and, thus, unauthorized external access, the GAO report identified five specific instances in which classified information residing on secure data systems were compromised via their electronic links to unclassified Defense systems externally connected to the Internet. The most damaging of these intrusions took place in March and April 1994, during which more than 150 successful intrusions were perpetrated against the United States Air Force's Command and Control Research Laboratories at Rome Air Force Base (AFB), New York.[53]

Using Trojan horses and sniffer programs first to penetrate and then to harvest Rome AFB user accounts and passwords, these cyber intruders made over 150 successful penetrations of Rome's networks, eventually seizing "root," or system administrator control of Rome's operational computer networks. From the Rome base of operations, the intruders proceeded to hack into a number of interconnected United States Government computer networks, including those supporting NASA's Goddard Space Flight Center and those at Wright-Patterson Air Force Base. From the purloined Rome MILNET connections, the Rome hackers successfully penetrated the computer networks of an undisclosed number of interconnected Defense contractors and "several" other private sector organizations.[54]

DOD's costs for the 1994 Rome Laboratory incident were placed at over $500,000. This number includes the investigative costs incurred by the Air Force Office of Special Investigations (OSI) and the Air Force Information Warfare Center, who working with the FBI, eventually tracked down and arrested the two perpetrators (discovered to be two teenagers: one American and one English). Longer term damage control and associated costs were many. They included a thorough, top-down assessment of the damage done to Rome's computer network, the requisite steps taken to ensure that the data stored within Rome's electronic information repository had not been corrupted by the intruders, and the engineering of software security patches

to plug Rome's computer access vulnerabilities and failed system security safeguards.[55]

The Rome incident was not an isolated occurrence. The GAO report warns that the Rome incident serves as but one example of the mounting evidence that on-going attacks on Defense computer systems pose a serious and growing, asymmetric threat to national security. The GAO report warns that the same Internet connectivities and associated vulnerabilities, demonstrated through the Rome AFB attacks, enable the DOD's global information interconnectivity. This same interconnectivity is available to potential adversaries willing to leverage the United States' dependence on electronic communications and the ready availability of commercial software and hardware tools necessary to plan and wage Strategic Information Warfare (SIW). Major disruptions in military operations and military readiness could threaten national security if SIW attacks were successful in corrupting sensitive information and systems, or denied United States military or civilian decision makers access to vital communications, power, transportation, or other information-based, electronically-networked, critical national infrastructure systems.[56]

The GAO report cites a National Security Agency (NSA) acknowledgment that potential adversaries are developing a body of knowledge about United States critical information systems and effective methods for attacking these systems. According to NSA and Defense

officials cited in the GAO report, these methods, which include the use of sophisticated computer viruses and automated attack and denial of service programs, would permit adversaries to launch virtually untraceable economic and military operations against the United States from anywhere in the world. NSA estimates identify over 120 countries as having or in the process of developing such computer attack capabilities.[57]

The GAO report concludes by observing that, while networked systems offer tremendous potential for streamlining and improving the efficiency of Defense operations, they also greatly increase the risks that information systems supporting critical Defense functions will be attacked:

> The hundreds of thousands of attacks that Defense has already experienced demonstrate that (1) significant damage can be incurred by attackers and (2) attacks pose serious risks to national security. They also show that top management attention at all levels and clearly assigned accountability is needed to ensure that computer systems are better protected. The need for such attention and accountability is supported by the Joint Security Commission, which considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century. The Commission itself believes there is insufficient awareness of the grave risks Defense faces in this arena.[58]

On 15 May 1996, the GAO discussed the draft of this report with officials representing the responsible information systems security offices within the Office of the Secretary of Defense, DISA, the United States Army, Navy, and Air Force. While stating that many of DOD's computer and network system security problems stem from poorly designed systems and the use of commercial off-the-shelf computer hardware and software

products having little or no inherent security capabilities, DOD officials collectively agreed with the report's findings, stating that the report, "fairly represents the increasing threat of Internet attacks on the Departments' computers and networks and acknowledges the actions Defense is taking to address that threat."[59]

Executive Order 13010: Critical Infrastructure Protection

On 15 July 1996 and in anticipation of the findings from the Defense Science Board Task Force on Information Warfare, President Clinton signed Executive Order 13010, Critical Infrastructure Protection, a major policy initiative creating the President's Commission on Critical Infrastructure Protection (PCCIP).

President Clinton's Commission on Critical Infrastructure Protection was the first national effort to address the cyber and network vulnerabilities created by the Information Age. The Commission was chartered to formulate a comprehensive national strategy for protecting the United States' critical national infrastructure from physical and cyber terror threats and to report back to the President with recommendations for addressing those vulnerabilities. The critical infrastructure components were defined as telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Because many of these critical infrastructure components are owned by the private sector, Executive Order 13010 made it clear that the government and the private sector would work together to develop a strategy for protecting them and assuring their continued operation.[60]

Executive Order 13010 established the PCCIP as a 20 member, joint government and private-sector commission, whose goal would be to develop a national strategy for protecting the critical infrastructure of the United States from a range of threats and to assure their uninterrupted operation. Selected to chair the PCCIP was retired U.S. Army General Robert Thomas (Tom) Marsh.[61]

The Executive Order also directed the formation of an Infrastructure Protection Task Force (IPTF), to be chaired by the DOJ, and with full-time representation from the FBI, NSA, DOD, and part-time support from the other Federal departments and agencies. The IPTF would be an interim response team to address any infrastructure events or crises before the Commission had time to complete its work or the President to make decisions based upon the Commission's findings and recommendations.[62]

General Accounting Office: Information Security--Opportunities for Improved OMB Oversight of Agency Practices

On 24 September 1996, the General Accounting Office issued a report to Congress entitled, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices.* In the report, the GAO confirmed that over a two-year period, beginning in September 1994, serious computer security

vulnerabilities had been identified in 10 of the 15 largest Federal agencies. Based upon the findings, the GAO concluded that poor information security was a widespread Federal problem "with potentially devastating consequences." The report recommended that the Office of Management and Budget (OMB) assume a more proactive role in overseeing agency practices and managing improvements.[63]

Defense Science Board: 1996 Task Force on Improved Application of Intelligence to the Battlefield

At the direction of the Under Secretary of Defense for Acquisition and Technology, the Defense Science Board established a Task Force to review and evaluate the progress made in implementing the recommendations of the 1995 Defense Science Board Task Force on Improved Application of Intelligence. The 1995 study focused on United States peacekeeping efforts in the Bosnia Theater of Operations. The new Task Force was directed to identify further actions that could be taken in support of the coalition forces in Bosnia prior to and during their planned redeployment out of country. Finally, the 1996 Task Force was directed to compile Information Technology and its in-theater application "lessons learned" from the Bosnia deployment and recommend longer-term actions to prepare for future engagements and contingencies.[64]

The Task Force met from May through July 1996, led, as in the 1995 study, by Mr. Charles Gandy and General James O. McCarthy, USAF (Ret.). Unlike the technology focus of the 1995 effort, the 1996 Task Force

concerned itself with and focused its attention on contributions that changes in operations and doctrine could make in leveraging the technologies and telecommunications infrastructures recommended in the Task Force's 1995 final report. Three broad areas, the Task Force reported, require a "special sense of urgency" for their implementation to support the anticipated redeployment of coalition forces within the Bosnian Theater of Operations:

- Continuing the process of getting information and tools down to the battalion level;
- Executing a paradigm shift where higher level Intelligence Centers become more proactive and push tailored products to lower level users via improved techniques for "smart pull," i.e., proactively extracting data rather than awaiting its distribution;
- Organizing collection management teams to integrate data from national theater, and organic intelligence, surveillance, and reconnaissance assets and provide the warfighter with needed information.[65]

The Task Force final report reflected several themes common to both the 1995 and 1996 study results. First, information dominance for the warfighter can only be achieved after the DOD eliminates the significant internal, "stovepiped" barriers to communications content, bandwidth, and connectivity. Second, information dominance can only be achieved by coordinating and targeting data collection, production, and dissemination

activities directly against the mission requirements of the warfighter, including creating the tools necessary to catalyze the fusion of disparate data sources into a unified battlefield view. Third, by addressing and funding operations, management and equipment requirements down to the lowest echelon, the development and application of information management tools and techniques with the warfighter needs firmly in mind, greatly enhances DOD's chances of improving the application of intelligence to the battlefield.[66]

In the longer term, the Task Force said that information management deserves greater attention, recommending that information systems like those deployed in Bosnia and employing high-bandwidth telecommunications capabilities, be evolved for DOD-wide implementation. The Task Force discovered that DOD's global communications infrastructure, including elements of the Internet, MILNET, and SIPRNET facilitated the concept of information "reachback," i.e., utilizing information resources remote from the battlefield, to be effectively used and accepted in the field. Reachback permits the use of information management facilities remote from the battlefield to store, process, and fuse vast amounts of data, prepare tailored products, and transmit them to the warfighter over large bandwidth communications systems.[67] The Task Force further concluded that the continued evolution and integration of commercial information management tools and techniques, relative to warfighter needs, would help to create the

paradigm shift required to achieve the desired application of intelligence to the battlefield and United States information dominance capabilities.[68]

CONGRESS--1996

United States Senate Committee on Governmental Affairs

In the midst of the Defense Science Board investigation of improved applications of intelligence to the battlefield, on 25 June 1996, Senator Fred Thompson (R-TN), Chairman of the U.S. Senate Committee on Governmental Affairs, presided over hearings of the Permanent Subcommittee on Investigations focused on information warfare programs and capabilities of foreign governments. Speaking on behalf of the Administration, John M. Deutch, Director of Central Intelligence, offered the text of a white paper entitled, "Foreign Information Warfare Programs and Capabilities," as part of his prepared testimony.[69]

In his remarks, Director Deutch identified the threat of Strategic Information Warfare (SIW) against the United States by terrorists, rogue nations, and foreign powers, as a matter of "greatest concern":

> My greatest concern is that hackers, terrorist organizations, or other nations might use information warfare techniques as part of a coordinated attack designed to seriously disrupt infrastructures such as electric power distribution, air traffic control, or financial sectors, international commerce, and deployed military forces in time of peace or war. Virtually any "bad actor" can acquire the hardware and software needed to attack some of our critical information-based infrastructures. Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation or foreign terrorist organization that is interested in developing an

> information warfare capability. In fact, hackers with or without their full knowledge may be supplying advice and expertise to rogue states, such as Iran and Libya.[70]

In concluding his testimony, Director Deutch referenced the findings of a National Intelligence Council (NIC) study produced to assess foreign Strategic Information Warfare (SIW) capabilities and plans:

> While the details are classified and cannot be discussed here, we have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks. At present, most of these efforts are limited to information dominance on the battlefield; that is, crippling an enemy's military command and control centers, or disabling an air defense network prior to launching an air attack. However, I am convinced that there is a growing awareness around the world that advanced societies, especially the United States, are increasingly dependent on open, and potentially vulnerable information systems.[71]

S.982: The National Information Infrastructure Protection Act of 1996

On I August 1996, S.982, the National Information Infrastructure Protection Act of 1995 was reintroduced by Senator Jon Kyle (R-AZ) as the National Information Infrastructure Protection Act of 1996. The bill was read twice and referred to the Committee on Judiciary on 1 August 1996. The Committee Chair, Senator Orin Hatch (R-UT) ordered the bill reported out favorably on 2 August 1996. The bill was placed on the Senate Legislative Calendar No. 563 under General Orders on 27 August 1996 and Senator Hatch filed a written report under the authority of the order of the 2 August finding (Report No. 104-357).[72]

On 18 September 1996, the Senate approved the measure by unanimous consent. Two minor amendments, proposed by Senator Hatch, were passed by unanimous consent of the Senate on 19 September 1996. The measure was forwarded to the House Committee on the Judiciary on 19 September 1996. On 4 October, the House Committee on the Judiciary referred the Senate bill to the House Subcommittee on Crime.[73] No further actions were taken on this measure.

H.R. 4095: The National Information Infrastructure Protection Act of 1996

Two days before receiving Senate bill S.982, H.R. 4095, the National Information Infrastructure Protection Act of 1996, was introduced to the House of Representatives on 17 September 1996. Sponsored by Congressman Robert Goodlatte (R-VA), the House companion bill to S.982 was intended to further revise certain provisions of the Federal criminal code regarding fraud and related activity in connection with computers.[74]

The National Information Infrastructure Protection Act of 1996 Act would set penalties with respect to anyone who knowingly accessed a United States Government computer without authorization or, exceeding the authorized access, obtained restricted information or data and willfully communicated that information to anyone not entitled to receive it, or willfully retained it and failed to deliver it to the U.S. officer or employee entitled to receive it.[75]

The House Resolution was referred to the House Committee on the Judiciary on 17 September 1996 and from there to the Subcommittee on Crime on 4 October 1996. There was no floor action taken on this bill. Once again, as in previous attempts, the Congress failed to pass an infrastructure protection-related, computer access control measure.[76]

CLINTON ADMINISTRATION--1997

The White House: A National Security Strategy for a New Century

In May 1997, and in accordance with Section 603 of the Goldwater-Nichols Defense Reorganization Act of 1986, the White House delivered to Congress a global security assessment and strategy for the national security entitled, *A National Security Strategy for a New Century.*[77]

Dependence on the nation's critical information infrastructure, though not an underlying theme of the Clinton Administration strategy articulated in *A National Strategy for a New Century*, is identified as an "overarching capability necessary for the continued worldwide application of United States national power":

> The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well.[78]

President's Commission on Critical Infrastructure Protection (PCCIP)

Pursuant to Executive Order 13010 and the formal creation of the President's Commission on Critical Infrastructure Protection (PCCIP), President Clinton established an Advisory Committee to provide independent guidance to the PCCIP. In addition to the Advisory Committee, President Clinton established a Steering Committee to provide senior Department-level guidance and high-level liaison between the White House and General March's PCCIP. While the PCCIP began holding its hearings in the spring of 1997, President Clinton announced several key appointments to both the Advisory and Steering Committees. On 6 June 1997, the President announced the appointment of Jamie Gorlick as Chair and Maurice R. Greenberg, Margaret Greens, Erle Nye, and Floyd Emerson as members of the Advisory Committee to the Commission. Gorlick had previously served first as Chair of the Joint Security Commission in 1994 and then as a member of the DOJ's Critical Infrastructure Working Group (CIWG) in 1995. The findings and recommendations of this Working Group helped spawn EO 13010 and the PCCIP.

This announcement was followed on 11 July 1997 by the announcement by the President of the appointment of Attorney General Janet Reno, Donald Gips, and Brigadier General Donald Kerrick (USA) as members of the Steering Committee. On 13 August 1997, President Clinton announced his appointment of former Senator Sam Nunn (D-GA) as Co-

Chair of the Steering Committee, along with David Campbell, Charles Lee, and Elvin Moon as members of the Steering Committee. This announcement was followed two weeks later on 27 August 1997 with the announcement of the appointment of Deputy Secretary of Defense John J. Hamre as a member of the Advisory Committee.

On 18 September 1997, the President announced the appointment of Jeffrey Jaffe, Mayor Sharon Sayles Belton of Minneapolis, MN, and Joseph Holmes as members of the Advisory Committee to the President's Commission on Critical Infrastructure Protection. This announcement was followed on 21 October by the appointment of Robert L Baxter, also as an Advisory Committee member.

On 13 October 1997, two days shy of 15 months to the day President Clinton announced the formation of the PCCIP, General Marsh delivered to the President the Commission's final report entitled, *Critical Foundations: Protecting America's Infrastructures.* In his conveyance letter to President Clinton, General Marsh stated that, though the Commission found no evidence of an impending "electronic Pearl Harbor," it found the United States' increasing dependence on networked information and communications systems a "source of rising vulnerabilities":

> We found no evidence of an impending cyber attack, which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm--particularly through information

networks--is real; it is growing at an alarming rate; and we have little defense against it.[79]

Underscoring a major Clinton Administration position, Marsh concluded his letter by stating that, although the majority of the nation's telecommunications assets and networks are owned by the private sector, the Commission found that critical infrastructure protection must be a shared responsibility between the public and private sectors:

> Because the infrastructures are mainly privately owned and operated, we concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors. The only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government. Consequently, in addition to our recommendations about improving our government's focus on infrastructure assurance in the Information Age, you will find some recommendations for collaborative public and private organizational arrangements that challenge our conventional way of thinking about government and private sector interaction.[80]

The Commission report drew four significant conclusions from its 15-month study of United States critical infrastructure protection issues. The main conclusions reached are:

- First, critical infrastructure protection is central to the nation's defense, both in terms of national security and national economic power;
- Second, the growing complexity and interdependence between critical infrastructures create an increased possibility that minor or routine infrastructure disturbances or outages could cascade into national security emergencies;

- Third, vulnerabilities are increasing steadily and the means to exploit weaknesses are readily available; practical measures and mechanisms must be urgently undertaken before the United States is confronted with a crisis of national proportions;
- Fourth, establishing a foundation for critical infrastructure security will depend on achieving new mechanisms for and levels of cooperation between the public sector and the private sector, owners and operators of many of the critical infrastructures upon which the national and economic securities depend.

The Commission identified a framework of seven strategic objectives for establishing what the PCCIP considered "an essential foundation" to a longer-term effort of sustained critical infrastructure protection. The objectives identified by the Commission are:

- **Objective 1:** Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.[81]
- **Objective 2:** Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.[82]
- **Objective 3:** Establish national structures that will facilitate effective partnership between the Federal Government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning, and programs.[83]

- **Objective 4:** Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.[84]

- **Objective 5:** Initiate a series of information security management activities and related programs demonstrating government leadership.[85]

- **Objective 6:** Sponsor legislation to increase the effectiveness of Federal infrastructure assurance and protection efforts.[86]

- **Objective 7:** Increase the investment in Information Assurance research from $250 million to $500 million in FY1999, with incremental increases in investment over a five-year period to $1 billion in FY2004. Target investment in specific areas with high potential to produce needed improvements in infrastructure assurance.[87]

The Commission recommended that the quickest and most effective way of achieving a significant increase in the level of protection from cyber threats would be a cooperative strategy of information sharing and technology exchanges between private sector infrastructure owners and operators and their government agency counterparts. To facilitate this new partnering relationship, the Commission acknowledged that new mechanisms would be needed within government to promote and extend private sector cooperation and information sharing, while at the same time, protecting proprietary information.[88]

The Commission recommended establishment of Sector information clearinghouses (i.e., telecommunications, banking, transportation, etc.) to provide a focus for industry cooperation and data exchange with their government agency counterparts. The Commission recommended creation

of a private-public sector council, made up of industry CEOs, representatives from state and local governments, and Cabinet secretaries, to provide policy advice and implementation commitments as the principal critical infrastructure liaison to the White House. The Commission also recommended that the government establish a real-time capability for attack warning, analysis, and assessment. Finally, the Commission recommended that a top-level, policy- making office be created within the White House to serve as a focus for the government's resources and efforts to assure critical infrastructure protection.[89]

In articulating its, "Strategy for Action," the Commission recommended the adoption of four, government-led, practical measures to promote the Administration's vision of a government-private sector partnership for critical infrastructure protection:

> Infrastructure protection must be ingrained in our culture, beginning with a comprehensive program of education and awareness. This includes both infrastructure stakeholders and the general public, and must extend through all levels of education, both academic and professional. The Federal Government must lead the way into the Information Age by example, tightening measures to protect the infrastructures it operates against physical and cyber attack. The government can also help by streamlining and clarifying elements of the legal structure that have not kept pace with technology. Some laws capable of promoting assurance are not as clear or effective as they could be. Others can operate in ways that may be unfriendly to security concerns. Sorting them out will be an extensive undertaking, involving effort at local, state, Federal, and international levels.
>
> The government must lead in research and development. Some of the basic technology tools needed to provide improved

> infrastructure protection already exist, but need to be widely employed. However, there is a need for additional technology with which to protect our essential systems. We have, therefore, recommended a program of research and development focused on those needed capabilities.[90]

The Commission recommended that government investment in infrastructure research should increase from the FY1998 level of $250 million to $500 million in FY1999, with additional incremental increases over a five year period to $I billion by FY2004.[91]

The Commission's views and its recommendations did not meet with universal approval. Mark Rotenberg, Executive Director of Washington, D.C.'s Electronic Privacy Information Center (EPIC) warned that the recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP) constituted:

> A proposal to extend the reach of law enforcement, to limit the means of government accountability, and to transfer more authority to the world of classification and secrecy. These proposals are more of a threat to our system of ordered liberty than any single attack on our infrastructure could ever be.[92]

Rotenberg and EPIC were responding to PCCIP recommendations to the President to create a new Federal security bureaucracy, with expansive authority over both public and private sector infrastructure, including the National Information Infrastructure (NII) and all aspects of electronic commerce. The EPIC report, entitled "Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection," called the Commission to

task for recommending that national intelligence agencies, in particular the National Security Agency (NSA), expand their areas of responsibility beyond the current international intelligence role, to incorporate lead roles in domestic computer security. "If not properly monitored and controlled, these new national security structures may be used by the government and private corporations to further erode the privacy of United States and foreign citizens," the report said. Responding for the Clinton Administration, Richard Clarke stated, "We think we can defend computer systems without encroaching on privacy rights."[93]

President's Commission on Critical Infrastructure Protection (PCCIP): Legal Foundations Study--Privacy Laws and the Employer-Employee Relationship

In December 1997, the President's Commission on Critical Infrastructure Protection issued a white paper entitled, "Privacy Laws and the Employer-Employee Relationship." This report was issued at the conclusion of one of twelve special studies undertaken by the PCCIP in preparing its results entitled, *Critical Foundations: Protecting America's Infrastructures.* These studies were undertaken to garner opinions and suggest options for addressing legal impediments associated with Federal Government and private sector efforts at protecting the nation's critical infrastructures.[94]

"Privacy Laws and the Employer-Employee Relationship," explores the options available to the Federal Government to ensure that an adequate legal foundation exits for the collaborative collection, archiving, and

exchange of public and private sector personnel information, deemed essential for achieving the Infrastructure Assurance (IA) objectives of the United States. The study explores avenues available to private-sector owners of critical infrastructure for legally employing methods used at the Federal level to screen employees in sensitive security-related positions. These methods are generally unavailable for use by the private sector, due to restrictions in current Federal and state law.[95]

The effective screening of personnel employed with privately owned and operated critical infrastructures, without violating the privacy rights of those employees, is a key issue in Infrastructure Assurance. This is due to the historical threat posed by employees working within those infrastructures. A 1997 CSI/FBI computer security survey revealed that 87% of survey respondents cited "disgruntled employees" as the most likely source of cyber attacks within their company.[96] A 1994 *University of Missouri at Kansas City Law Review* article cites insider theft as responsible for $120 billion dollars in annual commercial losses.[97] Despite these alarming statistics, few recommendations have been made to address the problem due to reluctance on the part of legislators and jurists alike, concerned over enacting and enforcing sweeping security statutes that infringe on the legitimate privacy rights of law-abiding citizens.[98]

Privacy issues associated with "insider threats" to United States critical infrastructures is but one of two legal challenges addressed by the

study. The second issue relates to the issue of states' rights versus federalism. The PCCIP white paper notes that though the Federal Government has jurisdiction over the nation's critical infrastructures through its interstate commerce powers, and despite at times enacting heavily regulatory controls of many critical infrastructures, the Federal Government has left issues associated with employee privacy to the respective states. This is consistent with the constitutional authority granted the states to exercise general policing powers, including legislating for the public health, safety, morals, and welfare of their citizens. The result has been an inconsistent treatment of employee privacy rights by the states. The paper concludes by suggesting that overarching Infrastructure Assurance objectives create a de facto need for an exemption to the states-based privacy status quo.[99]

CLINTON ADMINISTRATION--1998

Presidential Decision Directive 62: Combating Terrorism

After more than four years of studies and debate over issues central to critical infrastructure protection, on 22 May 1998, President Clinton signed Presidential Decision Directive 62 (PDD-62), Combating Terrorism. PDD-62 is a framework for a more systematic approach by the United States in addressing the threat from terrorism. It reinforces the mission of many agencies charged with combating terrorism, while attempting to codify and clarify roles and responsibilities across the range of United States counter-

terrorism programs, from apprehension and prosecution to enhancing physical and cyber security and protection of key assets and critical infrastructures.[100]

PDD-62 highlights the growing threat of unconventional terrorist attacks against the United States and establishes a mechanism for creating a more nationally focused and comprehensive effort to combat such terrorist acts. To accomplish these goals, PDD-62 established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, reporting to the President through the Assistant to the President for National Security Affairs. President Clinton announced the appointment of Richard Clarke to the Office of the National Coordinator. The National Coordinator is charged with overseeing the broad range of national programs in the areas of counter-terrorism, critical infrastructure protection, national preparedness and consequence management in the use of weapons of mass destruction by terrorists against the United States.[101]

The National Coordinator chairs the Critical Infrastructure Coordination Group, a policy coordination and implementation advisory group of senior agency and Department officials at the assistant secretary level or higher. Through this forum, the National Coordinator provides the Office of the President advice on agency budget requests for combating terrorism.[102]

Presidential Decision Directive 63: Protecting America's Critical Infrastructure

In parallel with the release of PDD-62 on 22 May 1998, President Clinton issued PDD-63, Protecting America's Critical Infrastructure. PDD-63 embodies the major critical infrastructure protection policy declarations of the Clinton Administration through 1998. In PDD-63, the Clinton Administration defined "Critical Infrastructures" as those physical and information technology-based systems essential to the minimum operation of the economy and the government, including systems supporting the nation's telecommunications, energy, banking and finance, transportation, water, emergency services, and essential government functions. As these infrastructure systems have become more and more reliant on Information Technology (IT), they have become more automated and more interdependent. The efficiencies realized through IT have come at the cost of making these critical systems vulnerable to equipment failure and natural disaster, but also to malicious destruction through physical and/or cyber-based terrorist attack or nontraditional network-centric warfare.[103]

Through PDD-63, the Clinton Administration established national goals for achieving an initial critical infrastructure protection operating capability by the year 2000, along with the elimination of any significant vulnerabilities to the nation's critical infrastructures by May 2003. PDD-63 defined this to mean the elimination of any exploitable infrastructure weaknesses that would significantly diminish:

> The ability of the Federal Government to perform essential national security missions and to ensure the general public health and safety; the ability of state and local governments to maintain order and to deliver minimum essential public services; and the ability of the private sector to ensure orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.[104]

The recurring public-private partnership theme of the Clinton Administration's Information Technology policy became a hallmark of PDD-63 and its implementation. PDD-63 embodies the Clinton Administration conviction that the nation's information infrastructure must evolve under private sector investment and ownership and that the protection and defense of both privately held and government owned critical infrastructure resources would depend on the evolution of an effective private-public sector partnership:

> Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the United States Government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.[105]

PDD-63 identified sectors of the national infrastructure, primarily in the private sector, which provide critical services or functions. It designated lead agencies within the Federal Government to work as liaisons with these identified sectors, to begin building public-private partnerships. PDD-63

additionally recognized that the traditional elements of national defense, foreign affairs, intelligence, and law enforcement are basic foundation components, fundamental to infrastructure protection, and as such are inherently the domain of the government. PDD-63 stipulated that sector coordinators be designated for these areas from the associated lead government agencies.[106]

To execute the provisions of PDD-63, the Federal Government created four, new or expanded organizations: a Critical Infrastructure Coordination Group; an expanded National Infrastructure Protection Center (NIPC) headquartered within the FBI; private-sector Information Sharing and Analysis Centers (ISACs); and, a public-private sector liaison council, the National Infrastructure Assurance Council (NIAC). A National Plan Coordination Staff would work with and among the separate organizations to focus the group activities toward evolving a national plan for critical infrastructure assurance.

Critical Infrastructure Coordination Group (CICG). In addition to the identification of lead agencies for government internal and private sector external coordination, PDD-63 created an interagency Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, to coordinate the implementation of the directive.[107]

National Infrastructure Protection Center (NIPC). PDD-63 enlarged the role of the FBI's National Infrastructure Protection Center (NIPC). The NIPC is an interagency center operating within the FBI. The center is designed to include representatives from the FBI, DOD, the intelligence community, other Federal departments and agencies, State and local law enforcement, and private industry.[108] PDD-63 expanded the NIPC into a truly national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.[109]

Information Sharing and Analysis Center (ISAC). PDD-63 introduced the concept for and promoted the establishment of a private-sector Information Sharing and Analysis Center (ISAC). ISACs serve as clearing houses for government consultations with owners and operators of the various critical infrastructures defined in PDD-63.[110]

National Infrastructure Assurance Council. Finally, PDD-63 established a mechanism for creating a National Infrastructure Assurance Council upon the recommendation of the lead agencies, the National Economic Council, and the National Coordinator. President Clinton used that mechanism to establish a National Infrastructure Assurance Council, to be made up of a panel of major infrastructure providers and state and local government officials to coordinate public-private sector partnering in the protection of the nation's critical infrastructures.[111]

General Accounting Office: Information Security--Serious Weaknesses Place Critical Federal Operations and Assets at Risk

On 23 September 1998, the General Accounting Office issued a report to Congress entitled, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk.* This was a follow up to GAO's 24 September 1996 report to Congress, *Opportunities for Improved OMB Oversight of Agency Practices.* In the 1996 report, the GAO confirmed that between September 1994 and September 1996, serious computer security weaknesses had been identified in 10 of the 15 largest Federal agencies.[112] The 1998 report found that the number of Federal agencies having significant computer security vulnerabilities had grown to 22. These agencies include the National Aeronautics and Space Administration and the Departments of Defense, Agriculture, and Treasury.[113]

United States Department of Energy, Sandia National Laboratories: A Common Language for Computer Security Incidents

One of the nagging impediments to the evolution of a national strategy on Information Assurance is a common language and understanding of terms unique to the subject. In October 1998, Dr. John D. Howard and Dr. Thomas A. Longstaff published a first attempt at codifying a "common language" for the field of computer security. Although not an effort to develop a comprehensive dictionary of terms, the goal of the Sandia Common Language Project is to develop and publish a minimum set of "high-level"

terms, along with a structure to indicate their relationship that could be used to classify and understand computer security incident information.[114]

The two long-term objectives of this research are to facilitate timely incident data sharing and analysis and to assure near real-time global exchange of computer security incident indications and warnings. As stated by the authors:

> Much of the computer security information regularly gathered and disseminated by individuals and organizations cannot currently be combined or compared because a "common language" has yet to emerge in the field of computer security. A common language consists of terms and taxonomies (principles of classification) that enable the gathering, exchange and comparison of information. This paper presents the results of a project to develop such a common language for computer security incidents.[115]

Identifying and codifying appropriate classifications and terminologies for computer security related incidents are a first step in developing tools and procedures to be used in the systematic and comprehensive analysis of incident data. Timely incident data sharing and analysis would facilitate improvements in incident response and would facilitate the effectiveness of current and future computer security strategies.[116]

Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office: Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructure

During the summer of 1998 and with its work completed, the PCCIP officially disbanded under Executive Order 13064. In its place was formed

the Transition Office of the President's Commission on Critical Infrastructure Protection. The role of the Transition Office was to ensure that work accomplished by the PCCIP would be transitioned in an orderly manner to its successor, the Critical Information Assurance Office (CIAO). The majority of this body of work was completed by the PCCIP prior to the May 1998 release of Presidential Decision Directive 63, Critical Infrastructure Protection, and the establishment of the Office of Science and Technology Policy of a Critical Infrastructure Protection Research and Development Interagency Working Group. Many of the staff and all of the information the PCCIP collected in preparing its final report were transferred to the newly formed National Plan Coordination Staff of the Office of Science and Technology Policy and to the Critical Information Assurance Office (CIAO).[117]

In July 1998, the Transition Office and the newly formed Critical Infrastructure Assurance Office (CIAO) jointly published *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures.* Building upon the work previously conducted by the PCCIP, this R&D roadmap establishes a notional framework for future critical infrastructure protection and assurance efforts. The work represented a four-month research effort to establish a foundation for the development of technologies to counter threats and to reduce infrastructure vulnerabilities in those areas having the potential for causing significant national security, economic, and social impacts.[118]

The report emphasized that government sponsored research and investment is essential for realization of any near-term or long-term goals of the proposed roadmap. The government research must be accompanied by technology investment and product development in the private sector to ensure that tools useful in critical infrastructure assurance, especially in computer-based systems, are developed and made commercially available. Specific technologies considered are those that protect infrastructure and thereby reduce vulnerability, detect intrusions, and provide warnings. While private sector investments and development activities are outside the scope of this study, the private sector-public sector technology transfer activities that facilitate both government research and development are qualitatively factored into the long-range planning upon which the report is based.[119]

The study team identified more than 70 specific research and development topics. Research and development goals, rationale, priority, and estimated resources required for investment over three specific timeframes--near-term (before 2002), mid-term (before 2005), and long-term (before 2010)--were developed for each research and development topic. Near-term (FY2000-FY2002) and mid-term (FY2003-FY2005) investment needs are estimated in the report to total approximately $2 billion each. The estimate for long-term (FY2005-FY2010) research and development resource needs is $3 billion. Information Assurance (IA) related research and development investments represent approximately one-third of the total

investment portfolio called out in the report. Monitoring and detection R&D represent about 15% of the proposed portfolio of investment; vulnerability assessment, modeling, and simulation represent approximately 10%.[120]

The report emphasized that future critical infrastructure protection and assurance research and development investments must be in concert with the evolving national infrastructure assurance policy. Such policy must provide a framework, the report concludes, for establishing R&D objectives, setting R&D priorities, and shaping multi-year R&D investment portfolios commensurate with the perceived threat and need.[121]

Department of Defense--Joint Publication 3-13: Joint Doctrine for Information Operations

On 9 October 1998, the Department of Defense published *Joint Publication 3-13: Joint Doctrine for Information Operations*. This milestone document represents the establishment of a doctrine and concept of operations (CONOPS) for the use Information Operations (IO) by Unites States' joint forces to support the national military strategy. In his introduction to the document, General Henry H. Shelton, United States Army and Chairman of the Joint Chiefs of Staff, said:

> Our ability to conduct peacetime theater engagement, to forestall or prevent crisis and conflict, and to fight and win is critically dependent on effective IO at all levels of war and across the range of military operations...The guidance contained herein provides joint forces commanders and their component commanders with the knowledge needed to plan, train for, and conduct IO. [122]

As a Joint Doctrine, *Joint Publication 3-13* is an authoritative guidance; as such, the document is mandated policy for joint service IO, to be followed "except when, in the judgement of the commander, exceptional circumstances dictate otherwise."[123]

Joint Publication 3-13 defines Information Operations as:

> Actions taken to affect adversary and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. They are a critical factor in the joint force commander's (JFC's) capability to achieve and sustain the level of information superiority required for decisive joint operations.[124]

Joint Publication 3-13 establishes a detailed understanding of DOD joint services Information Operations. It provides doctrine, principles, and concepts on the fundamentals of Information Operations and its significance to joint operations. The concepts of both offensive and defensive Information Operations are extensively addressed, with an emphasis on individual capabilities and activities. Organization is defined as a key ingredient to successful Information Operations. Equally important are the strategic, operational, and tactical planning aspects of Information Operations. Finally, *Joint Publication 3-13* emphasizes essential preparation of those personnel and organizations responsible for planning and executing Information Operations be achieved through extensive training, modeling, and simulation mirroring the Operations Concept (OPSCON) of *Joint Publication 3-13.*

President's National Security Telecommunications Advisory Committee (NSTAC)

On 3 November 1998, the NSTAC's Legislative and Regulatory Group (LRG) agreed to develop a Telecommunications Outage and Intrusion Sharing Report to address existing and proposed private sector channels for sharing information infrastructure outage and cyber intrusion information with both public and private sector organizations. The report was generated in response to and in assessment of the information infrastructure incident sharing channels identified in President Clinton's Presidential Decision Directive 63, Protecting America's Critical Infrastructure.[125]

The NSTAC/LRG identified ten separate industry and government consortiums established as forums for the sharing of information related to computer and network security, intrusion detection, and reporting. The entities identified are:

- **Agora**, a Seattle, Washington-based forum representing 100 companies, law enforcement, and state and Federal Government officials from 45 agencies from five northwest states and Canada.[126]

- **Computer Emergency Response Team (CERT) Coordination Center**, part of the Software Engineering Institute, a Federally funded research and development (R&D) center at Carnegie Mellon University in Pittsburgh, Pennsylvania, established in response to the Robert Morris University Internet worm incident in 1988.[127]

- **FBI.** Under the Federal provisions of the Computer Fraud and Abuse Act of 1986, the FBI shares jurisdiction for computer crime with the U.S. Secret Service. To facilitate the sharing of incident information, the FBI developed the

National InfraGard Program in Cleveland, Ohio in 1998, with an aim to expanding it to all of its 56 national field offices.[128]

- **FCC**. Title 47 of the Code of Federal Regulations requires that all local exchange common carriers that experience an outage which affects 30,000 subscribers or more, must report the outage in real-time to the FCC's duty officer, if the outage lasts more than 30 minutes. This must be followed by a formal, written report to the FCC within 30 days of the incident.[129]

- **Forum of Incident Response and Security Teams (FIRST)**. FIRST was formed in 1990 following an October 1989 security incident involving the Space Physics Analysis Network (SPAN). FIRST links together over 60 individual incident response teams from educational, commercial, government, law enforcement and military organizations including the CERT Coordination Center, U.S. Air Force CERT, DOE's Computer Incident Advisory Capability, DISA, NASA, and NIST.[130]

- **Information and Communications Sector Liaison Official (SLO/Sector Coordinator [SC])**. As envisioned by PDD-63, an information and communications SLO and SC would be appointed to represent each critical infrastructure in developing a public-private partnership to eliminate vulnerabilities in that critical infrastructure.[131]

- **Information Sharing and Analysis Centers (ISACs)**. PDD-63 calls for the creation of one or more private sector entities to coordinate the sharing of information related to vulnerabilities, threats, intrusions, and anomalies affecting the critical infrastructure.[132]

- **National Coordinating Center for Telecommunications (NCC)**. The NCC was originally established in 1984 to share information on telecommunications outages and to expedite service restoration. The NCC expanded its scope to include the sharing of information relating to electronic intrusions affecting telecommunications critical to national security and emergency preparedness (NS/EP). The NCS Manager operates the NCC.[133]

- **National Infrastructure Protection Center (NIPC).** The DOJ and the FBI created the NIPC in February 1998, as a result of recommendations made by the President's Committee on Critical Infrastructure Protection (PCCIP) to develop an integrated Information Assurance capability to protect the Nation's critical infrastructure. PDD-63 expanded its role significantly directing the NIPC to serve as a national critical infrastructure threat assessment, warning, vulnerability, law enforcement investigation, and response entity.[134]

- **Network Security Information Exchanges (NSIE).** Two NSIE have been formed: an NSTAC NSIE and a government NSIE. Each has a charter membership, but they meet jointly to share information on threats, incidents, and vulnerabilities affecting the public networks. Nondisclosure agreements signed between the principals promotes the sharing of otherwise proprietary information between the represented private sector participants.[135]

CLINTON ADMINISTRATION--1999

Assignment of Lead Agency Responsibility, DOD Information Assurance

A key agency assignment for critical infrastructure protection and Information Assurance fell to the United States Air Force, U.S. Space Command. On 8 April 1999, at the 15th National Space Symposium in Colorado Springs, Colorado, General Richard Myers, Commander-in-Chief (CINC), US Space Command, announced that U.S. Space Command had been given responsibility for coordinating the development of United States' strategy and concept of operations for conducting both defensive and offensive cyberwar. [136]

The seemingly unusual nature of this assignment was explained by General Howell M. Estes III, USAF (Ret), Former Commander in Chief, United States Space Command, during an interview at the 15th Annual National Space Symposium, Broadmoor Hotel, Colorado Springs, CO. General Estes explained:

> This assignment actually makes perfect sense if you consider how utterly dependent the Nation's critical information infrastructure is on space and our space assets. The Nation must evolve a comprehensive critical infrastructure protection policy, much as we at U.S. Space Command, responding to a directive from Washington, evolved the draft of a comprehensive space policy for the protection of our critical space assets and to ensure our continued successful exploitation of the space dimension for our commercial and National security needs.[137]

General Estes' comments were echoed by space policy advocate and author Dr. James Oberg, who opinioned:

> To effectively practice space control, the United States must develop the capability to know what information all satellites are collecting and transmitting, and to whom it is being provided. This requirement is related to U.S. concerns regarding Information Assurance and Information Operations. The National policy community, in concert with the warfighting CINCs, must develop a strategy and policy for space control during times of crises, tensions, and war – whether netwar or physical war is immaterial. We need a crisp policy that defines where the lines will be drawn.[138]

Executive Order 13130: National Infrastructure Assurance Council (NIAC)

On 14 July 1999, President Clinton issued Executive Order 13130, establishing the National Infrastructure Assurance Council (NIAC). The

NIAC, identified as an advisory council in PDD-63, would be composed of 30 members appointed by the President and selected principally from private sector entities representing the critical infrastructures identified in Executive Order 13010, as well as from state and local governments."[139]

The Executive Director of the NIAC would be the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism at the National Security Council, reporting to the President through the Assistant to the President for National Security Affairs.[140]

The main function of the NIAC, as established by EO 13130, was to enhance the partnership of the public and private sectors in protecting the United States' critical infrastructure processes. A major thrust in this direction would be to propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including telecommunications and information systems.[141]

The NIAC was charged with monitoring the development of Private Sector Information Sharing and Analysis Centers (PSISACs), providing recommendations to the National Coordinator and the National Economic Council on how these organizations might best foster improved cooperation among PSISACs, the National Infrastructure Protection Center (NIPC), and other Federal Government agencies.[142]

Executive Order 13133: Working Group on Unlawful Conduct on the Internet

Although the use of new technologies to commit traditional crimes is not new, the quantum advances afforded by Information Technology has provided criminals tremendously powerful, new electronic tools to engage in unlawful conduct. The Internet, in particular, poses a particularly significant challenge to law enforcement. The Internet's easy access and unprecedented speed and reach make it an ideal medium for both legal and illegal activity.

In response to this emerging threat, on 6 August 1999, President Clinton issued Executive Order 13133, establishing the Working Group on Unlawful Conduct on the Internet. The Executive Order 13133 charge to this interagency working group was three-fold: first, determine the extent to which current Federal law provides a sufficient basis for investigation and prosecution of Internet-based crime; second, determine the extent to which new technology/ tools may be required to affect the investigation and prosecution of Internet-based crime; and, third, determine the potential for new or existing tools to educate and empower teachers and parents to prevent or minimize risk from unlawful conduct that involves the use of the Internet.[143]

Pursuant to Executive Order 13133, Attorney General Janet Reno was named Chair of the Working Group on Unlawful Conduct on the Internet. Other charter members of the Working Group would include the Director of

the Office of Management and Budget; the Secretary of the Treasury; the Secretary of Commerce; the Secretary of Education; the Director of the Federal Bureau of Investigation; the Director of the Bureau of Alcohol, Tobacco and Firearms; the Administrator of the Drug Enforcement Administration; the Chair of the Federal Trade Commission; and the Commissioner of the Food and Drug Administration.[144]

Additional agency representation would be added based upon expertise and interest in the subject matter. Representatives from the following Federal agencies expected to participate in the Working Group include the Consumer Product Safety Commission, the United States Customs Service, the DOD, the Department of State, NASA, the National Commission on Libraries and Information Science, the Postal Inspection Service, the United States Secret Service, and the Securities and Exchange Commission.[145]

General Accounting Office: Information Security--Serious Weaknesses Continue to Place Defense Operations at Risk

At the request of Secretary of Defense William S. Cohen, the General Accounting Office undertook a reassessment of the state of DOD information security in a follow-up to GAO audits of DOD computer security practices and vulnerabilities performed in the spring and summer 1996. The 1996 survey resulted in the 22 May 1996 publication of the GAO report, *Information Security: Computer Attacks at the Department of Defense Pose Increasing Risks.* This was followed in September 1996 by a second, limited release

report. This report, designated Limited Official Use due to its sensitive information content, was derived from GAO's analyses and testing of DOD general computer controls. For the purposes of the two reports, GAO defined computer controls as, "the policies and procedures that affect the overall security and effectiveness of computer systems and operations, as opposed to being unique to any specific computer program, office, or operation."[146]

As in the1996 assessment, the GAO found that serious weaknesses in DOD information security continue to plague Defense computing, providing cyber terrorists and other unauthorized intruders to DOD systems the opportunity to modify, steal, or destroy sensitive DOD data. The report cites weaknesses in DOD computer security as impairing DOD's ability to control physical and electronic access to its systems and data and its inability to certify that software running on its systems are functioning as intended. These process deficiencies limit DOD's ability to block the use of Defense computers in performing unauthorized functions, while limiting DOD's ability to recover and reinitialize Defense computing in the event of a system-wide failure or compromise.[147]

In reporting these results to Secretary Cohen, Robert F. Dacey, Director of GAO's Consolidated Audit and Computer Security Issues, said:

> Our current review found that some corrective actions have been initiated in response to the recommendations our 1996 reports made to address pervasive information security weaknesses in DOD. However, progress in correcting the specific control weaknesses identified during our previous reviews has been inconsistent across the various DOD

> components involved and weaknesses persist in every area of general controls. Accordingly, we reaffirm the recommendations made in the 1996 reports.[148]

Although the GAO found that most DOD component activities evaluated did not have effective processes for identifying and resolving computer systems security weaknesses, it did find an exception in the Defense Information Systems Agency (DISA). DISA, which operates DOD's major regional data processing centers, called Defense Megacenters (DMC), had established and, at the time of the report, had begun implementing a comprehensive computer controls and security review process for all of its computing assets. Since 1996, DISA development of Standard Technical Implementation Guides (STIGs), which prescribe detailed standards for configuring system software, and the Security Readiness Review (SRR) process, enables DISA to test DMC compliance with the STIGs and other DISA security standards, allows DISA to track weaknesses identified through the testing, and to monitor and report on corrective actions taken. At the time of the report, DISA had "identified and resolved thousands of security weaknesses."[149]

Despite these positives, GAO found that DISA was still developing guidelines for configuring much of its system software and had not, as yet, completed a security review of all of its computer systems. Further, the GAO audit revealed that some deficiencies reported by DISA as having been

addressed had not actually been affected. This was especially true of security issues identified with the regional DMC's.[150]

In January 1998, DOD announced plans to develop a Defense-wide Information Assurance Program (DIAP) under the auspices and jurisdiction of the DOD's Chief Information Officer. In February 1999, DOD's CIO approved an implementation plan and organizational structure to support the DIAP. And though the GAO report notes that the DIAP implementation plan provides a framework for a comprehensive DOD-wide computer security program, an independent assessment of the efficacy of the plan could not be made at the time of the GAO report.[151]

General Accounting Office: Critical Infrastructure Protection--Report to the Senate Committee on the Year 2000 Technology Problem

On 1 October 1999, Acting Assistant Comptroller General Jeffrey C. Steinhoff, responding to a request for information from Senator Robert F. Bennett (R-UT), Chairmen of the Senate Special Committee on the Year 2000 (Y2K) Technology Problem, issued a summary report of GAO findings on computer security and critical infrastructure protection, in concert with a GAO preliminary analysis of Year 2000 lessons learned applicable to critical infrastructure protection efforts. The summary report, covering the time period February 1997 through September 1999, contained a chronological listing of 197 GAO reports published and transcripts of GAO testimonies presented to Congress concerning Federal computer security topics.[152]

The GAO report identified a wide range of potential risks associated with the nation's reliance on its interconnected computer systems. In his letter accompanying the report, Steinhoff emphasized the GAO Y2K findings on computer-based interdependencies and the vulnerabilities of government computer systems to disruption:

> Recent efforts to address the Year 2000 computing problem have called attention to some important aspects of these risks. It has underscored the need to develop awareness, cooperation, and a disciplined management approach to adequately address such problems. In many ways, the Year 2000 challenge can be viewed as a major test of our nation's ability to protect its computer-supported critical infrastructures; although, protecting critical infrastructures from hostile attacks on a continuous basis will require addressing a broader array of issues.[153]

On 6 October 1999, Jack L. Brock, Jr., Director, Government-wide and Defense Information Systems, Accounting and Management Division, General Accounting Office, testified before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information. Brock testified that recent GAO Inspector General audits of Federal agencies had discovered that 22 of the largest agencies had significant computer security weaknesses. In analyzing these weaknesses, Brock stated:

> Senior agency officials have not recognized that computer-supported operations are integral to carrying out their missions and that they can no longer relegate the security of these operations solely to lower-level technical specialists. For [this] reason, it is essential that this fundamental problem be addressed as part of an effective information technology

> management strategy, which will also serve to strengthen critical infrastructure protection.[154]

Brock went on to state that, while Administration efforts to develop fundamentally sound computer and network policies and guidance were widespread, effective improvements were not taking place. This, Brock contended, was due to the flawed nature of the prevailing "bottoms up approach" employed across government departments and agencies:

> I want to stress that there are no simple solutions to improving computer security throughout government. What is clear is that a bottom-up approach will not work. To begin to meet the lofty goal of PDD-63, making the government a model, will require sustained top management support, consistent oversight, and additional levels of technical and funding support. Taking steps to address the issues outlined in my statement could help the government put its own house in order and more effectively work with the private sector to protect critical infrastructures.[155]

The White House: A National Security Strategy for a New Century

In December 1999, and in accordance with Section 603 of the Goldwater-Nichols Defense Reorganization Act of 1986, the White House submitted to Congress the Clinton Administration's assessment and vision for the United States' national security strategy. Entitled, *A National Security Strategy for a New Century* and nearly twice the volume of the 1997 report (29 versus 49 pages), the 1999 report articulates a more sophisticated view of geopolitics and a more comprehensive introspection on national security planning than evidenced in the 1997 report.[156]

The report, acknowledging the key roles played by information, information processes, and Information Technology in United States military planning and operational readiness, as well as in the command and control of military forces, states:

> Operational readiness, as well as the command and control of forces rely increasingly on information systems and technology. We must keep pace with rapidly evolving Information Technology so that we can cultivate and harvest the promise of information superiority among United States forces and coalition partners while exploiting the shortfalls in our adversaries' information capabilities.[157]

The 1999 report, a milestone for the White House in terms of its recognition of the importance of Information Assurance, addresses critical infrastructure protection as a key component of the Administration's national security strategy. Acknowledging a concern for information attacks that "threaten our citizens and critical national infrastructures at home,"[158] the report states that the nation's security and economy rest on a foundation of critical infrastructures and that the national dependence on these infrastructures places the United States at risk:

> More than any nation, America is dependent on cyberspace. We know that other governments and terrorists groups are creating sophisticated, well-organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depend on them.[159]

The report cites a Clinton Administration commitment to executing a plan for defending United States' critical infrastructures by May 2001 and to

having a fully functional, cyber-defensive capability operational by December 2003:

> We are creating the systems necessary to detect and respond to attacks before they can cause serious damage. For the first time, law enforcement, intelligence agencies and the private sector will share, in a manner consistent with United States law, information about cyber threats, vulnerabilities, and attacks. The government is developing and deploying new technologies to protect Defense Department and other critical Federal systems, and we are encouraging the private sector to develop and deploy appropriate protective technology as well. A nationwide system for quickly reconstituting in the face of a serious cyber-attack is being developed. Every Federal Department is also developing a plan to protect its own critical infrastructures, which include both cyber and physical dimensions.[160]

Finally, echoing a basic and consistent theme of the Clinton Administration that dates to the 1992 presidential campaign, the report states:

> The Federal Government is committed to building this capability to defend our critical infrastructures, but it cannot do it alone. The private sector, as much as the Federal Government, is a target for infrastructure attacks, whether by cyber or other means. A new partnership between the Federal Government and the private sector is required. Acting jointly, we will work to identify and eliminate significant vulnerabilities in our critical infrastructures and the information systems that support them.[161]

Of significant note, the White House's, *National Security Strategy,* would retreat from the Clinton Administration's national goals for achieving critical infrastructure protection by stated in PDD-63, published in 1998. PDD-63 established national goals for achieving an initial critical infrastructure protection operating capability by the year 2000, along with the

elimination of any significant vulnerabilities to the nation's critical infrastructures by May 2003.[162]

CONGRESS--1999

H.R. 2413: The Computer Security Act of 1999

In 1999, after a three-year hiatus, Congress was prepared once again to take action in pursuit of its own information systems security solution. On 1 July 1999, Congressman James Sensenbrenner (R-WI) introduced H.R. 2413, the Computer Security Enhancement Act of 1999. The specific measures identified within the bill were intended to accomplish two goals: first, to assist NIST in meeting the ever-increasing computer security needs of Federal civilian agencies; second, to allow the Federal Government, through NIST, to harness the power and creativeness of the private sector to help address its computer security needs.[163]

The bill would amend the National Institute of Standards and Technology Act by directing NIST to work with the private sector in establishing voluntary interoperable standards for the establishment of non-Federal public-key infrastructures (PKI). The PKI established would then be certified for use in communicating with and conducting business with the Federal Government.[164]

The bill would require NIST to evaluate and test commercially available security products for their suitability for use by Federal agencies for protecting sensitive information in computer systems. At the same time, the

bill would prohibit NIST from promulgating or adopting standards or engaging in security practices that would create a de facto Federal encryption standard that would then be required for use in computer systems other than Federal Government computer systems.[165]

H.R. 2413 would also amend and update the Computer Security Act of 1987 by enhancing the role of the independent Computer System Security and Privacy Advisory Board in NIST's decision-making process. The board, which is made up of representatives from industry, federal agencies and other outside experts, would assist NIST in its development of standards and guidelines for Federal systems.[166]

Finally, H.R. 2413 would address the national shortage of university students studying computer security by establishing a new computer science fellowship program for graduate and undergraduate students studying computer security. This provision of the bill is based upon the statistic that of 5,500 PhDs in Computer Science awarded between 1994-1999 in Canada and the United States, only 16 were in fields related to computer security.[167]

Following its introduction on the House floor on 1 July 1999, H.R. 2413 was referred to the House Committee on Science. In the interest of time, the Committee's Subcommittee on Technology scheduled hearings on the bill for 30 September 1999 and prior to the bill being officially referred from the full Committee. The hearings were held in Room 2318 of the Rayburn House Office Building. Testifying in support of the bill for the Clinton

Administration were Raymond Kammer, Director of the National Institute of Science and Technology, Department of Commerce and Keith Rhodes, Director of the Office of Computer and Information Technology, General Accounting Agency.[168]

On 20 October 1999, the bill was brought before the Subcommittee for consideration. A Subcommittee Mark-up Session was held resulting in the bill being amended and approved on a voice vote before being forwarded by the Subcommittee on Technology to the full Committee on Science. The full Committee took no further action on the bill.[169]

CLINTON ADMINISTRATION--2000

Defending America's Cyberspace: National Plan for Information Systems Protection--An Invitation to a Dialogue

On 7 January 2000, President Clinton unveiled his long-awaited plan for defending America's cyber space entitled, *Defending America's Cyberspace: National Plan for Information Systems Protection--An Invitation to a Dialogue (Version 1.0).* These 159 pages of what Jack L. Brooks, GAO's Director of Governmentwide and Defense Information Systems, described as the "first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks,"[170] in testimony before the House Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, focuses largely on initial Federal efforts undertaken to protect the nation's critical cyber-based infrastructures.

Subsequent versions are to address a broader range of concerns, including the specific role industry and state and local governments will play in protecting physical and cyber-based infrastructures from deliberate attack, as well as international aspects of critical infrastructure protection. The end goal of this process is to develop a comprehensive national strategy for infrastructure assurance as envisioned by Presidential Decision Directive (PDD) 63.

Acknowledging that the plan was a first step in a long-term planning and implementation effort, President Clinton, in his introductory letter accompanying its publication, stated:

> The National Plan for Information Systems Protection is the first major element of a more comprehensive effort. The Plan for cyberdefense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats. It presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety.
>
> For this plan to succeed, government and the private sector must work together in a partnership unlike any we have seen before. This effort will only succeed if our Nation as a whole rises to this challenge. Therefore, I have asked the members of my Cabinet to work closely with representatives of the private sector industries and public services that operate our critical infrastructures. We cannot mandate our goals through government regulation. Each sector must decide for itself what practices, procedures, and standards are necessary for it to protect its key systems. As part of this partnership, the Federal Government stands ready to help.[171]

Protection of the critical computer-based information infrastructures of the United States is essential to the national security. President Clinton

directed the development of this Plan toward the goal of attaining a national capability to protect the nation's critical information infrastructure by the year 2003. To achieve this goal, Version 1.0 of the Plan was designed around three broad objectives supported by ten executable programs. These three objectives and their subordinate programs are designed to make the United States Government a model of information security, while laying the foundation for the requisite public-private partnership necessary to defend the nations critical information infrastructure. The Plan objectives and programs are:

- Objective 1, Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on the nation's critical information networks and build an infrastructure that remains effective in the face of such attacks.
  - Program 1: Calls for the government and the private sector to identify key assets and shared interdependencies, focusing on shared vulnerabilities of critical infrastructure components to cyber attack.[172]
- Objective 2, Detect and Respond: Develop the capabilities necessary to identify and asses a cyber attack in a timely way, contain the attack, minimizing collateral damage, recover and then reconstitute the affected systems with the least amount of damage or loss of user capability.
  - Program 2: Calls for the installation of advanced intrusion detection devices, scanners, firewalls, anomalous behavior identifiers,

enterprise-wide management systems, and malicious code scanners to detect attacks and unauthorized intrusions into Federal computing systems.

- Program 3: Directs the law enforcement and intelligence communities of the Federal Government to develop robust intelligence, enforcement capabilities and tools to protect critical information systems, consistent with United States statutes.
- Program 4: Calls for the creation of a more effective, nationwide system to share cyber attack warnings and attack assessment data in a timelier manner. This nation-wide system is intended to be inclusive of the private sector, as well as to state and local governments, on a voluntary basis.
- Program 5: Creates capabilities for attack response, infrastructure system reconstitution, and network recovery to limit the effectiveness of a cyber attack and to institutionalize system attack and recovery planning, including provisions for rapid deployment of defensive measures, isolation of affected network nodes, automated fail-overs to secure system enclaves, support for minimal essential operations, and rapid repair and reconstitution of affected systems.[173]

- Objective 3, Build Strong Foundations: Establishes requirement to create the requisite infrastructure and national support necessary to enable the

United States to prepare, prevent, detect, and respond to attacks on the nations' critical information networks and infrastructures.

- Program 6: Established the research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that United States information security technology stays ahead of the evolving cyber threat.
- Program 7: Calls upon the government to institute the necessary actions to train and retain an adequate Federal Information Technology staff, including on-going recruitment and education of additional personnel to meet skill-level shortfalls.
- Program 8: Requires that the government conduct an extensive outreach and education program to secure the public support for the need to act responsibly before a catastrophic cyber terror event.
- Program 9: Challenges the government to evolve the necessary laws and legislative framework to enable the initiatives and programs of this Plan.
- Program 10: Requires that in every step and component of the Plan, full protection of American citizens' civil liberties are ensured by creating the necessary mechanisms within each program to highlight and address privacy and data protection issues and rights.[174]

Version 1.0 of the Plan was clearly focused on current efforts being undertaken by the Federal Government to protect the nation's critical cyber-

based infrastructures. According to John Tritak, Director of the Critical Infrastructure Assurance Office, subsequent versions of the plan would be more broadly focused:

> Later versions of the Plan will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interest and concerns expressed by Congress and the general public based on their feedback. That is why the Plan is designated Version 1.0 and subtitled An Invitation to a Dialogue--to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.[175]

Jack I. Brock, Jr., Director of Governmentwide and Defense Information Systems of GAO's Accounting and Information Management Division, testifying before the Senate Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary expressed stronger reservations about the Plan:

> There are opportunities for improvement as the Plan is further developed as well as significant challenges that must be addressed to build the public-private partnerships necessary for infrastructure protection. In particular, we believe the Plan should place more emphasis on providing agencies the incentives and tools to implement the management controls necessary to assure comprehensive computer security programs, as opposed to its current strong emphasis on implementing intrusion detection capabilities. In addition, the Plan relies heavily on legislation and requirements already in place that, as a whole, are outmoded and inadequate as well as poorly implemented by the agencies.[176]

Department of Justice: Attorney General Janet Reno Testimony on Computer Crime Before the Senate Committee on Appropriations

Computer hacking and other unauthorized intrusions into United States computer-based information infrastructure, including those perpetrated by foreign governments or operators outside the United States are a violation of United States Federal law. As such, their investigation and disposition under the law falls within the purview of the Department of Justice. The Computer Crime and Intellectual Property Section (CCIPS), an organization of the Department of Justice's Criminal Division, and its attorney staff of 18 lawyers, focuses exclusively on issues pertaining to computer and intellectual property crime. CCIPS attorneys advise Federal prosecutors and law enforcement agents, comment upon and propose legislation, coordinate international efforts to combat computer crime, litigate cases, and train all law enforcement groups on computer crime and intellectual property law. Other areas of expertise possessed by CCIPS attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations, and intellectual property crimes.[177]

A substantial number of CCIPS attorneys hold degrees in computer science, engineering, and other technical fields. Approximately half of the attorney staff has prior government or private sector experience in computer-related or computer-related legal positions. CCIPS was originally formed in 1991 as the Computer Crime Unit of the former General Litigation and Legal

Advice Section of DOJ's Criminal Division. CCIPS became a Section of the Criminal division in 1996.[178]

In her 16 February 2000 testimony on "Cybercrime" before the United States Senate Committee on Appropriations, Attorney General Janet Reno stated:

> The cornerstone of our prosecutor cybercrime program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS...With the help of this Subcommittee, CCIPS has grown from five attorneys in January 1996, to eighteen attorneys today. CCIPS works closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators" (CTCs) in United States Attorney's Offices around the country. Each CTC is given special training and equipment, and serves as the district's expert in computer crime cases.
>
> In addition, CCIPS provides expert legal and technical instruction and advice for exercises and seminars to senior personnel on information warfare, infrastructure protection, and other topics...CCIPS also led the Department's efforts to counter cyberterrorism through its work on PDD-63, the Five-Year Counterterrorism Strategy, and its support to the National Infrastructure Protection Center.[179]

Executive Order 13133: Working Group on Unlawful Conduct on the Internet

Pursuant to Executive Order 13133, in March 2000, the President's Working Group on Unlawful Conduct on the Internet published its report entitled, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet.* Chaired by Attorney General Janet Reno, the Working Group was chartered by President Clinton to provide an initial

analysis of legal and policy issues surrounding the use of the Internet to commit unlawful acts.[180]

Based upon the specific charge of the President's Executive Order, the Working Group established a three-fold framework for examining the issue of unlawful conduct on the Internet. First, the Working Group examined the extent to which existing Federal law is sufficient to address unlawful conduct involving the use of the Internet. Second, the Working Group assessed the extent to which new tools, capabilities, or legal authorities may be needed for effective investigation and prosecution of such conduct. Third, the Working Group examined the potential for using education and empowerment tools to minimize the risks or impacts from unlawful use of the Internet.[181]

Consistent with the Clinton Administration's overall Internet technology policy, the Working Group conclusions and three-part recommendations for addressing unlawful conduct on the Internet assumed a technology-neutral approach, looking to the private sector for leadership:

- First, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that accounts for other important societal interests such as privacy and protection of civil liberties;

- Second, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and

among Federal, state, and local law enforcement agencies, and coordination with and among international counterparts; and,

- Third, there should be continued support for private sector leadership and the development of methods—such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts—that educate and empower Internet users to prevent and minimize the risks of unlawful activity.[182]

General Accounting Office: Information Security--Serious and Widespread Weaknesses Persist at Federal Agencies

On 28 July 2000, Congressman Stephen Horn (R-CA), Chairman of the House Subcommittee on Government Management, Information and Technology, Committee on Government Reform, wrote to Director Robert F. Dacey, the General Accounting Office Director of Information Security, requesting a summary of recent GAO security audits of Federal agencies. Director Dacey, responding to Congressman Horn in a letter dated 6 September 2000 and appended in the GAO report entitled, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies,* stated:

> This report summarizes audit findings for the 24 Federal agencies that were included in a similar review that we reported on in September 1998--agencies that, during fiscal year 1999, accounted for almost 99 percent of Federal outlays. In our 1998 report, we concluded that significant computer security weaknesses had been reported for each of those agencies and that, as a result, critical Federal operations and assets were at risk.[183]
>
> Evaluations of computer security published since July 1999 continue to show Federal computer security is fraught with weaknesses and that, as a result, critical operations and assets

> continue to be at risk. As in 1998, our current analysis identified significant weaknesses in each of the 24 agencies covered by our review. Since July 1999, the range of weaknesses in individual agencies has broadened, at least in part because the scope of audits being performed is more comprehensive than in prior years. While these audits are providing a more complete picture of the security problems agencies face, they also show that agencies have much work to do to ensure their security programs are complete and effective.[184]

While the GAO report cites a number of factors contributing to weak Federal computer system security, the report identifies poor security program management and poor administration of control techniques as fundamental, underlying causes. While agencies have taken steps to begin the process of remediating the most glaring of computer system security deficiencies, 1999-2000 GAO audit results validate Federal agencies have not as yet incorporated even the most fundamental management practices necessary for ensuring that computer-based controls and security measures can be successfully implemented.[185]

CONGRESS--2000

In February 2000, House Speaker J. Dennis Hastert (R-IL) established a cybersecurity team comprised of 18 senior Republican members of Congress.[186] The Republicans, all in leadership positions within the House committee structure and led by Congressman J. C. Watts (R-OK), were directed to use their positions of authority within the Republican Congressional leadership hierarchy to share computer security information with other lawmakers from both political parties. Speaker Hastert formed the

congressional team in part as a result of denial-of-service attacks on commercial web sites in January and February 2000. Hastert stated:

> We must recognize that there are cyberrogues out there who want to cause trouble and create mischief. We should see to it that our privacy, financial information and electronic commerce transactions are protected, while allowing the Internet to grow unfettered.[187]

H.R. 4246: Cyber Security Information Act

On 12 April 2000, Representative Thomas M. Davis (R-VA) introduced H.R. 4246, the Cyber Security Information Act, a bill to encourage the secure disclosure and protected exchange of information concerning cyber security problems, solutions, test practices, test results, and related matters in connection with critical infrastructure protection. The bill would address concerns raised by industry over the voluntarily sharing of critical infrastructure protection information with the government due to antitrust laws, Freedom of Information Act (FOIA) disclosure, or liability issues. [188]

After its reading on the House floor, the bill was referred concurrently to the House Committees on Government Reform and on the Judiciary, for consideration of provisions of the bill falling within the jurisdictions of each Committee.[189]

On 8 May 2000, the House Government Reform Committee referred the bill to its Subcommittee on Government Management, Information and Technology for consideration. On 22 June 2000, the Subcommittee held formal hearings on the bill. Representing the Clinton Administration in

support of H.R. 4246 was Joel C. Willemssen, Director of Civil Agencies Information Systems, Accounting and Information Management Division, General Accounting Office. In his testimony before the Subcommittee, Director Willemssen provided a blunt assessment of the state of federal computer security and critical infrastructure protection:

> By removing private sector concerns about sharing information on critical infrastructure threats, H.R. 4246 can facilitate private-public partnerships and help spark the dialogue needed to identify threats and vulnerabilities and to develop response strategies. For the concepts in H.R. 4246 to work, however, this legislation needs to be accompanied by aggressive outreach efforts; effective centralized leadership; and good tools for collecting, analyzing, and sharing information. Moreover, the Federal Government cannot realistically expect to engage private-sector participation without putting its own house in order. Doing so will require concerted efforts by senior executives, program managers, and technical specialists to institute the basic management framework needed to effectively detect, protect against, and recover from critical infrastructure attacks. Moreover, it will require cooperative efforts by executive agencies and by the central management agencies, such as OMB, to address crosscutting issues and to ensure that improvement are realized.[190]

Following the Subcommittee hearings, the bill was returned to the full Committee, where it was tabled.[191]

H. CON. RES. 285: Expressing the Sense of Congress Regarding Internet Security and Cyberterrorism

On 15 March 2000, Representative Jim Saxson (R-NJ) introduced House Concurrent Resolution 285, expressing the sense of Congress regarding Internet security and cyberterrorism. H. CON. RES. 285 designates cyberterrorism as an emerging threat to the national security of

the United States, having the potential to cause great harm to the nation's critical electronic Infrastructure. H. CON. RES. 285 calls for:

- A partnership between the Federal Government and private industry in combatting the "cyber menace";
- A revised legal framework for the prosecution of "hackers" and "cyber terrorists";
- A new interagency study to be conducted by the Departments of Commerce and Defense, the National Security Agency, the Central Intelligence Agency, and the Federal Bureau of Investigation to assess the threat posed by "cyberterrorists." [192]

H. CON. RES. 285 was read twice on the floor of the House of Representatives, then forwarded concurrently to the House Committees on the Judiciary and Commerce, for a period of time to be subsequently determined by the Speaker of the House and for consideration of those provisions falling within the respective jurisdictions of the two standing Committees.[193] No action has been taken by either Committee to move the bill along.

S. 2430: Internet Security Act of 2000

On 13 April 2000, Senator Patrick Leahy (D-VT) introduced S 2430, the Internet Security Act of 2000, a bill to combat computer hacking through enhanced law enforcement and to protect the privacy and constitutional rights of United States citizens from being electronically violated as a result of:

> Acts that damage or attempt to damage computers used in the delivery of critical infrastructure services such as telecommunications, energy, transportation, banking, and financial services, and emergency and government services pose a serious threat to public health and safety and cause or have the potential to cause loss to victims that include costs of responding to offenses, conducting damage assessments, and restoring systems and data to their condition prior to the offense, as well as lost revenue and costs incurred as a result of interruptions of service.[194]

The Act would amend Section 1030 of title 18, United States Code giving the United States Government jurisdiction to investigate acts affecting protected computers, even if the acts take place outside the United States.[195] The bill would also establish a grant program, in the amount of $25 million for each of fiscal years 2000 through 2003, to help state and local law enforcement agencies in enforcing state and local criminal laws relating to computer crime, provide training and public education, acquire equipment, and facilitate the sharing of information and expertise between Federal law enforcement officials and those at the state and local levels.[196]

On 13 April 2000, S. 2430 was read twice on the floor of the Senate and then referred to the Committee on the Judiciary. No action was taken by the Committee to advance the bill to the full Senate for disposition.[197]

S. 2448: Internet Integrity and Critical Infrastructure Protection Act of 2000

On 13 April 2000, Senator Orrin G. Hatch (R-UT) introduced S. 2448, the Internet Integrity and Critical Infrastructure Protection Act of 2000, a bill to enhance security protections on the Internet by making it illegal for interactive

computer services, i.e., Internet service providers (ISPs), from disclosing any personally identifiable information without the subject's consent. The bill would also amend the United States Criminal Code to provide criminal penalties for engaging in fraudulent acts on the Internet where the defendant is proven to have involved individuals of less than 18 years of age to commit the offense, or when the offense causes damage to a government computer system used in the administration of justice, national defense, or national security.[198]

The bill would also require the United States Attorney General to appoint a Deputy Assistant Attorney General for Computer Crime and Intellectual Property to advise Federal prosecutors and law enforcement personnel regarding computer and intellectual property crime and coordinate national and international activities for combating such crime.[199]

On 13 April 2000, S. 2448 was read twice on the floor of the Senate and was then referred to the Senate Committee on the Judiciary. The bill failed to advance out of Committee.[200]

H.R. 2413: Computer Security and Enhancement Act of 2000

On 24 October 2000, Representative James Sensenbrenner (R-WI) reintroduced H.R. 2413 as the Computer Security Act of 2000, asking unanimous consent of the House Members to suspend the House rules and approve the bill, as amended. Previously referred to the House Committee on Science, where it had been amended and then reported favorably out of

Committee on 24 July 2000, H.R. 2413 was the 2000 version of Congressman Sensenbrenner's Computer Security Act of 1999. The previous version of bill had not made its way out of committee prior to the end of the 1st Session of the 106th Congress.

In his remarks introducing H.R. 2413 to the House Members, Congressman Sensenbrenner stated:

> Mr. Speaker, H.R. 2413 updates the Computer Security Act of 1987 to improve computer security for Federal civilian agencies and the private sector. The Computer Security Act of 1987 gave authority over computer and communications security standards and Federal civilian agencies to NIST. The Computer Security Act of 2000 strengthens that authority and directs funds to implement practices and procedures, which will ensure that the Federal standards-setting process remains open to public input and analysis. When implemented, the bill will provide guidance and assistance on protection of electronic information to Federal civilian agencies.
>
> Since 1993, the General accounting Office has issued over 35 reports describing serious information security weaknesses at major Federal agencies. In 1999, the GAO reported that during the previous two years serious information security control weaknesses had been reported for most of the Federal agencies. Recently, the GAO gave the Federal Government an overall grade of D-minus for its computer security efforts. Specifically, hearings held by the Committee on Science earlier this year identified information security leaks in the Department of Energy and the Federal Aviation Administration that threaten our Nation's safety, security, and economic well-being.
>
> Much has changed in the years since the Computer Security Act of 1987 was enacted. The proliferation of networked systems, the Internet, and Web access are just a few of the dramatic advances in information technology that have occurred. The Computer Security Act of 2000 addresses these changes, promotes the use of commercially available products, and encourages an open exchange of information between NIST and the private sector, all of which will help facilitate

> better security for Federal systems. Finally, the legislation is technology neutral and is careful not to advocate any specific computer security or electronic authentication technology.[201]

Though enjoying a generally bipartisan support in the House, upon announcement by Speaker pro tempore Hansen that H.R. 2413 had been approved by voice vote, Congressman Hall (D-TX) objected, raising a point of order on the ground that a quorum was not present. Accordingly and pursuant to House Rule XX, Clause 8, the Speaker pro tempore postponed further proceedings on Congressman Sensenbrenner's motion for approval of H.R. 2413. However, later that day, a motion to reconsider was laid on the table and was agreed to without exception. The bill was passed by the House on a voice vote and received in the Senate for consideration the following day, 25 October 2000. No further action was taken by the Senate on this bill.[202]

SUMMARY

Critical infrastructures are among the basic foundations of society. As such, their defense is of strategic concern to the preservation of the security and economy of society. No nation has been as advantaged or has benefited as much from Information Technology and the advent of the Information Age as the United States. Computer-based information infrastructures and networks interconnect vital aspects of life in the United States, as in no other country. The unprecedented economic and technological advantages that Information Technology and electronic commerce have created for the

United States sustains the nation as the world's only true economic and military superpower. But this pre-eminence comes at a price. Those same infrastructures that underpin and underwrite this society and its economic and military power are also its Achilles heel. Vulnerabilities in the critical national infrastructures, particularly those supporting computer-based information, place the economic and security interests of the United States at risk.

The Information Age phenomenon of computer hacking has spawned an unprecedented Information Age threat in the form of cyber terrorism. Employing the same commercially available tools and techniques used to build this vast electronic latticework of interconnected services, individuals, groups, and even nations, using the global reach of the World Wide Web, can disrupt or destroy the vast interconnected network of computer systems that underpin this nation's security, economy, and society.

Over a nearly eight year period, the Clinton Administration expended considerable resources and energy to defend a critical infrastructure policy heavily dependent on the private sector assuming the lion's share of responsibility for the protection of the nation's information networks. For the first time in the nation's history, the defense of a vital part of the nation's essential societal foundation, its Information Age electronic infrastructure, is primarily left in the hands of the private sector, giving rise to question's concerning the Federal Government's responsibility to "provide for the

common defense." The wisdom of that policy and its effect on Information Assurance policy remain very much in question.

The case study results from this Chapter Seven, Critical Infrastructure Protection Policy and Legislative Initiatives During the Clinton Administration (1993-2000), along with the results from the preceding two chapters, Chapter Five, Federal Information Technology Policy and Legislative Initiatives During the Clinton Administration (1993-2000) and Chapter Six, Federal Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), serve as the foundation for the case study analysis in Chapter Eight. In Chapter Eight, the PIES Model is applied to the results of the case studies from Chapters Five, Six and Seven, establishing a framework for the systematic analysis of the evolution of Clinton Administration Information Assurance policy between 1993 and 2000.

[1] The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue,* 7 January 2000.

[2] Ibid, iii.

[3] Graham Allison, *Essence Of Decision: Explaining the Cuban Missile Crisis,* (Boston, MA: Little, Brown and Company, 1971), 1-2.

[4] National Communications System, *Background and History,* http://www.ncs/html/NCSHistoryBkgrd. html, 1.

[5] Ibid., 1.

[6] Ibid., 1.

[7] The President's National Security Telecommunications Advisory Committee, *Information Infrastructure Group Report,* September 1997, ES-1.

[8] Ibid., ES-1.

[9] Ibid., ES-2.

[10] Executive Order 12472 of April 3, 1984, *Federal Register,* Vol. 49. No. 67, as reprinted on http://www.ncs.gov/ncs/html/Executive Order12472.htm, 1.

[11] Ibid., 1.

[12] Ibid., 1.

[13] *NCS Manager,* http://www.ncs.gov/ncs/, 1.

[14] United States General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, D.C.: GAO/AIMD-96-84), 22 May 1996, 32.

[15] Ibid., 31.

[16] Ibid., 33.

[17] Ibid., 33.

[18] Ibid., 33.

[19] Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence from the Joint Security Commission,* 28 February 1994, ix.

[20] Ibid., ix.

[21] Ibid., ix.

[22] GAO/AIMD-96-84, 32.

[23] Joint Security Commission, 4.

[24] United States Department of Defense, Office of the Under Secretary of Defense for Acquisition and Technology, Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington D.C.: October 1994), ES-1.

[25] Ibid., 58.

[26] Ibid., 37

[27] Ibid., 23.

[28] Ibid., 36.

[29] Ibid., 24.

[30] Ibid., ES1-2.

[31] The President's National Security Telecommunications Advisory Committee, *Information Infrastructure Group Report,* September 1998, 1.

[32] Letter from Mr. William T. Esprey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States, the Honorable William Jefferson Clinton, 20 March 1995.

[33] Letter from the President of the United States, William Jefferson Clinton, to William Esprey, Chair of NSTAC, dated 7 July 1995.

[34] The President's National Security Telecommunications Advisory Committee, *Information Infrastructure Group Report,* September 1997, ES-1.

[35] The President's National Security Telecommunications Advisory Committee, *Information Infrastructure Group Report,* September 1998, 1.

[36] Op. Cit., 6.

[37] Ibid., ES-2.

[38] United States Department of Defense, Office of the Under Secretary of Defense for Acquisition and Technology, Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Improved Application of Intelligence to the Battlefield: May-July 1995* (Washington D.C.: September 1995), 3.

[39] Ibid., 5-8.

[40] Ibid., 28-35.

[41] United States Department of Commerce, Critical Infrastructure Assurance Office, *Statement of John S. Tritak, Director, Critical Infrastructure Assurance Office Before the Subcommittee on Technology, Terrorism and Government Information, Senate Judiciary Committee,* 6 October 1999, 2.

[42] Ibid., 2.

[43] United States Department of Defense, Office of the Under Secretary of Defense for Acquisition and Technology, Defense Science Board, *Report of the Defense Science Board Task Force On Information Warfare-Defense: November 1996 [IW-D]* (Washington, D.C.: 25 November 1996), 3.

[44] Ibid., 3.

[45] Duane P. Andrews, Chairman, Defense Science Board Task Force on Information Warfare (Defense), letter to Dr. Craig I. Fields, Chairman, Defense Science Board, 21 November 1996.

[46] Op. Cit., 3-146.

[47] Paul Richter, "Need for Anti-Terrorism Chief Debated," *Los Angeles Times* (23 January 1999), A11.

[48] Congress, Senate, Senator Jon Kyle of Arizona, "National Infrastructure Protection Act of 1995/6," S.982, 104th Congress, 2d sess., *Congressional Record* (8 February 1996), S9554.

[49] United States General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, D.C.: GAO/AIMD-96-84), 22 May 1996, 1.

[50] Ibid., 2.

[51] Ibid., 19.

[52] Ibid., 3

[53] Ibid., 22.

[54] Ibid., 23.

[55] Ibid., 4.

[56] Ibid., 4.

[57] Ibid., 4-5.

[58] Ibid., 40.

[59] Ibid., 41.

[60] Executive Order 13010, Critical Infrastructure Protection, Section 4, 15 July 1996, 1.

[61] Ibid., Section 7 (d).

[62] Ibid., Section 7 (d).

[63] United States General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110: 24 September 1996).

[64] United States Department of Defense, Office of the Under Secretary of Defense for Acquisition and Technology, Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Improved Application of Intelligence to the Battlefield: May-July 1996* (Washington D.C.: 3 March 1997), 3.

[65] Ibid., 4.

[66] Ibid., 4.

[67] Ibid., 20.

[68] Ibid., 4.

[69] John M. Deutch, Director, Central Intelligence Agency, "Foreign Information Warfare Programs and Capabilities," Testimony before the U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, 25 June 1996, 1

[70] Ibid., 2.

[71] Ibid., 2.

[72] Op. Cit., S10890 & H10672.

[73] Ibid., S10890 & H10672.

[74] Congress, House, Representative Robert Goodlatte of Virginia, "National Information Infrastructure Protection Act of 1996," H.R. 4095, 104th Congress, 2nd sess., *Congressional Record* (17 September), H10524 [17SE].

[75] Ibid., H10524.

[76] Ibid., H10524.

[77] The White House, *A National Security Strategy for a New Century,* May 1997, i.

[78] Ibid., 14.

[79] The White House, President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, i.

[80] Ibid., i.

[81] Ibid., 93.

[82] Ibid., 94.

[83] Ibid., 95.

[84] Ibid., 96.

[85] Ibid., 97.

[86] Ibid., 97.

[87] Ibid., 98-99

[88] Ibid., xi.

[89] Ibid., xi.

[90] Ibid., xi.

[91] Ibid., 98-99.

[92] Christopher J. Dorobek, "Report: White House's Cyberdefense Too Close for Comfort," *Government Computer News*, vol. 17, no. 39 (23 November 1998), 12.

[93] Ibid., 12.

[94] The White House, President's Commission on Critical Infrastructure Protection, *Privacy Laws and the Employer-Employee Relationship: A Legal Foundations Study,* Report 9 of 12, December 1997, 1.

[95] Ibid., 1.

[96] Ibid., CSI/FBI 1997 Computer Security Survey.

[97] Rochelle B. Ecker, "To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee," *University of Missouri at Kansas City Law Review*, Vol. 63 (1994), 251-252.

[98] The White House, President's Commission on Critical Infrastructure Protection, *Privacy Laws and the Employer-Employee Relationship: A Legal Foundations Study,* Report 9 of 12, December 1997, 4.

[99] Ibid., 4.

[100] The White House, Office of the Press Secretary, Fact Sheet: "Combating Terrorism: Presidential Decision Directive 62," 22 May 1998, 1.

[101] Ibid., 1.

[102] Ibid., Section IX, Annex A, 8.

[103] The White House, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," Section I (May 1998), 1.

[104] Ibid., Section I, 2.

[105] Ibid., Section IV, 3.

[106] Ibid., Section VI, 4.

[107] Ibid., Section VI, 1,4.

[108] Ibid., 19.

[109] President's National Security Telecommunications Advisory Committee, *Outage and Intrusion Information Sharing Report,* December 1998, 18.

[110] PDD-63, Section IX, Annex A, 8.

[111] Ibid., 8-9.

[112] United States General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110), 24 September 1996, 2.

[113] United States General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (Washington, D.C.: GAO/AIMD-98-92), 23 September 1998, 3.

[114] John D. Howard, Ph.D. and Thomas A. Longstaff, Ph.D., *A Common Language for Computer Security Incidents,* SAND98-8667 (Albuquerque, New Mexico: Sandia National Laboratories, October 1998), ii.

[115] Ibid., ii.

[116] Ibid., 18-19.

[117] The White House, Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Office, *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures,* July 1998, vii.

[118] Ibid., xiii.

[119] Ibid., 1-2; 1-3.

[120] Ibid., C-37.

[121] Ibid., 4-2.

[122] United States Department of Defense, *Joint Publications 3-13: Joint Doctrine for Information Operations,* 9 October 1998, i.

[123] Ibid., i.

[124] Ibid. vii.

[125] President's National Security Telecommunications Advisory Committee, *Outage and Intrusion Information Sharing Report,* December 1998, ES-1.

[126] Ibid., 4-5.

[127] Ibid., 6-7.

[128] Ibid., 8-9.

[129] Title 47 of the Code of Federal Regulations, Chapter 1, Subchapter B, Part 63.100 (b) (c).

[130] Ibid., 9-11.

[131] Ibid., 12-13.

[132] Ibid., 14-15.

[133] Ibid., 16.

[134] Ibid., 18-19.

[135] Ibid., 20-21,

[136] General Richard Myers, USAF, Commander in Chief, U.S. Space Command, Briefing and follow-up interview, 15th Annual National Space Symposium, Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

[137] General Howell M. Estes III, USAF (Ret), Former Commander in Chief, United States Space Command, interview, 15th Annual National Space Symposium, Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

[138] Dr. James E. Oberg, *Space Power Theory.* Interview. 15th Annual National Space Symposium, Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

[139] Executive Order 13130, Section 1, 14 July 1999.

[140] Ibid., Sections 1(b) and 3(B).

[141] Ibid., Sections 2 (1)-(2).

[142] Ibid., Section 2 (3).

[143] Department of Justice, President's Working Group on Unlawful Conduct on the Internet, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet," March 2000, 6-7.

[144] Ibid., 7.

[145] Ibid., 9.

[146] United States General Accounting Office, *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (Washington, D.C.: GAO/AIMD-99-107), 26 August 1999, 1.

[147] Ibid., 3.

[148] Ibid., 3.

[149] Ibid., 3-4.

[150] Ibid., 4.

[151] Ibid., 17.

[152] United States General Accounting Office, *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (Washington, D.C.: GAO/AIMD-00-1), 1 October 2000, 32-47.

[153] Ibid., 3-4.

[154] Jack L. Brock, Jr., "Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations," Testimony before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate, 6 October 1999, 2.

[155] Ibid., 11.

[156] The White House, *A National Security Strategy for a New Century,* December 1999, 1-48.

[157] Ibid., 12.

[158] Ibid., 16.

[159] Ibid., 17.

[160] Ibid., 18.

[161] Ibid., 18.

[162] The White House, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," Section I (May 1998), 1.

[163] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 1999," H.R. 2413, 106th Congress, 1st sess., *Congressional Record* (1 July 1999), E1491.

[164] Ibid., E1491.

[165] Ibid., E1491.

[166] Ibid., E1491.

[167] Ibid., E1492.

[168] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 1999," H.R. 2413, 106th Congress, 1st sess., *Daily Digest* (30 September 1999), D1070.

[169] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 1999," H.R. 2413, 106th Congress, 1st sess., *Bill Summary and Status* (25 October 2000), 1.

[170] United States General Accounting Office, *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection*, Testimony of Jack L. Brooks, Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, United States Senate (GAO/T-AIMD-00-72), 1 February 2000, 2.

[171] The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0--An Invitation to a Dialogue*, January 2000, iii.

[172] Ibid., xi.

[173] Ibid., xi.

[174] Ibid., xii.

[175] United States Department of Commerce, Critical Infrastructure Assurance Office, *Statement by John S. Tritak, Director, Critical Infrastructure Assurance Office before the Subcommittee on Government Management, Information and Technology, House Government Reform Committee,* 9 March 2000, 2.

[176] Testimony of Jack L. Brock Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, United States Senate, 1 February 2000, 2.

[177] United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), *What Does CCIPS DO?, http://www.usdoj.gov/criminal/cybercrime/ccips.html*, 16 March 2000. 1.

[178] Ibid., 1.

[179] Ibid., 1.

[180] The White House, The President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, March 2000, 3-4.

[181] Ibid., 4.

[182] Ibid., 53.

[183] United States General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (Washington, D.C.: GAO/AIMD-00-295), 6 September 2000, 1.

[184] Ibid., 2.

[185] Ibid., 27.

[186] Beside Watts, the members of the Congressional team identified were Representatives Brian Bilbray, David Dreier, Steve Horn, Steve Kuykendall, and Jim Rogan of California; Bill McCollum of Florida; Jim Shimkis of Illinois; Connie A. Morella of Maryland; Vern Ehlers of Michigan; Charles Bass of New Hampshire; Heather Wilson of New Mexico; Robin Hayes of North Carolina; Don Sherwood of Pennsylvania; Pete Sessions of Texas; Tom Davis and Bob Goodlatte of Virginia; and Orderrge Nethercutt of Washington.

[187] Shiruti Date, "House Speaker Hastert Sets Up Security Team of GOP Members," *Government Computer News*, vol. 19, no. 5 (13 March 2000), 1.

[188] Congress, House, Representative Thomas M. Davis of Virginia, "Cyber Security Information Act," H.R. 4246, 106th Congress, 2nd sess., *Bill Summary and Status for the 106th Congress* (12 April 2000), 1, *Congressional Record,* H2238.

[189] Ibid., H2238.

[190] United States General Accounting Office, *Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000,* Testimony of Joel C. Willemssen, Director, Civil Agencies Information Systems, Accounting and Information Management Division, Before the Subcommittee on Government Management, information and Technology, Committee on Government Reform, House of Representatives (GAO/T-AIMD-00-229), 22 June 2000, 11.

[191] Op. Cit., H2238.

[192] Congress, House, Representative Jim Saxton of New Jersey, "Expressing the sense of the Congress regarding Internet security and 'Cyberterrorism'," H. CON. RES. 285, 106th Congress, 2nd sess., *Bill Summary and Status for the 106th Congress* (15 March 2000), 2.

[193] Ibid., 1.

[194] Congress, Senate, Senator James Leahy of Vermont, "Internet Security Act of 2000," S. 2430, 106th Congress, 2nd sess., *Bill Summary and Status for the 106th Congress* (13 April 2000), 3-4.

[195] Ibid., 4.

[196] Ibid., 8.

[197] Ibid., 1.

[198] Congress, Senate, Senator Orrin G. Hatch of Utah, "Internet Integrity and Critical Infrastructure Protection Act of 2000," S.2448, 102nd Congress, 2nd sess., *Bill Summary and Status for the 106th Congress* (13 April 2000), 1-2.

[199] Ibid., 4.

[200] Ibid., 1.

[201] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin, "Computer Security Enhancement Act of 2000," H.R. 2413, 106th Congress, 2nd sess., *Congressional Record* (24 October 2000), H10608.

[202] Ibid., H10610.

CHAPTER EIGHT

ANALYZING THE GOVERNMENT'S INFORMATION TECHNOLOGY/INFORMATION ASSURANCE POLICY INITIATIVES (1993-2000)

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

This chapter is devoted to a comprehensive mapping of the Information Technology, Encryption, and Critical Infrastructure Protection policy elements that frame United States Information Assurance policy. The case study results from Chapter Five, Federal Information Technology Policy and Legislative Initiatives During the Clinton Administration (1993-2000), Chapter Six, Federal Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), and Chapter Seven, Critical Infrastructure Protection Policy and Legislative Initiatives During the Clinton Administration (1993-2000), serve as the foundation for the modeling and data analyses presented in this chapter. The PIES Model, introduced previously in this study, is applied to the results of the three case studies, establishing a framework for the systematic analysis of the evolution of Clinton Administration Information Assurance policy between January 1993 and December 2000.

The chapter is organized into three sections, with each corresponding to one of the three Information Assurance policy threads studied: Federal Information Technology policy, Federal Encryption policy, and Critical

Infrastructure Protection policy are individually decomposed, mapped, and analyzed within the PIES framework.

BACKGROUND--SETTING THE STAGE

Near the end of the Clinton Administration in December 2000, Federal Information Assurance (IA) policy existed as a patchwork of intersecting elements of pre-1993 policy fragments and evolving Clinton Administration Information Technology, Encryption, and Critical Infrastructure Protection policy elements. Although the individual components of this evolving Information Assurance policy were mostly complimentary, an analysis reveals that key interdependencies underlying these policies created at least three major tensions within United States Information Assurance policy.

First, Clinton Administration Information Technology policy championed rapid growth in electronic commerce and government, global networking, and multi-billion dollar, multi-year government investments in advanced telecommunications research and development, with a near term focus on the Next Generation Internet (NGI). These were core elements of the Administration's Information Technology policy. Simultaneously, Clinton Administration Encryption and Critical Infrastructure Protection policies did little to promote the essential information assurance technologies and infrastructures critical to securing the electronic data exchanges upon which the United States economy and security had grown increasingly dependent.

Second, the Clinton Administration's Information Assurance policy

suffered from an inherent tension between the national security and law enforcement imperative for access to all electronic information exchanges, against the public's right to privacy and the security assurances guaranteed by United States law for these electronic exchanges. This conflict underscored a fundamental incongruency between information security elements of the Clinton Administration's Encryption policy and information access elements of the Administration's Information Technology policy.

One end of the continuum represents the Clinton Administration's eight-year Information Technology policy investment in the National Information Infrastructure (NII), collaborative efforts with the private sector to create the Next Generation Internet (NGI), and efforts to ensure universal connectivity to the electronic Global Information Infrastructure (GII). Opposite are the Administration's eight-year efforts at restricting the export, sale, and use of data encryption products through highly restrictive encryption product and technology export and domestic use polices, e.g., the ill-fated key escrow/Clipper Chip program. These fundamental efforts in support of enhanced national security and law enforcement access to electronic data flowing across the NII, NGI, and GII were in direct conflict with the fundamental rights of these users to assured privacy and data integrity.

Third, the principal goal of the Clinton Administration's Critical Infrastructure Protection policy was to align the private and public sectors into an essential partnership, providing the means for the electronic "common defense" of United States critical infrastructures. In particular, this policy

focused on fundamental protections for those networked information infrastructures that underpin many crucial aspects of the society. In contrast, the Federal government's forty-year Encryption policy worked unrelentingly to ensure that even basic data encryption and computer security technologies remained out of the public's hands.

To address these policy conflicts and related Information Assurance policy issues, the Clinton Administration executed a broad array of Executive Orders and Presidential Decision Directives (refer to Appendix C); sponsored or supported complimentary legislation in Congress in support of a broad category of Information Assurance issues inherent in Information Technology Encryption, and Critical Infrastructure Protection policies; established both government and public-private sector technical and political advisory Presidential Commissions and Committees; and established a host of new government organizations to implement these policies (refer to Appendix D). These actions resulted in the creation of a new Federal bureaucracy, charged with resolving these Information Technology, Encryption, and Critical Infrastructure Protection tensions, while developing a comprehensive, integrated Information Assurance policy.

INFORMATION ASSURANCE (IA) POLICY ANALYSIS USING THE POLICY AS AN INCREMENTAL EVOLUTIONARY SPIRAL (PIES) FRAMEWORK

The Policy as an Incremental Evolutionary Spiral (PIES) conceptual framework, introduced in Chapter 1 and detailed in Chapter 2 of this study,

was used to map and then analyze the myriad elements of the Clinton Administration Information Assurance (IA) policy. As Figure 8-1 depicts, the PIES macro-framework decomposes the policy process into seven distinct lifecycle phases: Conceptualization, Promotion, Initialization, Implementation, Sustainment, Exit/Termination, and Post Analysis.

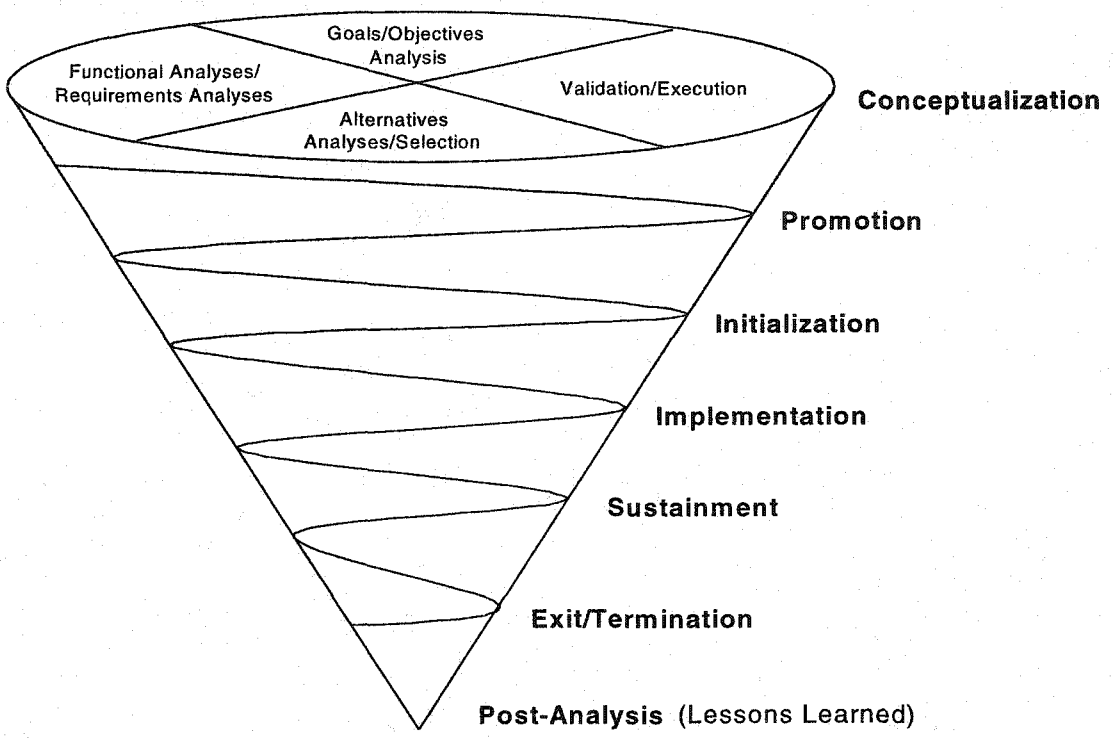


Figure 8-1: PIES Lifecycle Macroframework

Within the macro-framework, PIES decomposes each lifecycle phase into a series of policy iterations, depicted in the model as horizontal cross-sections representing an n-number of policy decision-making spirals. Each cross-sectional spiral represents a single iteration of the policy lifecycle,

evolving though each of four lifecycle states or quadrants: Goals/Objectives Analyses, Functional/Requirements Analyses, Alternatives Analyses/ Selection, and Validation/Execution. Within each phase, each increment of the evolving policy is iterated through a decision continuum, cycling as many times through the spiral as necessary for the requisite policy phase to evolve. Figure 8-2 depicts three concentric iterations of a single PIES policy spiral.

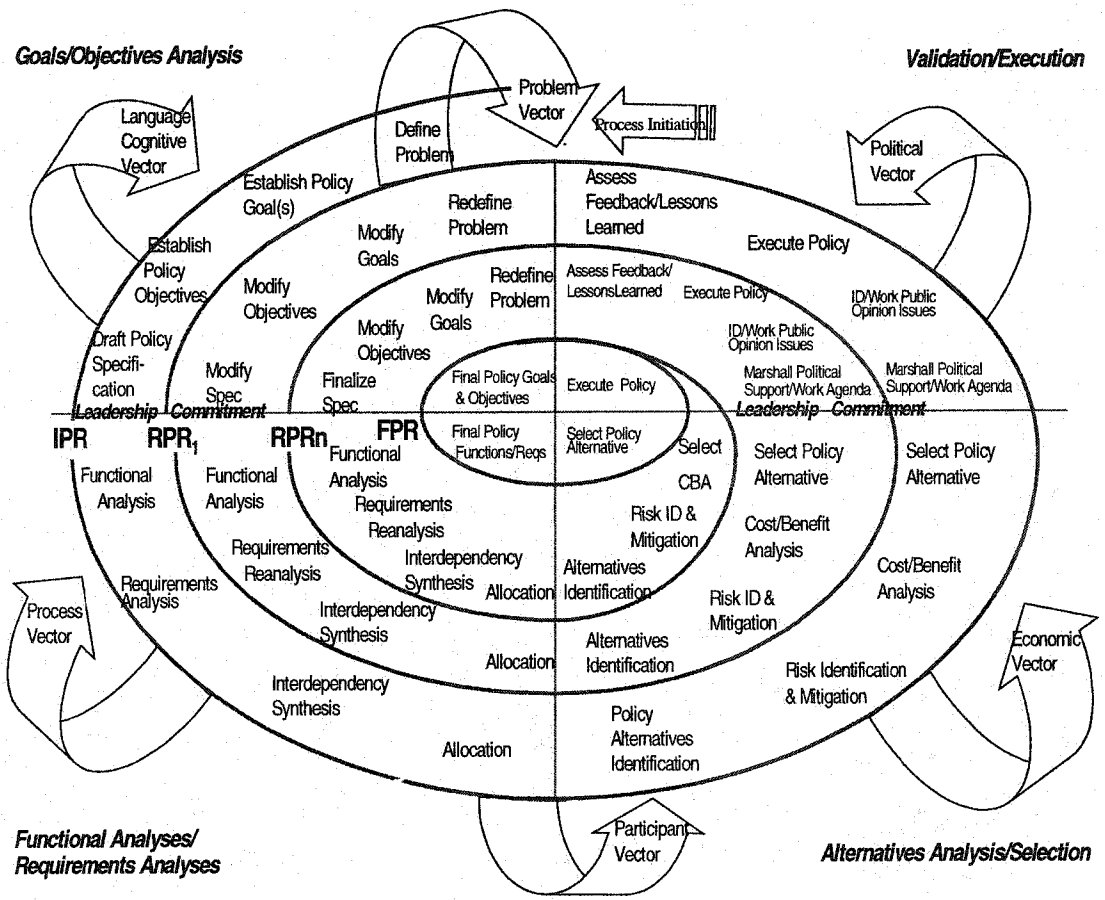


Figure 8-2: PIES Lifecycle Policy Spiral

FOUNDATIONS OF FEDERAL INFORMATION ASSURANCE POLICY: PIES INFORMATION TECHNOLOGY POLICY ANALYSIS

A formal strategy for creating a national information network had always been of central importance to the Clinton Administration. Prior to his election to the Presidency in November 1992, Candidate Clinton observed:

> In the new economy, infrastructure means information as well as transportation. More than half the United States' workforce is employed in information-intensive industries, yet we have no national strategy to create a national information network. Just as the interstate highway system in the 1950s spurred two decades of economic growth, we need a door-to-door fiber optics system by the year 2015 to link every home, every lab, every classroom, and every business in America... We should also change the way we create infrastructure for the next century. New sources of investment capital can be tapped from the private sector, in partnership with government. For example, we should consider creating a Federal, self-financing public-private corporation to support viable infrastructure projects that can attract some private capital.[1]

In January 1993, Clinton Administration plans for a National Information Infrastructure (NII) coalesced around results anticipated from research under the newly established High-Performance Computing and Communications (HPCC) Program. These results were key to President Clinton's ability to fulfill campaign pledges to answer the growing demand for a globally interconnected, electronic information infrastructure and to further encourage the growth of an e-Commerce sector valued, in 1993, at over $40 billion.

> The Clinton Administration believes that the Federal Government has several important roles to play in assisting the development of this infrastructure, which will be built and run primarily by the private sector. In many ways, the High-Performance Computing and Communications (HPCC)

Program provides the technological foundation upon which the Administration's strategy for the NII rests. [2]

The High-Performance Computing and Communications (HPCC) Program, authorized under provisions of PL 102-194, the High-Performance Computing Act of 1991, introduced on 24 January 1991 as S. 272 by Senator Albert Gore (D-TN), served as the centerpiece for all Clinton Administration National Information Infrastructure (NII) initiatives.

The HHPC Program also proved central to furthering the virtual government capabilities envisioned by the Administration's National Performance Review (NPR), unveiled on 1 September 1993. NPR's goal to reform the Federal administrative structure, in line with that of private industry, proved very much dependent on fundamental changes in the way government utilized Information Technology to perform its mission.[3]

In articulating its "Reinventing Government" plan, the NPR team identified a number of fundamental issues, each requiring the application of Information Technology to promote efficiency in the delivery of government services:

- The Information Technologies currently employed by the Federal Government were not delivering what the customer needed, nor was its potential being fully utilized;
- The Federal Government did not adequately coordinate its existing information systems;
- There was an insufficient understanding of who the customers for Information Technology were and what their needs were;

- Too many barriers existed within the government, both regulatory and legislative, to use Information Technology effectively;

- All levels of government workforce needed continuous education in Information Technology.[4]

President Clinton's initial formal act in support of these goals was to direct the Office of Science and Technology Policy (OSTP) to establish an Information Infrastructure Task Force (IITF) in May 1993. This was followed, in September 1993, by Executive Order 12864, which established the United States Advisory Council on the National Information Infrastructure (NII).

Information Technology Policy Vectors--Implementation Phase (IP)

Through the legacy left it by the out-going Bush Administration and the 102nd Congress, the Clinton Administration enjoyed the considerable advantage of inheriting a very useable Information Technology policy framework that comported to its own political needs. This Information Technology framework had evolved through its Conceptualization, Promotion, and Initialization Phases, culminating in the enactment of Public Law 102-194, the High-Performance Computing Act of 1991 and the establishment of the High-Performance Computing and Communications (HPCC) Program. For the Clinton Administration, its vision for United States Information Technology policy began to evolve with the initial policy (IP) iteration of the Information Technology Implementation Stage.

Figure 8-3 depicts the vector forces influencing the initial policy (IP) iteration of the Clinton Administration's Information Technology policy, circa 1993-1994. By 1993, the phenomenal growth in the use of the Internet by the United States Government, industry, and the private sector created a Problem Vector of increasing magnitude, challenging the Clinton Information Technology policy to produce an infrastructure to keep pace with demand.

For the Language Cognitive Vector, the explosive growth in Internet use by both public and private sectors, coupled with the rapid ascension of e-Commerce into the mainstream national economy, had the effect of exposing and acculturating much of the society to the specialized vernacular and lexicon of Information Technology.

Within the Process Vector, the new Administration worked to propose, lobby for, and then develop the requisite technical programs and investments necessary to promote its Information Technology policy. Congress established its Information Technology futures "mapping" through enactment of Public Law 102-194, the High-Performance Computing Act of 1991, which led to the establishment of the High-Performance Computing and Communications (HPCC) Program. Though Congress could be expected to debate the merits of the Clinton Administration's Information Technology proposals, clearly working within the constructs of the HPCC Program facilitated a "win-win" for a Democratic Administration and a Republican Congress, a fact lost on neither side of the political continuum.

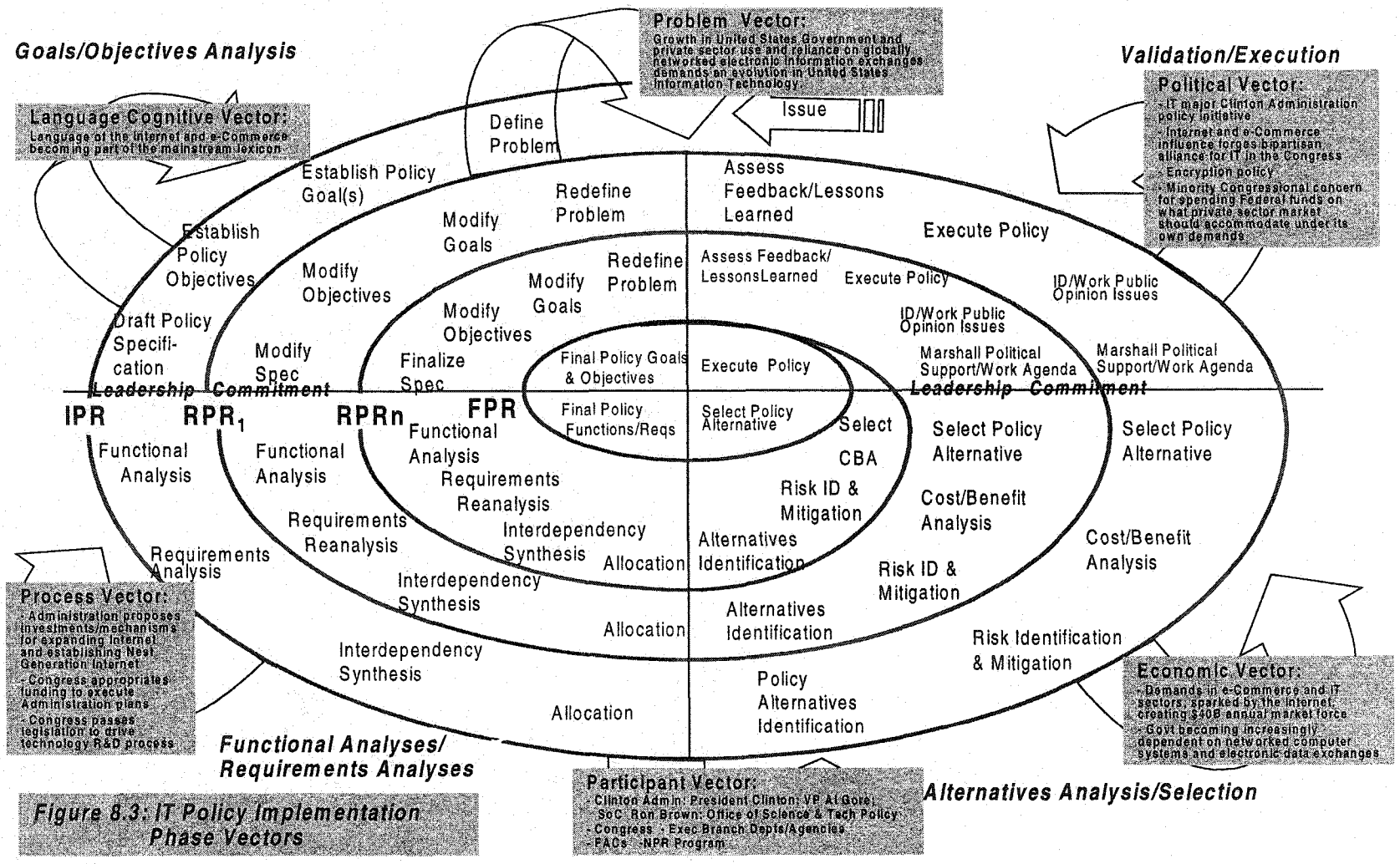


Figure 8.3: IT Policy Implementation Phase Vectors

The Participant Vector during this phase of Information Technology policy evolution was made much more complex, due to the high-level positions held by its hands-on participants. Keeping true to campaign promises to create a "high-tech Administration," both President Clinton and Vice President Gore were active participants in the shaping of Information Technology policy. President Clinton's first two acts in the area of Information Technology policy were appointing Dr. John H. Gibbons as Director of the Office of Science and Technology Policy (OSTP), then directing him in May 1993 to establish the Information Infrastructure Task Force (IITF). It was President Clinton who personally selected Secretary of Commerce Ronald H. Brown to chair the IITF, establishing a high-visibility spokesman for the Administration's Information Technology policy and its Next Generation Internet initiatives. And as Senator Gore (D-TN), it had been the Vice President's stewardship of S. 272, which led to the enactment of Public Law 102-194, the High-Performance Computing Act of 1991 and the establishment of the High-Performance Computing and Communications (HPCC) Program. Fittingly, it was Vice President Albert Gore, Jr. who was chosen to spearhead the Administration's primary Information Technology application initiative, the National Performance Review, also known by its more common name, "Reinventing Government."

The Economic Vector was driven by the explosive growth in both e-Commerce and the commercial Information Technology sectors (i.e., the commercial hardware and software industries) of the economy, each

accounting for some $40 billion in annual trade by 1993. The commercial information infrastructure pressures building were compounded by the exponential growth in demands placed on the electronic information infrastructure by its expanded use in both the public and private sectors.

Within the Political Vector, Information Technology initiatives were firmly entrenched in the Clinton Administration political mainstream. In Congress, the drive toward establishing a national Information Technology policy enjoyed strong, bipartisan support in both Houses of Congress and across both conservative and liberal wings of the two major political parties. Minor dissents were the exception, such as that raised by Representative Dan Burton (R-IL), over the expenditure of public funds to benefit privately owned information infrastructure. However, those concerns were distinctly in the minority.

Information Technology State Analysis--Implementation Phase (IP)

Figure 8-4 depicts the four states of the Clinton Administration Information Technology Implementation Phase PIES spiral during the years 1993-1994. As Figure 8-4 illustrates, the goal established in the early years of the Clinton Administration Information Technology policy was to establish a program to meet an evolving public and private sector information infrastructure need. Using the HPCC Program as a catalyst, the Clinton Administration objectives were to promote the growth of the National information Infrastructure (NII) through sustained, strategic government

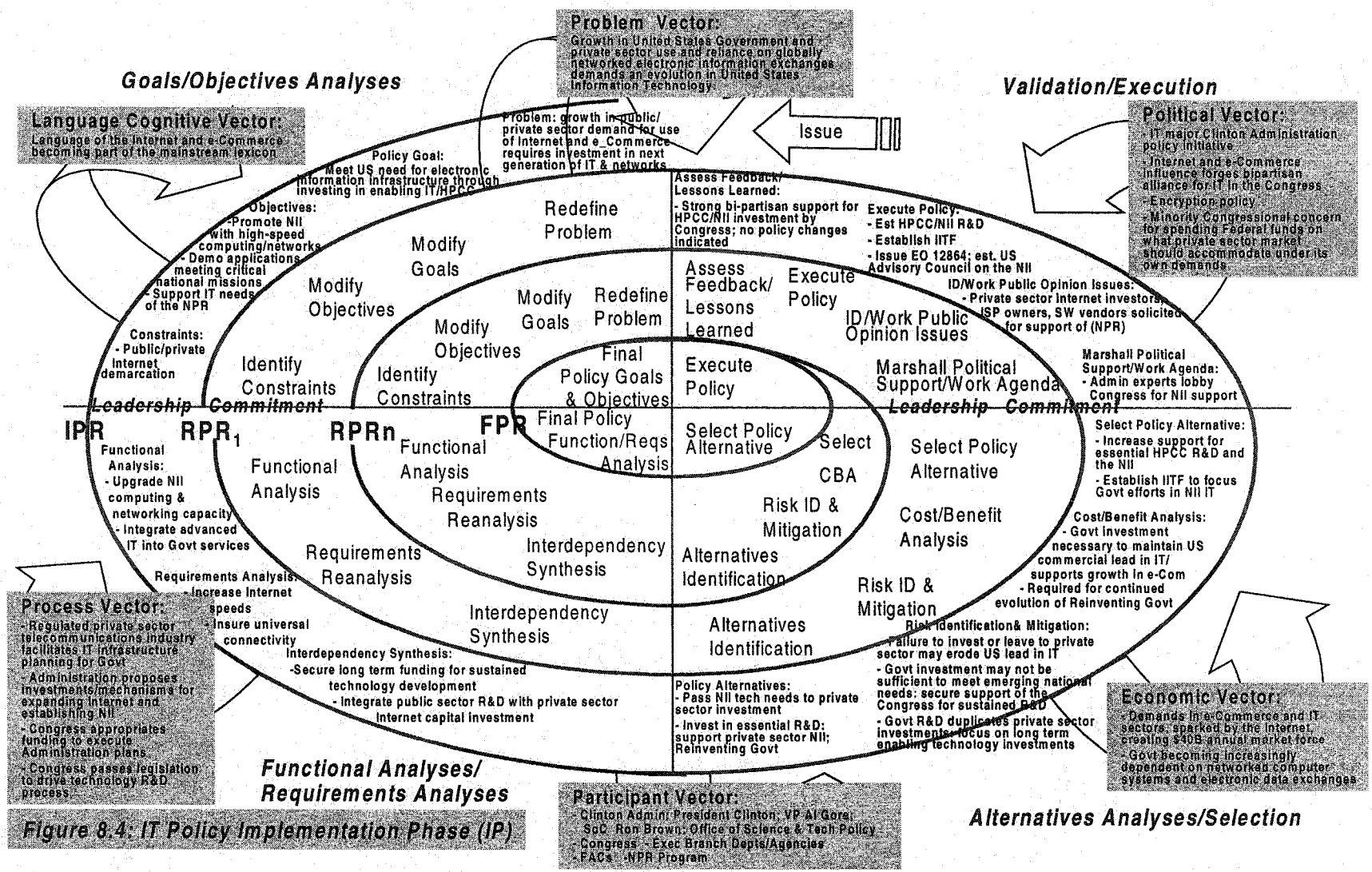


Figure 8.4: IT Policy Implementation Phase (IP)

investment in Information Technology research and development. That investment was focused on first developing, then demonstrating, computer and network applications that could meet strategic national mission needs in a variety of fields, including national security, transportation, health, and the sciences.

Constraining the Clinton Administration Information Technology policy planning was President Clinton's deeply held conviction that the private sector should bear the principal responsibility for building, operating, and maintaining the nation's information infrastructure. This vision dated to the 1991-92 presidential campaign. IITF's manifesto of 15 September 1993 entitled, "National Information Infrastructure: An Agenda for Action," spelled out the Clinton doctrine of private sector ownership and responsibility for developing and operating the NII, with strategic research and development assistance and political leadership coming from the Federal Government:

> While the superhighway is primarily a private sector initiative, all levels of government have significant roles to play in ensuring the effective development and deployment of the Information Superhighway...The Federal Government has a vital role in sustaining a strong research and development base in information technology, through university and corporate programs.[5]

Accordingly, Clinton Administration planning was limited to "national challenges," i.e., only those areas where no single infrastructure provider could be expected to address or invest in a solution to benefit the whole.

Within the Functional Analysis/Requirements Analysis State, the functional needs to be met by the Clinton policy were fundamentally to

employ the vast data management and information dissemination capacities inherent in Information Technologies to streamline government and its service provisions, making government more responsive to the needs of the citizenry. This would be achieved through a process of Reinventing Government, in accord with successes achieved in the commercial sector. This meant a maximum infusion of Information Technology precepts and technology into the government mainstream.

From the requirements perspective, enhancing access to and increasing the bandwidth and throughput capabilities for the National Information Infrastructure (NII) would facilitate this technology infusion. Addressing the requirement of making access to the National Information Infrastructure universal required an extensive amount of planning and coordination, along with a significant allocation of the nation's resources to support the "wiring" of the nation's primary and secondary schools, its universities, research facilities, and government facilities.

Synthesizing these functions and requirements into a physical architecture and executable strategy, the Clinton Administration concluded that these requirements and functions could only be addressed through long-term and sustained program support and a multi-year, renewable, research and development funding commitment on the respective parts of the Administration and the Congress. This could be achieved through the HPCC Program. The second element for meeting the plan needs would be achieved through operationalizing President Clinton's deeply-held conviction of the

strategic partnering imperative between the public and private sectors, with the private sector owner/operators bearing the majority burden of the cost and risk.

As the Alternatives Analysis/Selection State of Figure 8-4 depicts, analyzing the policy alternatives considered during this phase revealed two basic options: Administration commitment to long-term Information Technology research and development in support of a joint pubic-private sector evolution of the NII; or, abandonment of all Federal support in favor of a total reliance on the private sector, trusting in the NII's market-driven development. The Clinton Administration concluded that the national security and economic risks to the United States would be prohibitively problematic, if the nation's Information Technology future was entrusted entirely to the private sector.

Accordingly, the policy the Administration adopted was to increase its support for HPCC research and development and to create a Federal interagency task force to coordinate the implementation of the Administration's vision for the NII. In September 1993, President Clinton announced the formation of an Information Infrastructure Task Force (IITF). The IITF included membership from those Federal agencies and Departments that played key roles in the development of information technologies and policy for the Federal Government.[6]

In the Validation/Execution State, once an information Technology policy alternative consensus was reached, the Clinton Administration

immediately moved to take advantage of the considerable bipartisan support in Congress for Information Technology policy by promoting the evolution of the NII. To that end, Administration experts, working with their Congressional staffer counterparts, worked throughout 1993 to establish mutually acceptable funding allocation targets for expanding the HPCC Program and for establishing a bipartisan approach for securing the essential public-private partnership needed to evolve the NII.

In support of these objectives, President Clinton made two executive decisions. First, on 15 September 1993, President Clinton issued Executive Order 12864, which established a Federal Advisory Council, under the office of the Secretary of Commerce, whose role was to provide President Clinton advice on the development of a national strategy for promoting the National Information Infrastructure (NII). EO 12864 defined the National Information Infrastructure as:

> The integration of hardware, software, and skills that will make it easy and affordable to connect people with each other, with computers, and with a vast array of services and information resources.[7]

Chaired by Secretary of Commerce Ronald Brown, the Council was formed as a vehicle for making policy and implementation recommendations to President Clinton on the appropriate roles of the private and public sectors in developing the National Information Infrastructure. This was in keeping with President Clinton's desire to evolve a public and commercial applications framework necessary, in his mind, for the success of the

envisioned National Information Infrastructure. The Council was asked to address issues of national security, emergency preparedness, system security, and network protection for the NII, while exploring a national strategy for maximizing interconnectivity and interoperability within existing communication networks. Universal access and international connectivity issues were the major considerations of the Council.[8]

On 23 November 1993, President Clinton executed Executive Order 12881, which established the National Science and Technology Council (NSTC). A cabinet-level Council and chaired by the President himself, the NSTC's primary function was coordinating the science and technology policy-making process of the United States Government, consistent with the stated science and technology goals of the Clinton Administration. An important objective of the NSTC was the establishment of clear national goals for Federal science and technology investments, in the area of Information Technology, and to strengthen programs of fundamental research and development.[9]

Information Technology Policy Vectors--Sustainment Phase (SP)

Between November 1993 and October 2000, the Clinton Administration's Information Technology policy evolved from its Implementation Phase into its Sustainment Phase. Although the policy status quo was maintained during this time period, elements of the policy framework continued to change in concert with the

contemporary political and policy environments exerting influences upon it.

The content of the Problem, Language Cognitive, Economic and Political Vectors remained relatively constant between 1993 and 2000, consistent with those vectors identified during the Information Technology Implementation Phase between the years 1992 and 1993. However, the magnitude of the influences exerted by each of these vectors on the evolution of Information Technology policy increased significantly between 1993 and 2000, creating greater influences on the policy model. For these four vectors, explosive growth in United States Government and private sector use and reliance on the nation's electronic information infrastructure, coupled with continued strong support in Congress for investment in High-Performance Computing and Communications (HPCC) and the Next Generation Internet, expanded these vector influences significantly.

In January 1993, at the beginning of the Clinton Administration, no less than one million host computers were linked to the Internet/ World Wide Web.[10] By 1996, commercial companies formed to develop commercial web browser technology and products had helped boost the number of Internet hosts to 12.8 million subscriber systems.[11]

Between 1990 and 1999, the number of United States households owning at least one personal computer rose from 22% to 53%, while the

number of those households with Internet access increased from virtually none to 38%. The total number of global Web sites grew from 313,000 to 56 million. Product sales recorded by United States software vendors rose from $63 billion to $141 billion. This growth underpinned the meteoric rise of an expanding e-Commerce economy, estimated to be valued in excess of $100 billion by 1999.[12]

The Process Vector was impacted significantly by the passage of five Public Laws. First, PL 104-104, the Telecommunications Act of 1996, deregulated the telecommunications industry in the United States. Prior to PL 104-104, the national telecommunications planning had been accomplished by AT&T. Passage of PL 104-104 effectively fragmented that infrastructure planning and control, placing a significant burden on the Federal Government to assume the planning responsibility AT&T had previously assumed. Second, enactment of PL 104-106, The Information Technology Management Reform Act (ITMRA) of 1996, stripped control of Federal Information Technology from the GAO and placed it in the hands of the OMB, significantly modifying Administration processes as a result. Third and fourth, PL 104-13 and PL 105-277, The Paperwork Reduction Acts of 1995 and 1998 respectively, codified many aspects of the Clinton Administration's National Performance Review (NPR), establishing requirements for paperwork elimination and increased electronic interchange by government agencies. Fifth, and finally, the passage of PL 105-305, the Next Generation Internet Act of 1998, amended the High-Performance Computing Act of 1991

by authorizing appropriations for FYs1999 and 2000 for the Next Generation Internet (NGI) program. Enjoying strong bipartisan support in the House and Senate, the bill was signed into law on 29 October 1998.[13]

The Participant Vector also changed dramatically with the passage of Public Laws 104-104 and 104-106. First, prior to the passage of PL 104-104, the Telecommunications Act of 1996, the de-facto planning and provision of "National Telecommunications Services" were provided by AT&T (pre-divestiture) and by the Regional Bell Operating Companies (post-divestiture). Post-divestiture, the United States Government found itself increasingly dependent on private-sector standards bodies to provide representation on Federal advisory committees to affect the continued evolution of the NII. [14]

Second, PL 104-106, the Information Technology Management Reform Act of 1996 (ITMRA), also known as the Clinger-Cohen Act, repealed Section 111 of the Federal Property and Administrative Services Act of 1949 (popularly known as the "Brooks Act"). The ITMRA also amended Section 3506, of the Paperwork Reduction Act (PRA), establishing the position of agency Chief Information Officer within each Federal agency and Department.[15] This provision of ITMRA established a new statutory direction for the management and acquisition of information technology within the Executive Branch. This provision was intended to establish clear accountability for agency information resources management activities, provide for greater coordination among the agencies' information activities, and to ensure greater visibility of such activities within each agency.[16] Under

the ITMRA, the agency CIO was charged with facilitating the development, implementation, and maintenance of a sound and integrated information technology architecture for the host agency and promoting the effective design and operation of all major information resources management processes.[17]

Congress also enacted the Clinger-Cohen Act, in direct repudiation of the lengthy history of failed Information Technology projects managed by the General Services Administration (GSA). As a result of this series of technical failures and costly overruns, Congress used the ITMRA to strip control of Federal information processing systems from GSA, and placed it instead in the hands of OMB and the newly anointed agency CIOs, which made both instant players in NII strategic planning.[18]

Information Technology State Analysis--Sustainment Phase (SP)

Figure 8-5 maps the Information Technology policy's fifth lifecycle phase, the Sustainment Phase, into the PIES framework. Figure 8-5 also captures the influences of evolving vectors on the Information Assurance PIES model, as the Information Technology policy transitioned from its Implementation Phase to its Sustainment Phase. Finally, Figure 8-5 also maps into the Sustainment Phase changes manifested in all four states of the Information Technology Sustainment Phase PIES spiral during the years 1995-2000.

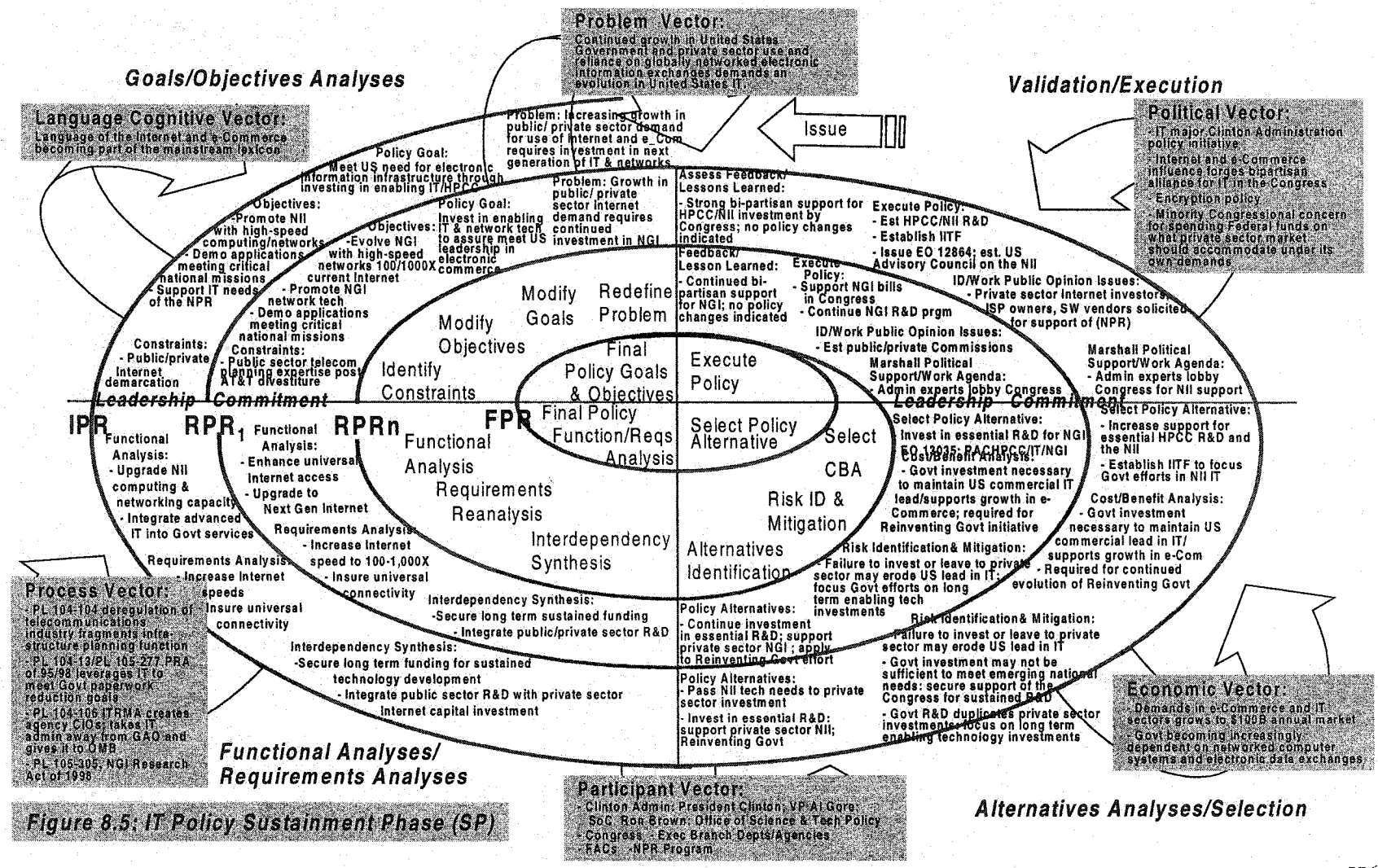


Figure 8.5; IT Policy Sustainment Phase (SP)

Reflected within the Goals/Objectives Analyses State of the Information Technology Sustainment Phase spiral is the high degree of IT policy stabilization enjoyed from the end of 1993 through 2000. This stabilization afforded the Clinton Administration the luxury of a frozen baseline, which allowed a sustained policy focus on maintenance of the continued growth of the Information Technology R&D activity of the Federal Government, through the long-standing HPCC Program. The policy objectives crystallized further with the advent of the Next Generation Internet (NGI) initiative, through which President Clinton identified three, near-term Information Technology goals. The first goal was to interconnect universities and national laboratories with high-speed networks 100-1,000 times faster than the then current Internet. The second goal was to promote experimentation with the next generation of networking technologies. And the third goal was to demonstrate new applications to meet "important national goals and missions."[19]

To fund this initiative, the Clinton Administration added $100 million annually to the Federal R&D budget, beginning with the 1998 fiscal year. While keeping with its policy that the "information superhighway" should be built, owned, and operated by the private sector, the Clinton Administration again reinforced the necessity of Federal R&D underwriting basic research initiatives, which would otherwise be cost-prohibitive for any single, private-sector company to address alone.

Within the Functional Analyses/Requirements Analyses State, a continued focus on support to the HPCC program was enhanced by emerging Process Vector influences resulting from PL 104-104's deregulation of the telecommunications industry and the Congressionally-mandated requirements of the Paperwork Reduction Acts of 1995 and 1998 (PLs 014-13 and 105-277, respectively), the latter of which played directly into President Clinton's National Performance Review tenets.

Additional Process Vector influence was felt as a result of PL 105-305, the NGI Research Act of 1998, which amended the High-Performance Computing Act of 1991, authorized appropriations for FYs1999 and 2000 for the Next Generation Internet program, and established an annual reporting requirement to the Congress by the President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet.[20]

The Clinton Administration focus on sustained investment in the HPCC was driven by a dearth of Information Technology policy alternatives offered during this time period. Both Alternatives Analyses/Selection and Validation/Execution States depict a rock-solid policy status quo, reflecting a mature policy underpinned by a bipartisan political equilibrium, sustained by an expansionist economy, and enjoying a successful track record for meeting programmatic objectives at minimal cost and risk.

From an Information Assurance perspective, the success of the Clinton Administration's Information Technology policy approach provided a solid infrastructure underpinning for the advancement of Information Assurance goals and objectives. The Clinton Administration Information Technology policy support of an expansive growth and technical evolution of the existing Internet into a National Information Infrastructure (NII), created a feedback for sustained United States' contribution to an emerging free-market, unregulated Global Information Infrastructure (GII). Investment in High-Performance Computing and Communications (HPCC) facilitated that feedback, permitting the HPCC metamorphosis into the Next Generation Internet (NGI) program, which itself enjoyed bipartisan Congressional funding support for Administration budgetary requests through the end of 2000.

Finally, it should be noted that the success of the Clinton Administration's Information Technology policy was largely attributable to President Clinton's hands-on direction and personal policy interventions. President Clinton's vision of the respective roles played by the public and private sectors in the technical evolution and capitalization of Information Technology and the Next Generation Internet (NGI) facilitated success of the Clinton Administration's Information Technology policy in affecting a controlling role in the evolution of the Internet, without assuming significant financial risks.

As a result, President Clinton was able to claim legitimate success in meeting his campaign commitment to become the nation's "high-tech

president." By creating an essential Federal momentum through the National Performance Review and investments in the HPCC program, the Clinton Administration met all of the essential political goals of its Information Technology policy. It accomplished this feat by maintaining a controlling interest in the direction of that policy without having to assume the capitalization, operation, or sustainment responsibilities for the nation's critical information infrastructures. These responsibilities were left squarely in the hands of the private sector owners and operators of the nation's telecommunications infrastructure.

FOUNDATIONS OF FEDERAL INFORMATION ASSURANCE POLICY: PIES FEDERAL ENCRYPTION POLICY ANALYSIS

The exponential growth in the use of and dependence on the Internet and the nation's telecommunications networks created a growing vulnerability to the privacy and security of those electronic communications, which placed at risk commercial, financial, governmental, defense, and privacy-related information transmitted across the nation's infrastructure. Conversely, law enforcement and government reliance on these inherent electronic vulnerabilities for real-time intelligence gathering on the current behavior and location of criminals, terrorists, foreign militaries and governments, was a tremendous tactical and strategic advantage for the United States Government.

This explosive growth of the Internet and electronic commerce, coupled with a lightening-fast evolution of advanced programming languages

and tools, was too much of an irresistible force to be contained for long, even for national security purposes. The Information Age demand for new and better products to protect the intellectual property and privacy rights of individual users on the Internet was undeniable. A new approach to the nation's Federal policies on encryption, encryption products, and their exports was needed. This was one of the Information Assurance challenges facing the Clinton Administration as it took office in January 1993.

Encryption Policy Vectors--Implementation Phase (IP)

Figure 8-6 depicts the vector forces influencing the Implementation Phase (IP) of the Federal Encryption policy inherited by the Clinton Administration in 1993. This spiral reflects the initial Clinton post-election policy review, i.e., Revised Policy Review (RPR-1), for the Federal Encryption policy. The Problem Vector depicted represents an emerging influence on Federal Encryption policy by a growing private-sector challenge for strong electronic data protection, pitted against the decades-old policy backdrop of law enforcement and Defense Department dependence on the Federal Government's virtual cryptographic monopoly. The government was prepared to protect its cryptographic advantage at all costs, despite the public's rapidly expanding need for data protection.

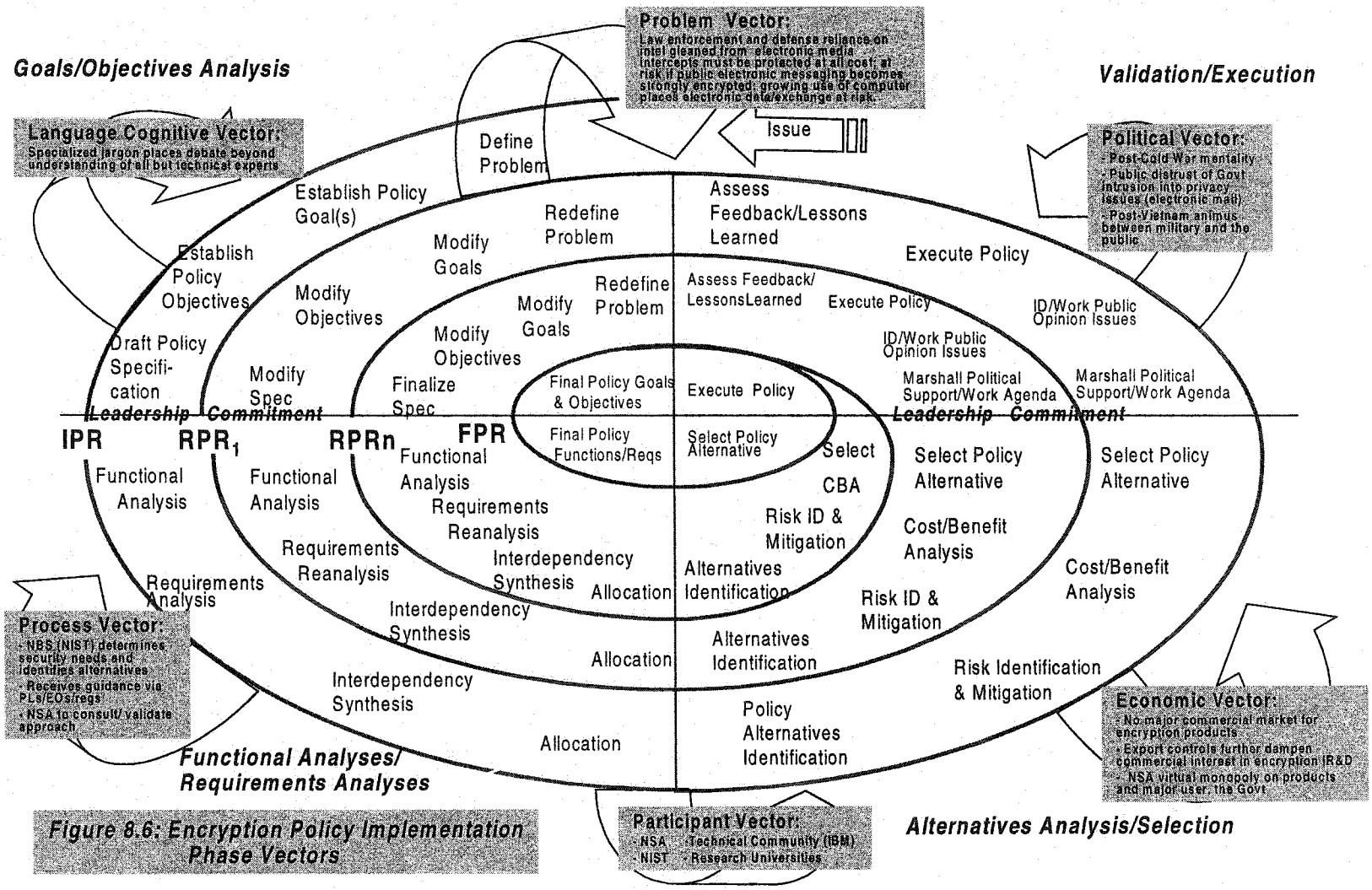


Figure 8.6: Encryption Policy Implementation Phase Vectors

During this phase of Encryption policy development, the Language Vector exerted a minimal influence on the policy evolution. The specialized jargon of computers had not, as yet, become part of the mainstream lexicon. The even more highly specialized mathematical language of encryption algorithms and software made the possibility of any social construction, based upon the language of encryption, a very remote possibility, indeed.

The Process Vector exerted a strong influence on Federal Encryption policy during the Implementation Phase, due to the strong roles and broad responsibilities exercised by the several Federal agencies that exerted process control over Encryption policy. During this cycle of the Encryption policy Implementation Phase, the Office of Management and Budget (OMB) held overall responsibility for computer security policy. The General Services Administration (GSA) was empowered to issue regulations for physical security of computer facilities and to ensure that security hardware and software met certain technological and fiscal specifications.

By far, the National Security Agency (NSA) exerted the strongest influence within this Process Vector. Within the United States Federal Government and particularly within the Department of Defense, NSA bore full responsibility for the security of all classified information, including establishing and maintaining technical standards for secure computer systems. NSA provided expertise to the private sector on data security standards and practices, working in a non-regulatory, advisory role with industry through NSA's National Computer Security Center. NSA's private-

sector role was severely restricted and rigidly controlled by the 1987 Computer Security Act, which limited the agency's role in all but Federal classified computer systems. The Computer Security Act assigned the role of protecting Federal-only computer systems to the Department of Commerce (DOC) and its National Institute of Standards and Technology (NIST).[21]

NIST's Institute of Computer Science and Technology (ICST) was the Federal agency responsible for developing computer security and information processing standards, such as the Federal Data Encryption Standard (DES). Also at the DOC, the National Telecommunications and Information Administration (NTIA) was responsible for analyzing, developing, implementing and applying executive branch policy for all of the telecommunications infrastructure employed within the Federal Government. Under the auspices and policy direction of the Executive Branch and operating within the legal guidelines provided by statutes enacted by the Legislative Branch, these organizations created and executed national computer security and encryption standards and policy for the United States Government.

Within the Participant Vector, several agencies shared responsibility for establishing and implementing computer security controls and standards for the Federal Government. In addition to these government agencies, the Participant Vector also encompassed the nation's research universities and commercial hardware and software vendors involved in computer security product development, such as IBM. Due to the monopolistic practices of NSA

and the restrictive nature of the commercial computer security industry, the vector influences of these commercial vendors was depicted as weak, partially due to the fact that during this cycle of the Implementation Phase, Encryption policy had not, as yet, captured the attention of Congress or the young Clinton Administration.

The Economic Vector reflects the weak influence played by the economy on this spiral of the Implementation Phase, for several reasons. First although the economy had gyrated between periods of stability and instability in the fifteen years leading to the 1993 ascendance of the Clinton Administration, the niche assumed by encryption products in a weak commercial market did not generate much in the way of policy influence. Restrictive Federal encryption product and technology export controls further depressed the commercial market, lessening the vector influence on policy. NSA's virtual monopoly on strong encryption products and technology completed the vector influence dilution.

The Political Vector did exert a slight, but growing, influence on the Encryption policy evolution during this lifecycle phase, driven in large measure by a still significant Cold War mentality and general public support for maintaining tools necessary to ensure the physical security of the United States. This was off-set, to some degree, by residual public distrust of government and the military following the end of the War in Vietnam in 1975, coupled with a growing concern for the preservation of 1st and 4th Amendment rights in the expanding electronic world of the Internet.

Encryption Policy State Analysis--Implementation Phase (IP)

Figure 8-7 depicts the four states of the Federal Encryption policy Implementation Phase PIES spiral during the years immediately preceding the Clinton Administration 1993 transition into office. As Figure 8-7 illustrates, the Goals/Objectives Analyses State reflects that by 1975, the National Security Agency (NSA) and the National Bureau of Standards (NBS) had recognized that the Privacy Act of 1974, and other Federal legislation, along with a growing use of computers and computer networks nationally was creating a demand for data protection and security products that the government or the commercial sector would be compelled to address. The challenge for the Federal Government was to meet a growing public demand for data security, while preserving the government's signal and electronic intelligence access to intercepted electronic messaging--all without violating either legal or Constitutional prohibitions, i.e., 1st and 4th Amendments, or revealing NSA trade or product secrets.

NSA was understandably reluctant to provide any of its products for commercial or even general government use, for fear that its widespread use would complicate the task of real-time decoding of intercepted electronic messages, impacting both law enforcement efforts and national security practices. Also, provision of encryption products to a larger clientele could lead to the compromise of NSA's own, most closely guarded cryptographic methods and tools.[22]

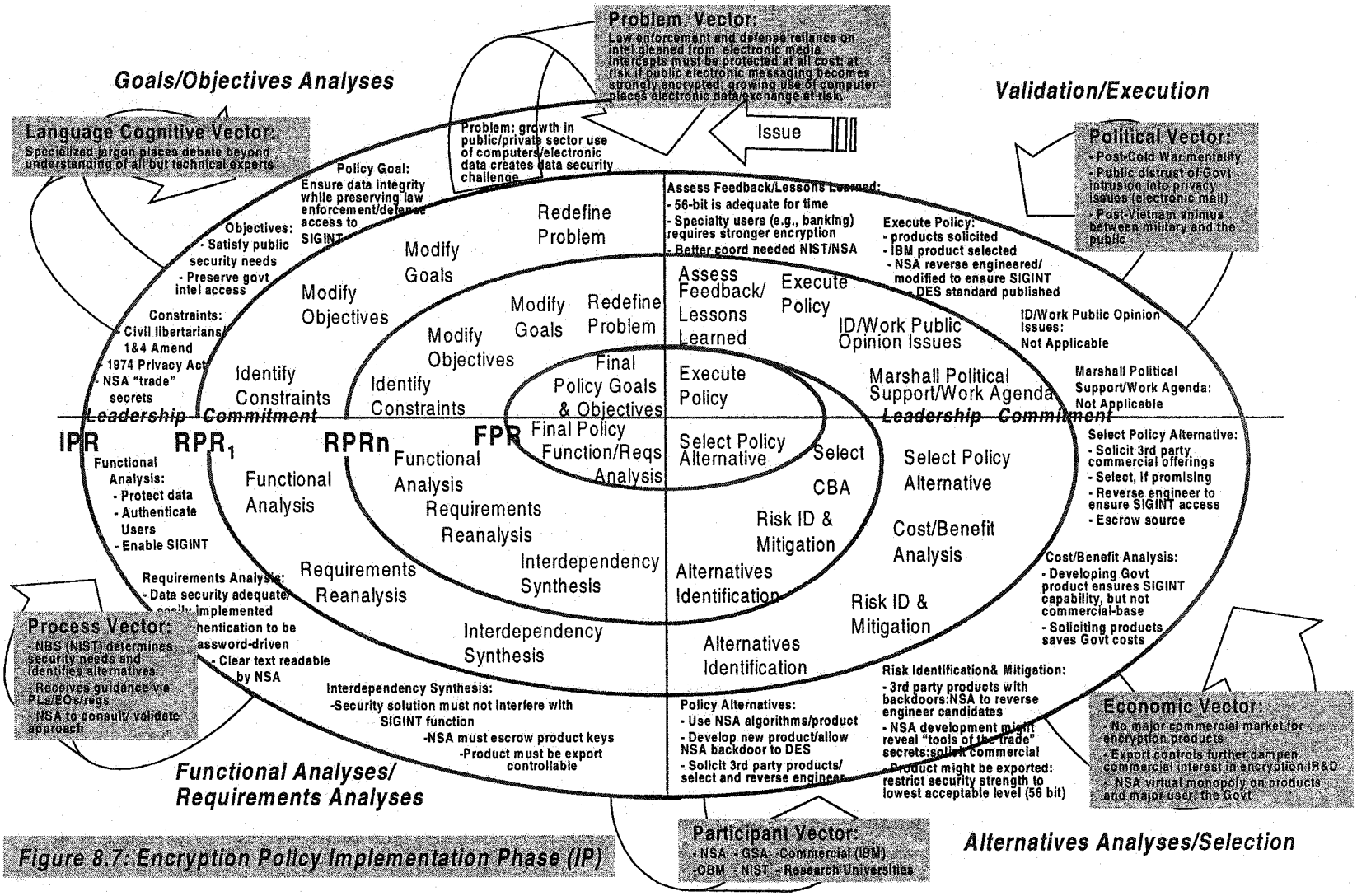


Figure 8.7: Encryption Policy Implementation Phase (IP)

In consideration of these imperatives, the Functional Analyses/ Requirements Analyses State, depicted in Figure 8-7, reflects the dichotomy of functions and requirements the evolving Federal Encryption policy and policy makers faced during this initial cycle of the Implementation Phase. On the one hand, policy pressures from the private sector and from non-Defense, public-sector users, were for robust encryption. The growing pressures to provide commercially available products to meet the data protection needs and the data and user authentication requirements of a rapidly-growing, electronic public, were in direct conflict with longstanding, law enforcement and Defense establishment needs for real-time access to clear text decrypts of intercepted messages. In addition, NSA policy to control, or escrow, all encryption products developed in the United States, coupled to highly-restrictive, export controls on encryption products, created an overwhelming dampening effect from the Process Vector on commercial product development.

The Encryption Policy Implementation Phase Alternatives Analyses/ Selection State, illustrated in Figure 8-7, reflects the three basic Encryption policy alternatives considered by the Federal Government circa 1975. Option One would have NSA use existing or modified NSA encryption algorithms to develop and release computer system and data security products for general use. Option Two required NSA to develop a new class of general use encryption algorithms. For Option Three, NBS would solicit the commercial

software industry for products that NSA would evaluate for use as a new commercial data encryption standard.

Option One carried with it the inherent risk that release of any NSA – based encryption product for general use allowed for the possibility that that product might be reverse engineered, exposing basic NSA cryptographic techniques to scrutiny and copy. Option Two carried with it the same risks as Option One, but would also require NSA to invest scarce R&D funds in the development of a commercial product suitable for general release.

Option Three offered several attractive elements not provided by Options One and Two. First, since NSA would not be releasing one of its own products, no risk was associated with the theft of NSA intellectual encryption property. Option Three required no investment by NSA in product R&D. Finally, Option Three would afford NSA a close look at the best commercially available encryption products industry could offer, allowing NSA to calibrate this commercial state-of-the-art against its own technology.

In recognition of these conflicting concerns, the government opted to openly solicit ideas for a new encryption product with the potential for widespread use. A 128-bit encryption algorithm, developed by a team from IBM and named "Lucifer," was submitted for evaluation to the National Bureau of Standards (NBS--now NIST). NBS forwarded "Lucifer" to NSA for evaluation and possible certification as a commercial data encryption standard.[23] NBS and NSA were suitably impressed with the capabilities of Lucifer that on 23 November 1977, it became the basis for an encryption

system that became the United States Data Encryption Standard, or DES (USDoC 1977).[24]

For the purposes of the Validation/Execution Phase of this spiral of the Encryption policy Implementation Phase, 56-bit key DES was a significant leap forward in useable data security technology. In the greater world of encryption and information assurance, DES was a relatively weak algorithm when compared to other products. A poor "country cousin" to the much more sophisticated NSA cryptography of the day, by 1978, NSA had developed 1,024-bit cryptographic algorithms and had approved at least one of them for use in commercial banking.

Encryption Policy Vectors--Implementation Phase: Revised Policy Review (IP:RPR-1)

Between January 1993 and December 1994, commercial pressures continued to mount for adequate data protection tools based upon encryption technologies. These pressures are reflected in the changing Problem Vector influences depicted in Figure 8-8 as reflective of the second cycle of the Encryption Policy Implementation Phase (IP-RP1). The longstanding imperative associated with law enforcement and Defense reliance on signals intelligence (SIGINT) began to be seriously challenged by a growing influence exerted on the Problem Vector through commercial need for encryption-based Information Assurance. However, by this time, restrictive Federal encryption export laws had so depressed the United States commercial software industry's encryption capabilities that many vendors

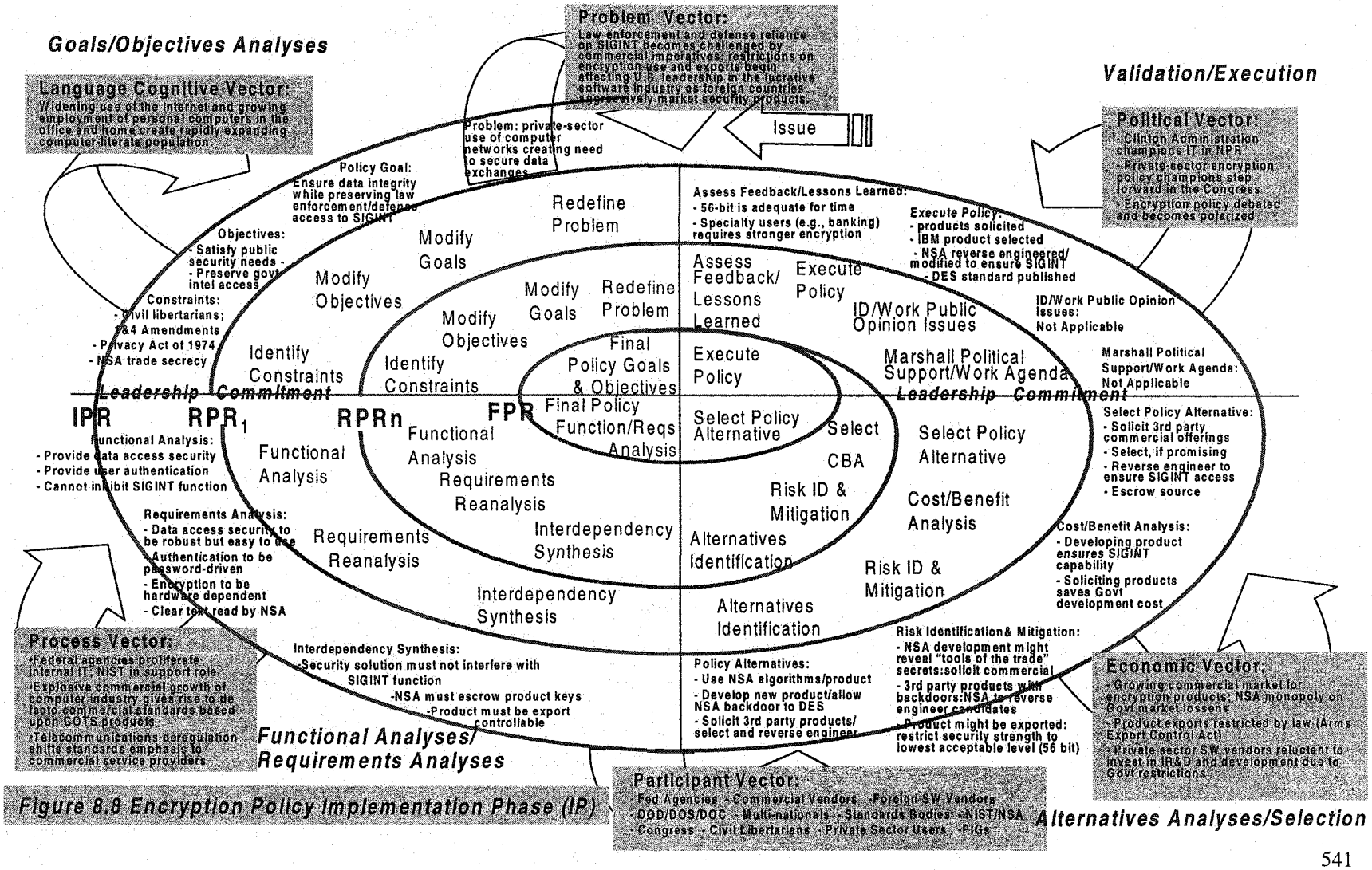


Figure 8.8 Encryption Policy Implementation Phase (IP)

refused to invest in products or product development, since the fruits of those investments could not be marketed overseas. As a result, "industrial strength" encryption could only be acquired through the importation of foreign products.

The influence of the Language Cognitive Vector had increased significantly by this lifecycle phase, primarily as a result of a widening use of the Internet among the general United States population and a growing use of personal computers in the home and in the workplace. This expansion in hand-on experience with computers contributed to the rapid growth of a computer-literate population, versed in the specialized vernacular of computer system.

The influence of the Process Vector remained significant and even increased by virtue of proliferating computer systems and networks across the Federal sector. Explosive growth in computer use and e-Commerce in the commercial sector spawned a comprehensive set of commercial standards, including those for encryption. These commercial standards became adopted by the Federal sector, as well. By the early 1990s, this upsurge in the influence of the commercial sector, as evidenced by the proliferation of commercial standards and standards organizations, helped drive a resurgence of the commercial computer and network security industries within the United States. Telecommunications deregulation, as a result of passage of PL 104-104, the Telecommunications Act of 1998, added to this Process Vector influence.

The numbers and influences of players in the Participant Vector continued to grow during this time period. Joining the existing Federal agencies with control of the Federal computer and data protection responsibility were the aforementioned commercial sector standards bodies. Due to the encroachment of foreign vendors in the market during the lingering down-turn in United States' software vendor participation in the encryption market, foreign companies and standards bodies also exerted an influence in this vector. Finally, two new groups began to significantly influence this vector. First, civil libertarians became increasingly engaged in the encryption debate, in support of 1st and 4th Amendment protectionism. Second, Congress, fully engaged in support of the Clinton Administration's High-Performance Computing and Communications (HPCC) program and the Next Generation Internet (NGI), began exploring legislative relief for some of the more onerous restrictions embodied in Clinton Administration encryption export law.

Beginning in March 1994 and continuing through November 2000, no less than seventeen bills, targeted at reforming aspects of Clinton Administration Encryption Export Control policy, were introduced in Congress. Only one, Public Law 103-414, the Communications Assistance for Law Enforcement Act of 1994 became law. This inability on the part of Congress to pass reform legislation to counter the restrictive encryption export policies of the Clinton Administration was attributable to caution on the part of key members of Congress [e.g., Senator John McCain (R-AZ),

Chairman of the Senate Commerce Committee], concerned with the national security risks involved in the lessening of the restrictive encryption export policies. These influential members of the House and Senate effectively served as policy "gate keepers," using their considerable influence to block legislation that appeared to place the national security at risk.

The Economic Vector continued to reflect a dichotomous influence on the policy process, with a growing influence exerted by virtue of the skyrocketing economic clout created by the growth of computing and Internet use in the United States. This was partially offset by the continuation of highly restrictive encryption export control laws and regulations, which had the mulitplicative effect of driving down commercial software industry investment in technology and product development.

Finally, the Political Vector enjoyed a considerable upsurge in influence, due primarily to three factors. First, the championing of Information Technology by the Clinton Administration created a "bow wave" of encryption product development pressure from users operating in both public and private sectors, who demanded data protection and data integrity as conditions for conducting e-Commerce. Second, market-driven, private sector Encryption Export reform champions exerted more influence in Congress. Senators Patrick Leahey (D-VT), Conrad Burns (R-MT), and John McCain (R-AZ), along with Congressmen Robert Goodlatte (R-VA) and James Sensenbrenner (R-WI) were frequent, albeit mostly unsuccessful, sponsors and spokesmen of legislation to reform United States Encryption

Export law. Only one of seventeen Encryption Export reform bills, submitted to either of the Federal legislative bodies, became law during this time period.

Of important note is that these vectors and their influences remained uniformly constant from March 1994 through the end of November 2000, providing a level of stability for the continued evolution of Federal and Clinton Administration Encryption policy.

Encryption Policy State Analysis--Implementation Phase: Revised Policy Review (IP:RPR1)

The Clinton Administration began a major review of its Encryption Export policy beginning on 1 April 1994, when it announced a liberalization of export licensing requirements for computers operating at up to 1,000 million theoretical transactions per second (MTOPS).[25] This was followed on 19 August 1994, with President Clinton's issue of Executive Order 12924, announcing a national state of emergency in response to the failure of the Congress to extend the life of the Export Administration Act of 1979. As part of that declaration, President Clinton invoked the presidential authorities available to him under the International Emergency Economic Powers Act (IEEPA) to continue the functions of EEA under emergency conditions.[26]

EO 12924 conferred upon the Secretary of Commerce a continuance of the export control authority granted by the Export Administration Act. The Executive Order charged the Secretary of Commerce with the responsibility of approving the issuance of all export licenses and for establishing the

requirements, reviews, and approval process for documentation and other forms of information supporting applications for export licenses. The Order would prohibit the export of any goods, technology, or service without appropriate licensing, subject to the Secretary's export jurisdiction and authority. Licensing the export of sensitive technologies, such as computers and encryption products, would only be made in consultation with the Secretaries of State and Defense.[27]

Figure 8-9 depicts the four states of the Federal Encryption policy Implementation Phase PIES spiral between January 1993 and December 1994. This time period witnessed the first revised policy review (RPR-1) of the Clinton Administration Encryption policy. Figure 8-9 illustrates, that the Goals/Objectives Analyses and Functional Analyses/Requirements Analyses States remained unchanged from the policy constructs inherited from the previous Bush Administration (see Figure 8-8). However, the Alternatives Analyses/ Selection State reflected in Figure 8-9, reveal a major policy shift by the Clinton Administration.

To control the public proliferation of encryption software, the Clinton Administration devised a two-step strategy. First, it resorted to a law, the Arms Export Control Act (22 U.S.C. 2571-2794), designed to control the export of arms and munitions. The Clinton Administration declared that all encryption software greater than a certain strength--in this case forty bits--"qualified" as a munition under the Act, and was therefore illegal to export.[28]

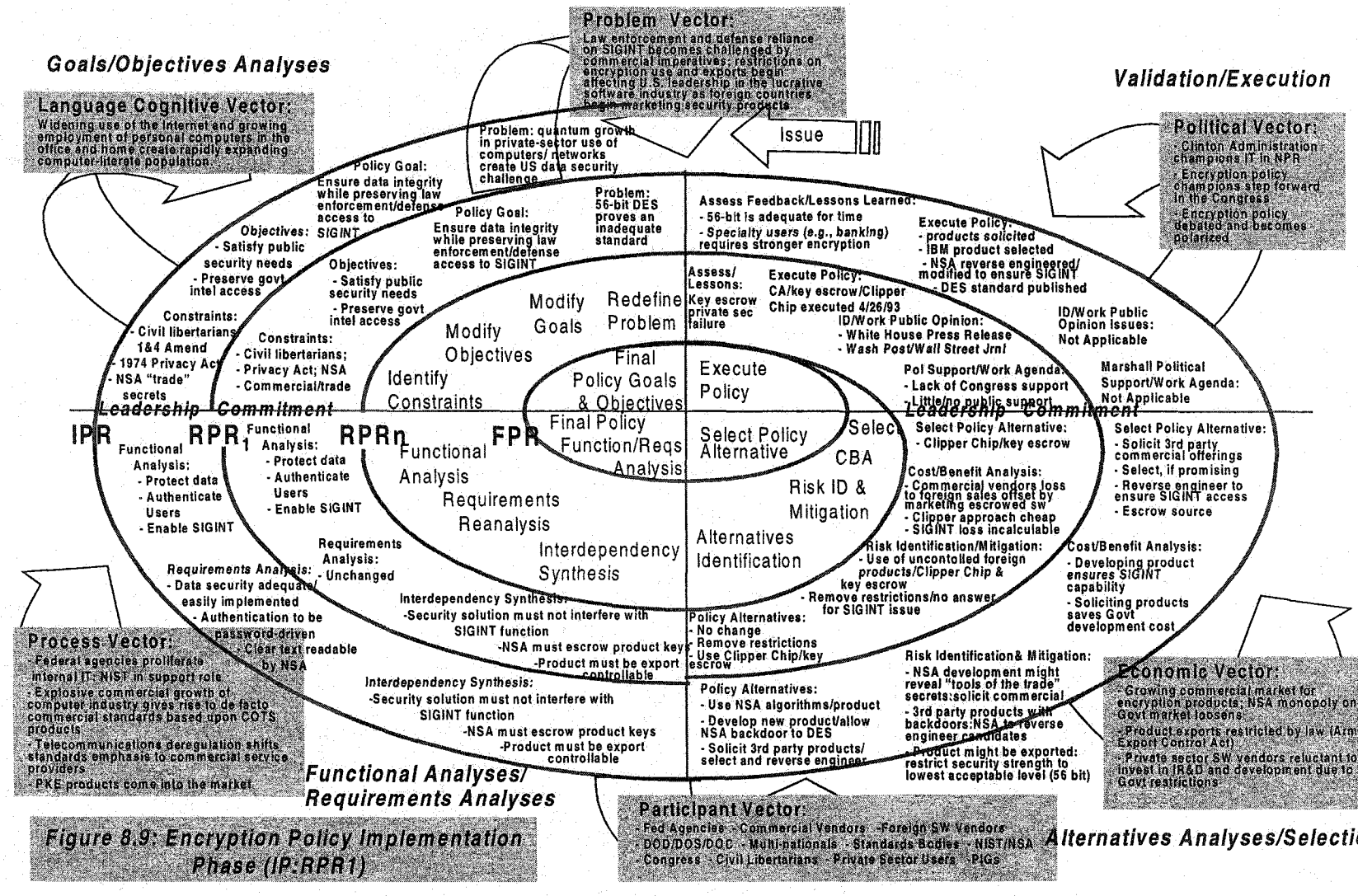


Figure 8.9: Encryption Policy Implementation Phase (IP:RPR1)

The second step of the Clinton Administration's control strategy created a government-sponsored, public-key alternative to the now commercially-based encryption products employing public-key technologies. The first of these key escrow or "spare key" programs was the Clipper Program, which made the term "Clipper" virtually synonymous with key escrow.

As Figure 8-9 depicts, the Validation/Execution State of this spiral of the Clinton Administration Encryption policy involved significant political and public opinion support on the part of the Clinton Administration. This culminated with the Administration's much-heralded public debut of the Clipper Program on 13 April 1993, with multiple press releases from the White House and other government institutions, along with Clinton Administration-orchestrated front-page news releases in the *Washington Post* and *New York Times.*[29]

The centerpiece of the announced policy was the adoption of a new Federal standard for protecting electronic communications. It called for the use of an advanced cryptographic system, one embodying a software "backdoor" that would allow the United States Government, and the government only, to decipher messages encrypted by the new system for law enforcement and national security purposes.

Key recovery, which refers to access to encryption key materials, allows individuals to retain the critical information necessary for a third party to reconstruct a key to the encryption code. Key escrow involves having a

third party, such as the government, hold the cipher key to a deployed encryption product. The ramifications of such a policy are significantly compounded if the keys were held by that third party in perpetuity--thus the vehement objections from 1st and 4th Amendment rights advocates to government-controlled key escrow schemes.

Subsequently adopted by the Clinton Administration over the unanimous opposition from civil libertarians and the computer and telecommunications industries, the Escrowed Encryption Standard (ESS) proved itself a very unpopular standard. As a result, software developed by American commercial companies largely continued to ignore provisions for serious data access protection, making most of the world's commercial-off-the-shelf (COTS) software extremely vulnerable to fairly simple cyberintrusion techniques and tools.[30]

Encryption Policy State Analysis--Implementation Phase: Final Policy Review (IP:FPR)

Figure 8-10 depicts the third of three Implementation Phase spirals of the Clinton Administration's Encryption Policy. This third spiral represents the Final Policy Review phase, the completion of which "promoted" the Clinton Administration's Encryption Policy into its Sustainment Phase. Vectors and both Goals/Objectives Analyses and Functional Analyses/Requirements Analyses States remained stable and unchanged from the previous spiral.

With its lack of success with the Clipper Program, the Clinton Administration began a sustained effort to evolve a new strategy to manage

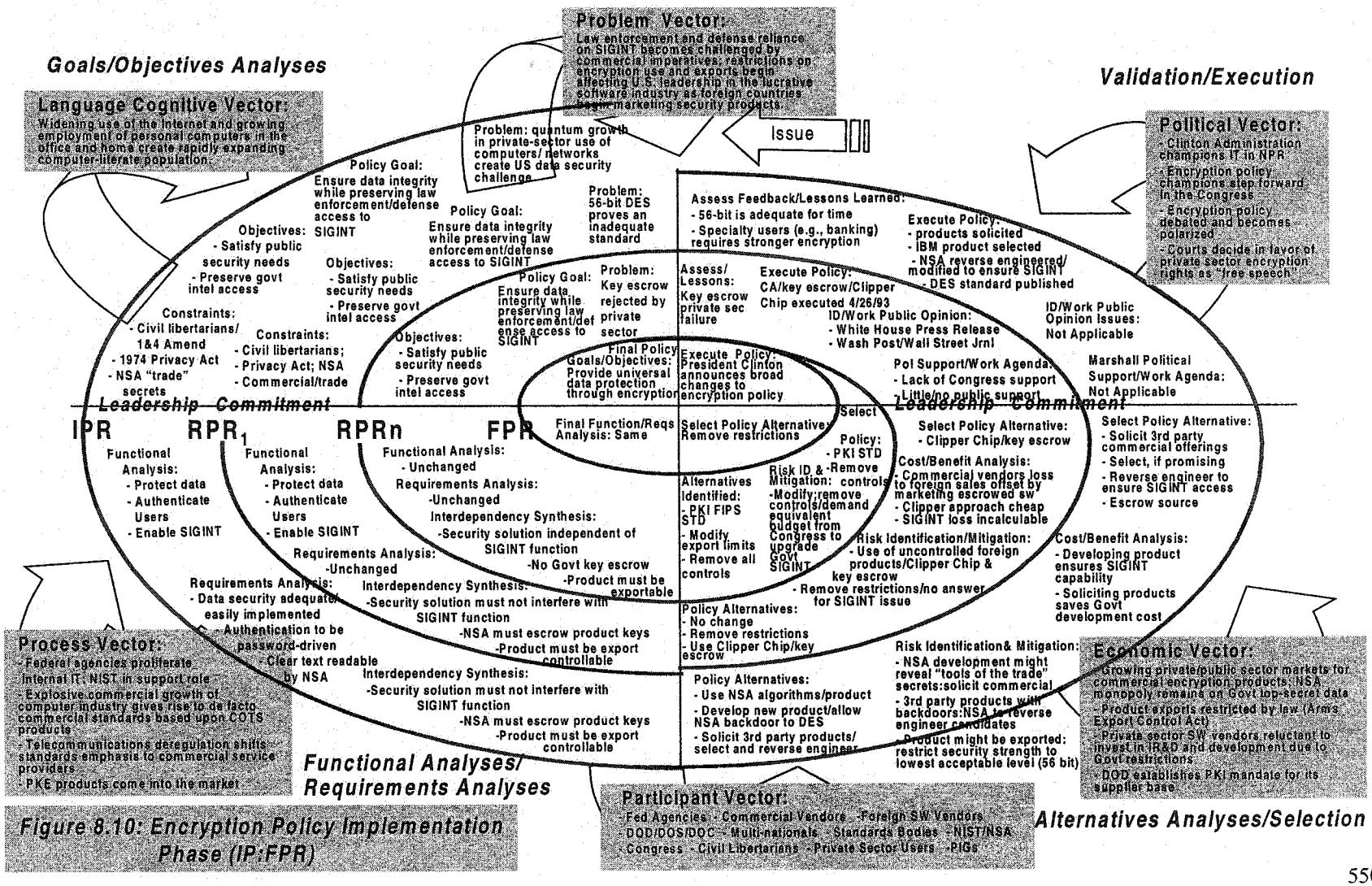


Figure 8.10: Encryption Policy Implementation Phase (IP:FPR)

the development, export, and proliferation of United States encryption products. The Alternative Analyses/Selection State reflects these efforts by the Clinton Administration, beginning on 2 January 1997 with the announcement of plans by the National Institute of Standards and Technology (NIST) to establish a new Federal Advanced Encryption Standard (AES). Based upon a hybrid asymmetric/symmetric algorithm combination, the new Federal standard would be chosen from algorithms and products solicited from the private sector. NIST announced that the new standard would be in place by 1 January 2002.[31]

That announcement was followed on 13 May 1997 by a second announcement from NIST for plans to develop a new Federal Information Processing Standard (FIPS) for public-key based cryptographic key agreements and exchange. The standard would be used in designing and implementing public-key based key agreements and exchange systems operated by Federal Departments and agencies. The notice specifically identified the RSA, Diffie-Hillman, and Elliptic Curve algorithms and encryption techniques as examples of acceptable approaches to address the Federal need, stating that more than one algorithm could be specified in the standard, consistent with sound security practices.[32]

The announcement further stipulated that the new cryptographic standard would support key recovery and key escrow under the current Clinton Administration Encryption policy:

> The Administration policy is that cryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable through an agency or third-party process and that keys used for digital signature (i.e., for integrity and authentication of information) shall not be recoverable. Agencies must be able to ensure that signature keys cannot be used for encryption. Any algorithms proposed for digital signature must be able to be implemented such that they do not support encryption unless keys used for encryption are distinct from those used for signature and are recoverable.[33]

This was followed on 14 May 1998, when the DOD announced its intention of requiring its entire commercial supplier base to adopt a public-key recovery system for all financial transactions with the DOD. Because of its enormous procurement leverage, the DOD placed itself in the position of jump-starting government efforts to build and use strong PKI encryption: "Agencies cannot wait for the government and industry to settle on a national policy," stated Deputy Defense Secretary John Hamre.[34]

On September 14, 1998, the Clinton Administration amended its encryption policy by streamlining the export licensing approval process for computer products employing the 56-bit Data Encryption Standard (DES). The change allowed multinational companies to begin passing relatively secure information across the Internet or via company-internal, private intranets using standards-based, 56-bit algorythms. The policy change also permitted the export of unlimited strength encryption products, such as those based upon 128-bit algorythms.[35]

The seminal Encryption policy change of the Clinton Presidency manifested itself on 16 September 1999 with the Validation/ Execution State

of the Final Policy Review spiral (see Figure 8-10) of the Implementation Stage, the Clinton Administration ' s published "Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace." Co-signed by Secretary of Defense William Cohen, Attorney General Janet Reno, Secretary of Commerce William Daley, and OMB Director Jacob Lew, this document reversed four decades of United States Government encryption policy by removing virtually all prohibitions on the use, sale, or export of encryption products. In explanation, the preamble of the document set the stage in the following manner:

> The Federal Government has sought to maintain a balance between privacy and commercial interest on the one hand and public safety and national security concerns on the other by limiting the export of strong encryption software. Preserving the balance has become increasingly difficult with the clear need for strong encryption for electronic commerce, growing sophistication of foreign encryption products and the proliferation of software vendors, and expanded distribution mechanisms. In the process, all parties have become less satisfied with the inevitable compromises that have had to be struck. United States companies believe their markets are increasingly threatened by foreign manufacturers in a global economy where businesses, consumers, and individuals demand that strong encryption be integrated into computer systems, networks, and applications. National security organizations worry that the uncontrolled export of encryption will result in diversion of powerful tools to end users of concern. Law enforcement organizations see criminals increasingly adopting tools that put them beyond the reach of lawful surveillance.[36]

With this introduction, the national policy paper proposed a "new paradigm" to address the national security and privacy interests of the United States based upon "three pillars--information security and privacy; a new

framework for export controls; and updated tools for law enforcement.[37]

In the areas of data security and information privacy, the new Clinton Administration policy was a radical departure from previous encryption policy positions:

> In updating enduring constitutional values for the computer age, we need to ensure that our citizens' personal data and communications are appropriately protected. Businesses need to privately communicate with their employees and manufacturing partners without risk that their proprietary information will be compromised through unauthorized access. Encryption is one of the necessary tools that can be used in this technological environment to secure information. Therefore, we encourage the use of strong encryption by American citizens and businesses to protect their personal and commercial information from unauthorized and unlawful access.[38]

On the subject of encryption exports, the new policy was again a significant departure from the "absolutes" established previously as policy underpinnings by the Clinton Administration:

> Encryption products and services are needed around the world to provide confidence and security for electronic commerce and business. With the growing demand for security, encryption products are increasingly sold on the commodity market, and encryption features are embedded into everyday operating systems, spreadsheets, word processors, and cell phones. Encryption has become a vital component of the emerging global information infrastructure and digital economy. In this new economy, innovation and imagination are the engines, and it is economic achievement that underpins America's status in the world and provides the foundation for our national security. We recognize that United States information technology companies lead the world in product quality and innovation, and it is an integral part of the Administration's policy of balance to see that they retain their competitive edge in the international marketplace.[39]

Accordingly, the Administration has revised its approach to

> encryption export controls by emphasizing three simple principles that protect important national security interests: a meaningful technical review of encryption products in advance of sale, a streamlined post-export reporting system that provides us an understanding of where encryption is being exported but is aligned with industry's business and distribution models, and a license process that preserves the right of government to review and, if necessary, deny the sale of strong encryption products to foreign government and military organizations and to nations of concern.[40]

Finally, the Clinton Administration looked to the private sector to fulfill the last condition for change to the long-standing encryption policy:

> It is well recognized that industry is designing, deploying, and maintaining the information infrastructure, as well as providing encryption products for general use. Industry has always expressed support, both in word and in action, for law enforcement, and has itself worked hard to ensure the safety of the public. Clearly, industry must continue to do so, and firms must be in a position to share proprietary information with the government without fear of that information's disclosure or that they will be subject to liabilities. Therefore, the law must provide protection for industry and its trade secrets as it works with law enforcement to support public safety and national security. The law must assure that sensitive investigative techniques remain useful in current and future investigations by protecting them from unnecessary disclosure.[41]

FOUNDATIONS OF FEDERAL INFORMATION ASSURANCE POLICY: PIES CRITICAL INFRASTRUCTURE PROTECTION POLICY ANALYSIS

Protecting the nation's critical infrastructure has long been a subject of government concern. Dams, bridges, tunnels, power plants, and other important physical structures have been specially protected over the past 50 years. Protection of the nation's telecommunications infrastructure, however,

has only been of major government concern since October 1962 and the Cuban Missile Crisis.

A growing body evidence suggests that on-going attacks on United States' critical information infrastructures poses a serious and growing, asymmetric threat to the nation's national security. The same Internet connectivities that facilitate the United States' global information interconnectivity are available to potential adversaries. These adversaries employ readily available commercial software and hardware tools, while leveraging United States' dependence on electronic communications, to plan and wage Strategic Information Warfare (SIW). Major disruptions in military operations and military readiness could threaten national security, if SIW attacks were successful in corrupting sensitive information and systems, or if they should deny United States military or civilian decision makers access to vital communications, power, transportation, or other information-based, electronically-networked, critical national infrastructure systems.[42]

The National Security Agency (NSA) has acknowledged that potential adversaries have developed knowledge about United States' critical information systems and effective methods for attacking these systems. These methods, which include the use of sophisticated computer viruses and automated cyber attack and denial of service programs, would permit adversaries to launch virtually untraceable economic and military operations against the United States from anywhere in the world. NSA estimates identify over 120 countries as having, or which are in the process of developing, such

computer attack capabilities.[43] In response, the Clinton Administration constructed the conceptual underpinnings of a national policy for critical infrastructure protection.

Critical Infrastructure Protection Policy Vectors--Conceptual Phase (CP)

Figure 8-11 depicts the initial Conceptualization Stage vectors for the Clinton Administration's Critical Infrastructure Protection policy. The Problem Vector identifies the increasing vulnerabilities manifested within the nation's critical infrastructure systems. Interactions between the government and private sector infrastructure owner/operators are identified as being through commercial standards-setting organizations and through the working of related Presidential Commissions and Committees.

The Participant Vector reflects the set of process owners identified through their functions in the Process Vector. Beside the private sector critical infrastructure owner/operators, NIST, along with the Federal Departments and agencies of the Executive Branch, make up the Participant Vector. Presidential Commissions, such as the President's National Security Telecommunications Advisory Committee (NSTAC), formed in September 1982 by President Ronald Reagan, was created to provide a forum for industry-based analyses and council to the President on a wide range of policy and technical issues associated with national security and emergency preparedness (NS/EP) telecommunications.[44]

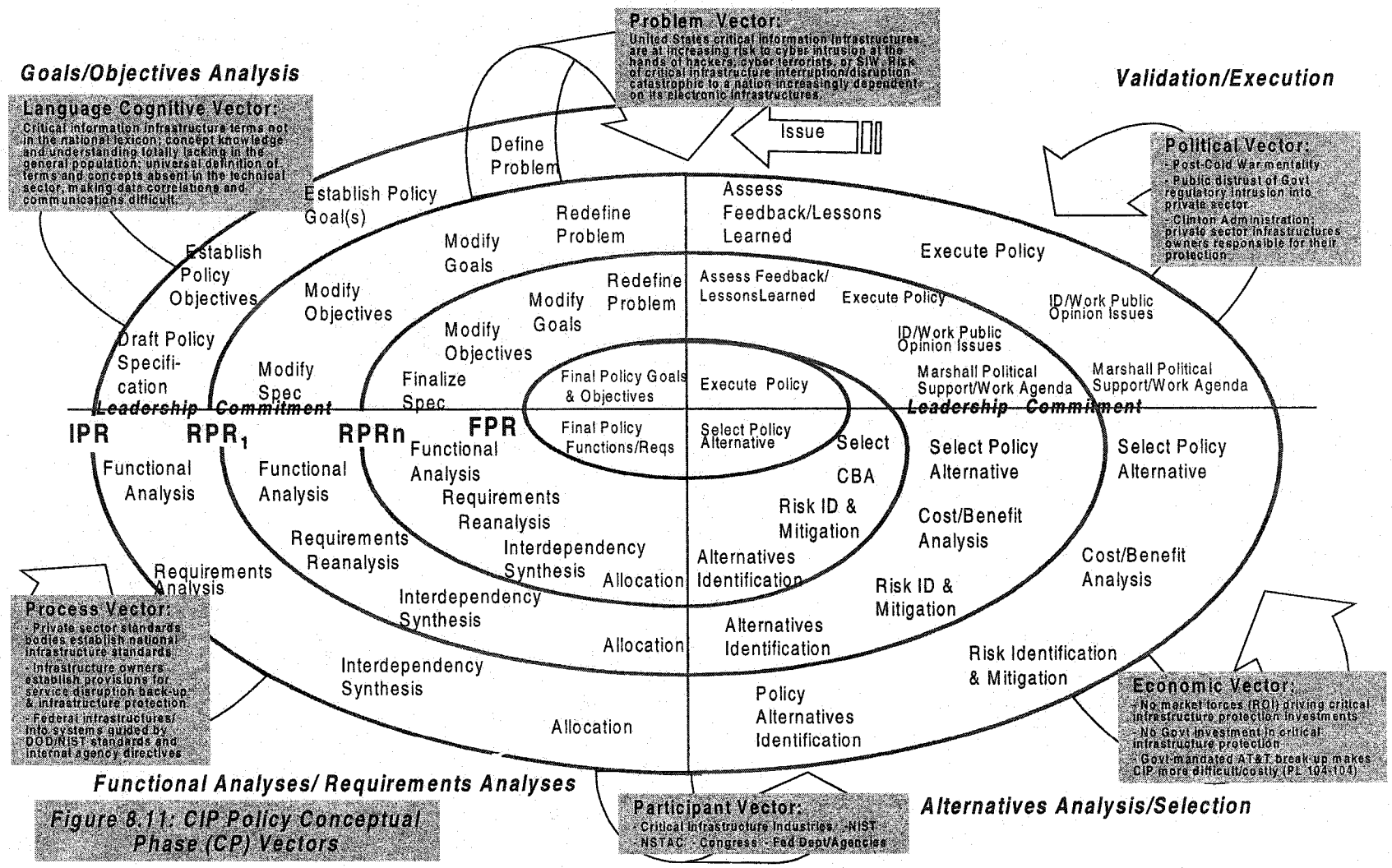


Figure 8.11: CIP Policy Conceptual Phase (CP) Vectors

The Market Vector could not exert much influence on the policy process during this phase of the lifecycle, as industry saw little to no return potential for investment in critical infrastructure protection, particularly in the absence of any defining focusing event. Infrastructures and in particular, the critical information infrastructures, continued to rapidly expand due to market demand, even as the global electronic economy and interconnectivities created vulnerabilities and heightened the risk of critical infrastructure service disruptions through the acts of cyber terrorists, hackers, and nation states beginning to execute various forms of low-level, strategic information warfare (SIW) against the United States.

At this stage in the policy lifecycle, the Language Cognitive Vector exerted very little influence on the policy evolution. This seemed at odds with the massively proliferating National Information Infrastructure (NII) and the computerization of private-sector America. However, the lexicon of critical infrastructure protection is unique. The conceptual knowledge and general understanding of the tenets of critical infrastructure protection were generally lacking within the general population. Even among the subject matter experts, there was no consensus on the exact terms and concepts of the discipline, making data correlations and event communications difficult, at best.

Based upon longstanding Clinton Administration policy requiring the private sector to provide for the defense of the nation's privately owned

critical information infrastructure, it was the voluntary, private-sector standards groups that established the information infrastructure standards, including those for infrastructure defense. Infrastructure owners established provisions for infrastructure service provision and back up in the case of service disruptions or outages. PL 104-104 further eroded the ability of the telecommunications industry to speak and plan with one voice. Government investment in critical infrastructure protection, including its own, was negligible.

Finally, the Political Vector continued to be driven by what is viewed as of a residual of Cold War mentalities and a continued general distrust of government regulatory intrusion into the private sector business. The overriding political consideration of the Clinton Administration's Critical Infrastructure Protection policy remained President Clinton's firm belief that all critical infrastructure protection should be provided by the owner/operators and not by the government.

Critical Infrastructure Protection Policy State Analysis--Conceptual Phase (CP)

Figure 8-12 offers an illustration of the Conceptualization Phase of the Clinton Administration's Critical Infrastructure Protection (CIP) policy. Conceptually, the Goals/Objectives Analyses State of Clinton Administration policy recognized the President's often-stated tenet that critical infrastructure protection is a shared responsibility, requiring an essential partnership. One of the immediate goals of the policy was to affect an educational process for

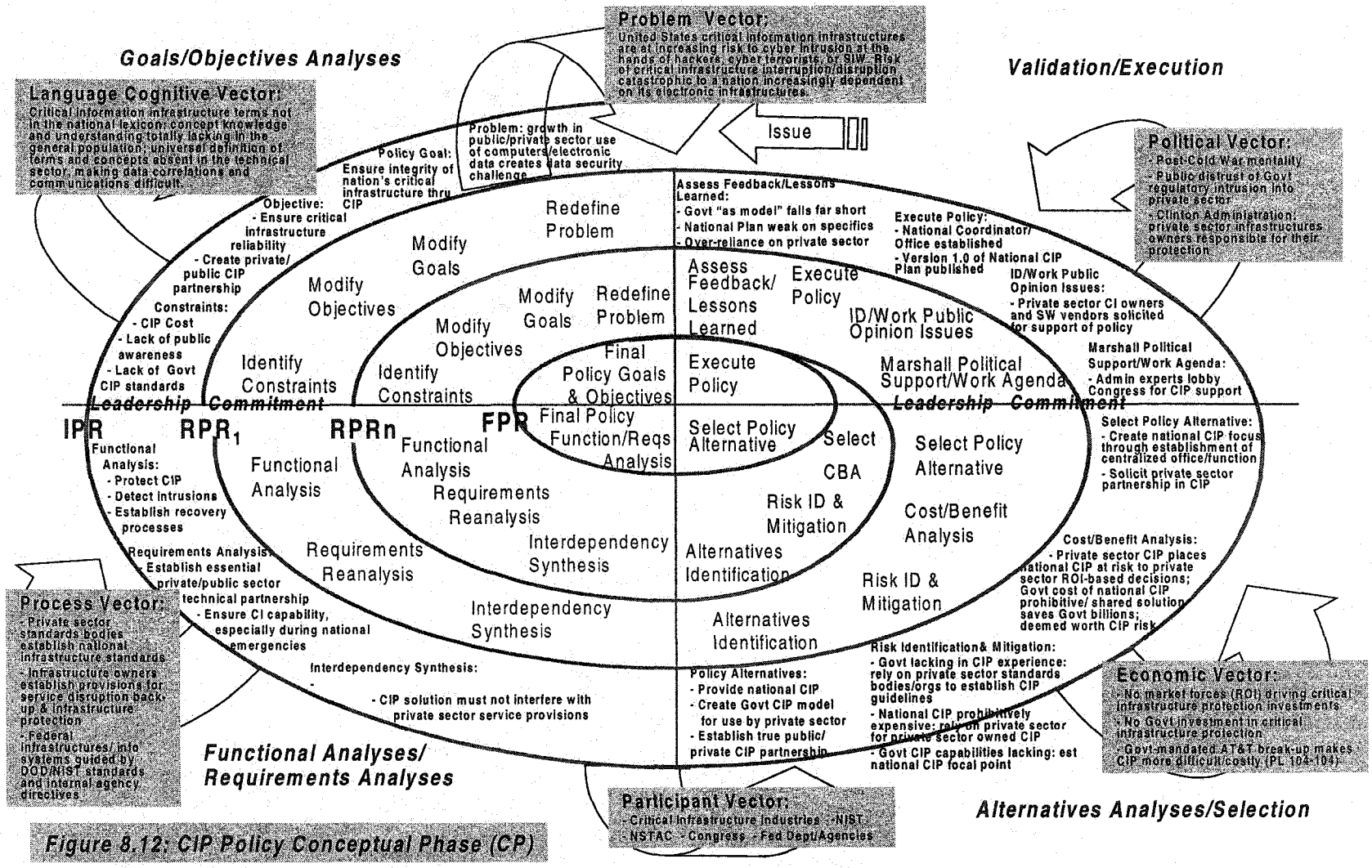


Figure 8.12: CIP Policy Conceptual Phase (CP)

the general public to improve and enhance national awareness of the resident critical infrastructure challenges facing the nation.

Within the Functional Analyses/ Requirements Analyses State, the set of functions that underpinned policy were threefold: first, the nation's critical infrastructure must be defended; second, physical and cyber intrusions must be detected and reported, through the appropriate chain of command, for resolution; and three, planning for emergency recovery from critical service disruption/ interruption must be accommodated. The Requirements Analysis in support of this Functional Analysis identified a strategic requirement to affect the essential public-private partnering in order that a critical infrastructure back-up capability could be established and made available for general use during times of national disaster.

In the Alternative Analyses/Selection State, the Clinton Administration identified a total of three policy alternatives: first, provide for the national defense and have the Federal Government assume responsibility for Critical Infrastructure Protection (CIP); second, create a government CIP model for use by the private sector infrastructure owner/operators; third, establish a true partnership between the public and private sectors to solve this policy issue.

The first option was quickly dismissed. A government owned and operated CIP bureaucracy would likely prove impossible to operate and prohibitively expensive. The government's lack of CIP expertise effectively eliminated the second option from serious consideration. The selected

option, which became the Clinton Administration's policy, was to affect the public-private partnership.

Finally, the Validation/Execution State of this chosen policy was manifest in two major activities. First, On 15 July 1996 and in anticipation of the findings from the Defense Science Board Task Force on Information Warfare, President Clinton signed Executive Order 13010, Critical Infrastructure Protection, a major policy initiative creating the President's Commission on Critical Infrastructure Protection (PCCIP).

President Clinton's Commission on Critical Infrastructure Protection was the first national effort to address the cyber and network vulnerabilities created by the Information Age. The Commission was chartered to formulate a comprehensive national strategy for protecting the United States' critical national infrastructure from physical and cyber terror threats and to report back to the President with recommendations for addressing those vulnerabilities. The critical infrastructure components were defined as telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Because many of these critical infrastructure components were owned by the private sector, Executive Order 13010 made it clear that the government and the private sector would work together to develop a strategy to protect them and to assure their continued operation.[45]

Second, On 7 January 2000, President Clinton unveiled his long-awaited plan for defending America's cyber space, *Defending America's Cyberspace: National Plan for Information Systems Protection--An Invitation to a Dialogue (Version 1.0).* Jack L. Brooks, GAO's Director of Governmentwide and Defense Information Systems, described this in congressional testimony as the, "first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks."[46] This 159-page report focused largely on initial Federal efforts undertaken to protect the nation's critical, cyber-based infrastructures. Subsequent versions were to address a broader range of concerns, including the specific role industry and state and local governments would play in protecting physical and cyber-based infrastructures from deliberate attack, as well as international aspects of critical infrastructure protection. The end goal of this process was to develop a comprehensive national strategy for infrastructure assurance as envisioned by Presidential Decision Directive (PDD) 63.

Acknowledging that the plan was a first step in a long-term planning and implementation effort, President Clinton, in his introductory letter accompanying its publication, stated:

> The National Plan for Information Systems Protection is the first major element of a more comprehensive effort. The Plan for cyber defense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats. It presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety.

> For this plan to succeed, government and the private sector must work together in a partnership unlike any we have seen before. This effort will only succeed if our Nation as a whole rises to this challenge. Therefore, I have asked the members of my Cabinet to work closely with representatives of the private sector industries and public services that operate our critical infrastructures. We cannot mandate our goals through government regulation. Each sector must decide for itself what practices, procedures, and standards are necessary for it to protect its key systems. As part of this partnership, the Federal Government stands ready to help.[47]

SUMMARY

The results from the case studies summarized in Chapters Five through Seven and analyzed in Chapter Eight indicate that the Clinton Administration struggled with and, for the most part, failed to evolve a comprehensive, national Information Assurance policy for the United States during its eight years in office.

Federal Information Assurance (IA) policy at the end of 2000 was an evolving synthesis of intersecting elements of established United States Federal and Clinton Administration Information Technology, Encryption, and Critical Infrastructure Protection policies. Although the individual components of this Information Assurance policy should have been complimentary, they were not. Not only did they not support each other, they actually conflicted with one another in at least three, specific areas. First, Clinton Administration Information Technology policy was the Federal Government's flagship for investment and growth in electronic commerce, electronic government, and

global networking. Yet, Clinton Administration Encryption and Critical Infrastructure Protection policies did little to promote essential Information Assurance technologies and infrastructure critical to securing the electronic data exchanges on which the United States economy and national security depend.

Second, the national security and law enforcement imperatives for electronic access to virtually all electronic information exchanged were in conflict with the basic 1st and 4th Amendment rights guaranteed by the United States Constitution. This conflict underscored a fundamental disconnect between restrictive elements of Encryption policy and information access elements of Information Technology policy. This fundamental conflict between efforts in support of enhanced national security and law enforcement access to electronic data and the fundamental rights of electronic mail /network users to assured privacy and data integrity must be resolved.

Third, and last, aligning the private and public sectors into an essential partnership to provide the means for the electronic "common defense " of United States critical infrastructures, failed the sanity check when weighed I 2000 against the government's forty-year Encryption policy, which functioned earlier to ensure that even the most basic data encryption and computer system protection technologies remained generally out of the hands of the public.

The Clinton Administration executed a significant number of Executive Orders and Presidential Decision Directives (refer to Appendix C), created many Presidential Commissions and Committees to study these issues, and even created a new and significant government bureaucracy to deal with the problem first-hand. These efforts enjoyed only marginal success in advancing the Clinton Administration's Information Assurance agenda.

Why? Of the policy makers involved in this eight-year process, most exhibited predictable decision-making pathologies in the presence of the technical uncertainty and causal risk associated with Information Assurance policy. These policy makers tended to reinforce the existing policy status quo in the absence of what they considered "constructive alternatives." Alternatives were not viewed as constructive as a result of their locus being outside the parochial bounds of the decision maker's decision space. As a result, these decision makers took on the role of "policy gate keepers;" in effect, preserving the existing policy despite the existence of viable alternatives, through a variety of organizational, procedural, and statutory means.

The analysis suggests that these policy "gate-keepers," both within the Clinton Administration and in Congress, maintained the policy status quo for a variety of reasons: political, patriotic, ideological, technological, and economic. This was the case in the long-running debate over the sale and use of encryption products. Advocates for the use of encryption as an effective mechanism for assuring network data security and privacy

protection were stonewalled by national security and law enforcement advocates' claims that such widespread use of encryption would interfere with their unfettered access to private electronic communications.

Inadvertently, this "policy paralysis" had the unintended consequence of forcing the Chief Executive to turn to alternative means of executing essential fact finding and establishing fundamental alternatives essential to decision making. The main alternative approach utilized by the Clinton Administration was to turn to change agents and subject-matter specialists outside the government bureaucracy, who, operating under the authority of the Federal Advisory Committee Act, executed the policy evolution and implementation tasks traditionally the purview of the professional Federal bureaucracy. The aforementioned "policy paralysis" afforded these change agents the requisite time first to organize and then to study policy-specific factors prior to offering value-based recommendations for substantive policy changes to the Administration's decision-making elite, including the President as the ultimate policy decision maker.

In the area of high-risk, high-technology Information Assurance-based national security policy, policy discovery and recommendations in this time period were made by a select few. Surprisingly, the organic bureaucracy, policy entrepreneurs, and key administrative appointees played very minor roles in this process. Extraordinary reliance was instead placed on the recommendations of a handful of elite subject-matter experts and key industry decision makers.

In the absence of focusing events, technical uncertainty and associated risk, Information Assurance policy often created opportunities for a slew of policy decision deferrals, rationalized as "bad decision" cost avoidances. Information Assurance policy stagnation and paralysis in the Clinton years resulted, although the record indicates that this policy inertia was eventually overcome through the direct intervention of President Clinton.

[1] Governor William Clinton, "The Economy," campaign speech presented to the Wharton School of Business, University of Pennsylvania, Philadelphia, PA. 16 April 1992.

[2] Statement of Dr. John H. Gibbons Director, Office of Science and Technology Policy before the Committee on Science, Space, and Technology U.S. House of Representatives, "Information Infrastructure and H.R.1757, the High-Performance Computing and High Speed Networking Applications Act of 1993, 27 April 1993.

[3] The White House, Office of the Vice-President, *Reengineering Through Information Technology—Part 1*, Executive Summary. Accompanying Report of the National Performance Review, 1 September 1993.

[4] Ibid., Appendix B.

[5] The White House, Information Infrastructure Task Force, "A Nation of Opportunity: Realizing the Promise of the Information Superhighway," Executive Summary, 30 January 1996, 2.

[6] The White House, Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," Section III, 15 September 1993, 5.

[7] Executive Order 12864, Section 2. Functions (a),15 September 1993, 1.

[8] Ibid., Section 2. (b) (1-10).

[9] The White House, Office of the Press Secretary, "Strategic Planning Document--Information and Communications," 15 January 1994, 1.

[10] Grier, 69.

[11] Office, 3.

[12] Robert J. Samuelson, "Puzzles of the 'New Economy'," *Newsweek*, vol. CXXXV, no. 16 (17 April 2000), 48.

[13] Ibid., D1204.

[14] National Security Telecommunications Advisory Committee (NSTAC), *Legislative and Regulatory Group Report*, December 1997, Annex C, 1.

[15] PL 104-106, 10 February 1996.

[16] Ibid., Section 5125(a).

[17] Ibid., Section S 125(c).

[18] Capen, 75.

[19] The White House, Office of the Press Secretary, "Internet Initiative Press Release," 10 October 1996, 1.

[20] Congress, House, Representative F. James Sensenbrenner, Jr. of Wisconsin. Next Generation Internet Research Act of 1998. H.R. 3332. 105th Congress, 2d sess. *Congressional Record* (12 November 1998): D1203-1204.

[21] Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington, D.C.: Department of Defense, Office of the Undersecretary of Defense for Acquisition Technology, October 1994), 36.

[22] Whitfield Diffie and Susan Landau, *Privacy on the Line* (Cambridge, MA: The MIT Press, 1998), 59.

[23] James Adams, *The Next World War* (New York, NY: Simon and Schuster, 1998), 215-216.

[24] Ibid., 215.

[25] The White House, Office of the Press Secretary, "Statement by the Press Secretary on Export Control Reform, 30 March 1994, 1.

[26] Executive Order 12924, 1.

[27] Ibid., 2.

[28] Diffie, 106 and Adams, 217.

[29] Office of the Press Secretary, The White House, "Statement by the Press Secretary," 16 April 1993, 1-2.

[30] Diffie, 7-12.

[31] Frank Tiboni, "In Turnabout, McCain Sponsors Bill to Ease Crypto Export Limits," *Government Computer News*, Vol. 18, No. 11 (26 April 1999): 6.

[32] Department of Commerce, National Institute of Standards and Technology, " Announcing Plans to Develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange," *Federal Register,* Vol. 62, No. 92 (13 May 1997), 26294.

[33] Ibid., 26294.

[34] Christopher J. Dorobek, "Defense Wants PKI Now," Government Computer News, vol. 17, no. 12 (4 May 1998), 1.

[35] Sharon Gaudin, "Feds Allow 56-bit Encryption," *Computerworld*, Vol. 32, No. 38 (21 September 1998): 6.

[36] William Cohen, Janet Reno, William Daley, and Jacob Lew, *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace,* 16 September 1999, 5.

[37] Ibid., 5.

[38] Ibid., 5.

[39] Ibid., 7.

[40] Ibid., 8.

[41] Ibid., 9.

[42] Ibid., 4.

[43] Ibid., 4-5.

[44] Ibid., ES-1.

[45] Executive Order 13010, Critical Infrastructure Protection, Section 4, 15 July 1996, 1.

[46] United States General Accounting Office, *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection*, Testimony of Jack L. Brooks, Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, United States Senate (GAO/T-AIMD-00-72), 1 February 2000, 2.

[47] The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0--An Invitation to a Dialogue*, January 2000, iii.

CHAPTER NINE

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS FOR FURTHER STUDY

PURPOSE OF THE CHAPTER AND ITS ORGANIZATION

Using a case study/participant-observer methodology, this dissertation examined the role that Information Technology and Information Assurance policy issues play in evolving the overall national security policy of the United States and, specifically, how that policy evolved during the eight-year Clinton Administration. The case study results from Chapter Five, Federal Information Technology Policy and Legislative Initiatives During the Clinton Administration (1993-2000), Chapter Six, Federal Encryption Policy and Legislative Initiatives During the Clinton Administration (1993-2000), and Chapter Seven, Critical Infrastructure Protection Policy and Legislative Initiatives During the Clinton Administration (1993-2000), served as the foundation for the case study analysis performed in Chapter Eight. In Chapter Eight, the PIES Model, developed for this study, was applied to the case study findings from Chapters Five, Six and Seven, establishing a framework for the systematic analysis of the evolution of Clinton Administration Information Assurance policy between 1993 and 2000. Those research findings are used in this chapter to address the five research questions and 17 propositions posed in Chapter 3 of this study.

Chapter Nine is organized into three sections. The first section, Findings, addresses each of the five research questions and their supporting propositions with results obtained through the case-study analyses in Chapters Five through Seven and the findings from Chapter Eight's PIES case-study modeling. These findings are summarized at the end of this first section.

The second section, Applicability of the Research Tool (PIES Model), provides a summary of the writer's assessment of the efficacy of the PIES model for future research or policy analyses, based upon its applicability for this study. The third section, Conclusions and Suggestions for Further Study, summarizes the conclusions derived from the study results and offers recommendations for future research based upon the open issues suggested by the results of this study.

FINDINGS

Research Question One: How has the Information Revolution affected the framework within which national security policy evolves and is implemented?

The Information Revolution has had a profound effect upon the framework within which United States' national security policy evolves and is implemented. The high value placed by Americans on the lives of their service personnel has led to the development of military strategies and methods that have become progressively less dependent on a quantitative

superiority of armed forces and material and more and more on a qualitative superiority in war-fighting technology, i.e., more advanced equipment, enhanced training, superior doctrine. Information Technology is the latest in a series of technology-based enablers that have reduced United States dependence on human assets in meeting its national security needs.[1]

The United States' quest for qualitative superiority in its military systems, a cornerstone of its strategic military planning, is viewed as a necessary offset to the general quantitative advantages enjoyed by many potential adversaries. It is also necessary to continue to enhance the United States' ability to wage casualty-free warfare, i.e., no American lives lost and minimal loss of military hardware. This ability to minimize casualties, while inflicting the maximum military and infrastructure damage on one's adversaries, is essential for maintaining popular and political support for overseas military interventions. Information superiority has become the cornerstone of that strategy.

The Gulf War and Operation Desert Storm established this new paradigm of warfare, in which human casualties and capital losses for the informationally-inferior protagonist is exponentially greater than those of the informationally-superior one. The new paradigm of high-tech warfare, moreover, requires the United States to be prepared to plan and execute military operations in an entirely unconventional way. Success in this new paradigm of warfare requires the resolution of difficult policy issues today that will determine tomorrow's national security direction.[2]

While the exact technological path to the future structure of Information Technology-based, Strategic Information Warfare may still be in its formative stages, the results of this research clearly point to the fact that electronic operations will be decisive in their own right and the systems incorporating electronic and information technologies will take warfare into an entirely new dimension.[3]

As pervasive as that future technology may become in deciding how future wars may be fought, technology alone is only enabling; it cannot ensure military victory. Military success in the future will require the development of an entirely new set of operational concepts in concert with the integration of new technologies designed to facilitate them.

These operational concepts can only be realized if substantial, organizational transformations occur within the hierarchical military infrastructure of the United States. Public and private organizations move from technical to strategic superiority by achieving the necessary transformations that promote organizational adaptability. Organizational change is THE key element of technological innovation. Its importance as a *multiplier during periods of significant technical innovation* and change cannot be underestimated.

The probability that future adversaries will exploit the tools and technologies of the Information Age to disrupt, destroy, or hold hostage the critical infrastructures of the United States is also fundamentally affecting the framework with which national security policy is developed and implemented.

With the advent of cyber war and cyber terrorism, governments, non-governmental organizations (NGOs), and disaffected individuals can gain an asymmetric political leverage through Information Technology that is unobtainable to them by conventional means, enabling the large-scale or massive disruption of key, strategic infrastructure components, such as electronic banking, electrical power, transportation, and telecommunications. Even on a temporary basis, such disruptions would have a major, debilitative effect on national morale and the nation's collective sense of security.

Proposition 1: The pervasiveness and technical complexities inherent in the dichotomy of Strategic Information Warfare (SIW) and Information Assurance (IA) have fundamentally altered the basic tenets upon which national security policy rests.

The results of this study support the proposition that the pervasiveness and technical complexities inherent in the tools and mechanisms of Strategic Information Warfare and Information Assurance have fundamentally altered the basic underpinnings upon which national security policy rests. A growing body of evidence demonstrates that on-going attacks on critical information infrastructures of the United States pose a more serious and growing threat than assaults on physical infrastructures. The advent of asymmetrical cyber war, in which off-the-shelf computer tools and software can be used to damage or destroy the critical infrastructures that underpin society, has fundamentally changed the rules of warfare.

The Internet linkages that facilitate the United States' global information interconnectivity are the same technologies available to potential adversaries willing to leverage the United States' dependence on electronic communications and the ready availability of commercial software and hardware tools necessary to plan and wage Strategic Information Warfare (SIW). Strategic Information Warfare (SIW) uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. Little in the way of special equipment is required to launch a sophisticated SIW attack on another's computer systems. The basic attack tools--computers, modems, telephones, and software--are essentially those employed by hackers, cyber terrorists, and criminals today. Compared to the often technologically-sophisticated and prohibitively-expensive military forces and weapons that in the past posed a strategic threat to a nation's infrastructures, SIW tools are cheap and readily available sources of strategic military power.[4]

Major disruptions in military operations and military readiness could threaten national security if SIW attacks were successful in corrupting sensitive information and systems, or denied United States military or civilian decision makers access to vital communications, power, transportation, or other information-based, electronically-networked, critical national infrastructure systems.[5]

In discussing the roles that information technology and its infrastructure would have on future conflicts involving the United States, Berkowitz perhaps summed it best when he wrote:

> What stands clear today is that Information Technology has reached critical mass. Information systems are so vital to the military and civilian society that they can be the main targets in war, and they can also serve as the main reasons for conducting offensive operations. In effect, SIW [Strategic Information War] is really the dark side of the Information Age. The vulnerability of the military and society to IW attack is a direct result of the spread of Information Technology. Conversely, SIW's potential as a weapon is a direct result of United States prowess in Information Technology.[6]

The National Security Agency (NSA) has acknowledged that potential adversaries have developed a body of knowledge about United States' critical information systems and effective methods for attacking these systems, identifying over 120 countries developing such computer attack capabilities.[7] These methods, which include the use of sophisticated computer viruses and automated cyber attack and denial of service programs, would permit adversaries to launch virtually untraceable economic and military operations against the United States from anywhere in the world.

Potential regional adversaries and peer competitors at the strategic level are finding Strategic Information Warfare tools and techniques useful in challenging the United States and its global interests. In the near term, weapons having SIW utility may be employed by regional adversaries in asymmetric strategies in lieu of more conventional military and political force, where the United States has a significant advantage.[8] It is against this policy

backdrop that the Clinton Administration began its construction of the conceptual underpinnings for a national policy for critical infrastructure protection.

Proposition 2: Decision-making processes at all levels of national security implementation have been radically impacted by the Information Revolution.

The results of this research support the proposition that the Information Revolution has radically impacted decision-making processes at all levels of the national security policy continuum. The near instantaneous and real-time access to a much wider universe of available information changes the fundamental decision-making focus of individuals and organizations. Deputy Under Secretary of Defense for Policy, Jan M. Lodal, stated:

> Information technology has the potential to revolutionize war. Nearly perfect battle-space awareness, real-time coordination of operations and just-in-time logistics are all made possible by the new information technology, and any one of these would constitute a revolution.[9]

But instantaneous access to and "near perfect awareness" of pertinent information, permitting a fundamental expansion in the depth and breadth of the decision maker's tactical and strategic frames of reference, may come with some significant and adverse side effects. The decision makers' dependence on "perfect" information, enabled by the Information Revolution, may have a debilitating effect on the ability to make timely decisions if

information received is less than "perfect," or if decisions must be made in the absence of complete data, or if access to that information is abruptly severed. In such cases, there is a real risk of creating major systemic and/or individual impedance in decision making as a result of an in-bred, over-dependence on having complete information.

In an opposite scenario, a dependence on electronic means to make better decisions, in the presence of overwhelming amounts of data, may also have the debilitating effect of creating decisional paralysis, due to information overload. Information overload is a phenomenon that occurs when the decision maker has so much data and associated decision points to consider that he or she becomes dysfunctional in attempting to process the decisional information.

In the past, decision making at all levels of national security implementation has relied on, to some degree, the intuitive judgment on the part of the decision maker. Exceptional leaders have this intuitive quality. The Information Revolution may be viewed as the great intuitive equalizer, since it holds the promise of replacing risk taking and intuition with "perfect" situational awareness. A radically different national security infrastructure and a very different style of decision making would certainly result. The specter of what results from the individual's ability to make decisions when the data source for that informationally-dependent, national security apparatus is suddenly severed is at least problematic.

Proposition 3: By virtue of its position in the world and its reliance on Information Technology, the United States is at risk from assault through asymmetric Information Technology means that could seriously impact the execution of foreign policy through the projection of military force.

The research findings support the proposition that the United States is at risk to asymmetric assault on its critical information infrastructures. It is the United States' heavy reliance on Information Technology that makes the nation vulnerable. The Information Technology-intensive infrastructure of the United States creates a singular vulnerability to SIW. That may induce a hostile nation to seek to gain an asymmetric leverage against the United States through an SIW attack on the nation's critical information infrastructure, thus crippling the United States' ability to project its conventional or even nuclear military power.

Critical information infrastructures are the basic foundations of society. As such, their defense is of strategic concern to the preservation of the security and economy of that society. No nation has been as advantaged or has benefited as much from Information Technology and the advent of the Information Age as the United States. Computer-based information infrastructures and networks interconnect every aspect of life in the United States, as in no other country. The unprecedented economic and technological advantages that Information Technology and electronic

commerce have created for the United States, sustains it as the world's only true economic and military superpower. But this pre-eminence comes at a price. Those same infrastructures that underpin and underwrite this society and its economic and military power are also its Achilles heel. Vulnerabilities in the critical national infrastructures, particularly those supporting the computer-based information infrastructures, place the economic and security interests of the United States at risk.

The Information Age phenomenon of computer hacking has spawned an unprecedented Information Age threat in the form of cyber terrorism, elevated to the strategic level through the advent of Strategic Information Warfare (SIW). Employing the same commercially available tools and techniques used to build this vast electronic latticework of interconnected services, individuals, groups, or even nations, using the global reach of the World Wide Web, can disrupt or destroy the vast interconnected network of computer systems that underpin this nation's security, economy, and society.

Research Question Two: How do policy and decision-makers frame or theorize about high-risk, technologically complex issues involving the development of national security policy?

As public policy decisions have become increasingly more dependent upon technology issues and solutions, the question of how government decision makers frame or theorize about these technically complex, national

security policy issues, becomes increasingly important in the analysis and pathology of decision making.

The professional bureaucracy was traditionally looked to as the source of subject-matter expertise and professional guidance in matters of policy development and implementation for the Federal Government. Based upon the results of this study, that may have changed. The study results support Lindblom's and Woodhouse's contention that the professional bureaucracy may be incapable of making rational policy decisions in the Information Age, suggesting that the professional bureaucracy has lost its ability to objectively frame new subject matter, such as that associated with Information Technology, having fallen victim to the defense of what Linblom and Woodhouse termed, "narrowed interests."[10]

Neustadt and May argued that decisions made by organizations reflect organizational "presumptions" based upon the routines and operating modes entrenched in the organizational culture. These "presumptions" make it difficult for organizations to frame or theorize about new or complex technologies and resultant policy paradigms.[11] The research supports this contention.

On example cited in the study involved a General Accounting Office audit of Federal computer security policies and implementations at the 24 largest Federal Departments and agencies. Responding to a request by the Congress to summarize GAO security audit findings, Director Robert F. Dacey, the General Accounting Office Director of Information Security wrote,

in a letter dated 6 September 2000 and appended to a GAO report entitled, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*:

> This report summarizes audit findings for the 24 Federal agencies that were included in a similar review that we reported on in September 1998--agencies that, during fiscal year 1999, accounted for almost 99 percent of Federal outlays. In our 1998 report, we concluded that significant computer security weaknesses had been reported for each of those agencies and that, as a result, critical Federal operations and assets were at risk.[12]
>
> Evaluations of computer security published since July 1999 continue to show Federal computer security is fraught with weaknesses and that, as a result, critical operations and assets continue to be at risk. As in 1998, our current analysis identified significant weaknesses in each of the 24 agencies covered by our review. Since July 1999, the range of weaknesses in individual agencies has broadened, at least in part because the scope of audits being performed is more comprehensive than in prior years. While these audits are providing a more complete picture of the security problems agencies face, they also show that agencies have much work to do to ensure their security programs are complete and effective.[13]

While the GAO report cited a number of factors contributing to weak Federal computer system security, the report identified poor security program management, policy evolution, and poor administration of control techniques as fundamental, underlying causes. While these agencies had taken steps to begin the process of remediating the most glaring of the computer system security deficiencies, the 1999-2000 GAO audit results validated that Federal agencies had not, as yet, incorporated even the most fundamental management practices necessary for ensuring that computer-based controls

and security measures could be successfully implemented. This, the GAO found, was as a result of senior management's inability to frame the requisite policy constructs needed to affect a constructive set of security practices and implementations.[14]

Proposition 4: The emergence of Information Assurance as a major policy issue compels government organizations to become both adaptive and directive in maintaining their power base vis-à-vis the evolving policy environment and their organizational competitors.

Government organizations exist in large part because they have a defined role or purpose that helps bound and justify their organizational existence. That justification is conditional upon an appropriate co-aligning, in both time and space, of such organizationally-intrinsic factors as the value set, the operational structure, the task orientation (i.e., organizational goals and objectives), and the technology core of the organization. As Thompson observed, organizational survival rests on the co-alignment of technology and task environment, within a viable domain, and of organization design and structure appropriate to that domain. When faced with an external environmental change, organizational maintenance, if not survival, is dependent on the organization's ability to adapt or redirect its core to accommodate the changing environment. [15]

The results of this research partially affirm this proposition. The emergence of Information Assurance as a major policy issue does compel at

least some, but not all, government organizations to become both adaptive and directive in maintaining their power base vis-à-vis the evolving policy environment and their organizational competitors. Based upon the research results, two pairs of examples are provided in support of this finding: the first member of each pair affirms this proposition; the second pair illustrating why it should be rejected. The Federal organizational pairs used in this example are the DOD--DISA and GAO--OMB.

In December 1992, the Department of Defense issued two directives, 8000.1 and 3600.1, formally charging the military establishment with the responsibility to, "protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within those systems."[16] In December 1992, and in response to DODDs 8000.1 and 3600.1, DISA created a program to assess the vulnerabilities and exploitable security holes DOD's massive computing infrastructure. In December 2000, some eight years later and despite the explicit mandates of DODD 8000.1 and DODD 3600.1, DISA reported that DOD had not initiated ANY DOD-wide policy requirements for correcting computer system or computer network deficiencies and vulnerabilities identified through the prior DISA security audits.[17]

Proposition 5. Technical complexities such as those associated with the Information Revolution, may exceed the capacity of the permanent

bureaucracy to effectively react to emerging policy needs in a timely manner, giving rise to alternative venues for policy evolution.

The results of this study support the proposition that technical complexities such as those associated with the Information Revolution, may well exceed the capacity of the permanent Federal bureaucracy to effectively react to emerging policy needs in a timely manner. The results of this study also support the proposition that due to this inability to be reactive, alternative venues for policy evolution have emerged.

An excellent example in support of this proposition is found in the Critical Infrastructure Protection case study. DOD's increasing reliance on the Internet global communications backbone has come at the price of increased opportunity for Internet-based cyber intrusions into Defense computer systems and networks. DOD's extensive and growing use of the Internet to exchange unclassified, but sensitive information, places military readiness and operations at risk to cyber-based exploitation of Defense computer security weaknesses.

As described in the previous section, in recognition of significant Defense computer security weaknesses, the Department of Defense issued DoD Directives 8000.1 and 3600.1, directing the uniformed services to protect their information systems by establishing mechanisms and procedures for "preserving the availability, integrity, and confidentiality of the systems and the information contained within those systems."[18]

DISA created the Vulnerability Analysis and Assessment Program (VAAP) specifically to assess vulnerabilities and exploitable security gaps within the Defense computing network. Under this initiative, DISA attempts to penetrate targeted Defense computing systems using widely known and commercially-available techniques. To make such probes even more limiting, DISA personnel were limited to exploiting only known computer system vulnerabilities previously publicized by DISA in their alerts to the military services and Defense agencies. [19]

In December 2000 and despite the explicit mandates of DODD 8000.1 and DODD 3600.1, DISA audits confirmed that DOD had not initiated any DOD-wide policy requirements for correcting identified computer system or computer network deficiencies and vulnerabilities, despite the fact that vulnerabilities and deficiencies that were identified had been immediately broadcast to Defense network administrators, along with suggested fixes.[20]

The second example involves the General Services Administration, the agency of the Federal Government charged with the responsibility of ensuring that all Federal Government infrastructures, including Information Technology infrastructures, are maintained adequately. On 10 February 1996, President Clinton signed into law the Information Technology Management Reform Act of 1996 (ITMRA). The ITMRA established a new statutory mandate for the management and acquisition of Information Technology within the Executive Branch, creating the office of agency CIO as the effective "czar of Information technology" within each agency.[21]

The results of this study also support the second premise of the proposition that due to this inability to be reactive, alternative venues for policy evolution have emerged. During the eight years of the Clinton Administration, President Clinton issued no less than nine Executive Orders (see Appendix C) and established no less than nineteen new Federal offices and/or Federal Advisory Commissions (see Appendix D) to address aspects of Information Technology policy. This was deemed necessary despite the existence of an Executive Branch, having thousands of employees dedicated to similar pursuits.

Proposition 6. Organizational history creates predictable decision-making patterns of behavior that resist change for framing and theorizing about even complex, high risk issues involving national security policy.

Organizations tend to look to their own histories when making decisions about current policy. Decisions tend to be made by organizations with set routines and operating styles that over time have become entrenched as part of the organizational culture. For the decision maker, it is important to understand how an organization thinks and reacts to choice opportunities in advance of that organization being tasked with making and executing a policy related decision.

The technique of placement, or identifying an organization's "institutional proclivities" by drawing inferences from the time line of its

relevant historical experiences, is one method validated by this study as an approach for predicting how organizations will act under conditions of uncertainty.[22]

This study affirmed the proposition that organizational history plays a significant role in the decision maker's ability to frame high-risk, technologically-complex issues involving national security policy.

Research Question Three: What effects do emerging and complex evolutionary shifts in society have on the framework of governance and the administrative institutions associated with it?

Using Information Technology as its lens, this study concluded that emerging and complex evolutionary shifts in society have a profound effect on the framework of governance and the administrative institutions associated with it. Change is as much a constant in political or organizational life as it is in every other facet of existence. When change comes upon an entrenched policy or government bureaucracy, survival depends on the ability of an organization to adapt a successful decision-making strategy for dealing with that change.

The Information Age and Information Technology have profoundly impacted and significantly altered many of the economic and informational foundations that underpin the global society. The Clinton Administration's National Performance Review--Reinventing Government--was predicated on just that sort of change dynamic.

The decision by President Clinton in September 1999 to reverse forty years of highly-restrictive regulatory control on encryption technology was made in recognition that Information Technology had radically changed the environment within which that policy existed, rendering it outdated.

The inability of the General Services Administration to evolve an effective management structure to control the Federal Government's massive computer infrastructure was another example of the impact that Information Technology had on the framework of governance and the administrative institutions associated with it.

When President Clinton signed into law the Information Technology Management Reform Act of 1996 (ITMRA) on 10 February 1996, he was acknowledging that at least part of the existing Federal bureaucracy was incapable of managing the Federal Government's Information Technology resources. The ITMRA established a new statutory direction for the management and acquisition of Information Technology within the Executive Branch. This provision was intended to establish clear accountability for agency information resource management activities, provide for greater coordination among the agencies' information activities, and to ensure greater visibility of such activities within each agency.[23]

The Clinton Administration responded to ITMRA by restructuring its internal Information Technology management policies and processes to align them with the ITMRA mandate, demonstrating a willingness and a resolve to modify Executive Branch organizational and management structures to

accommodate the emerging and complex evolutionary shifts brought about by Information Technology. This ability to adjust was key to the Clinton Administration's ability to evolve an effective framework of governance and the administrative institutions associated with it.

Proposition 7. Government policy often fails to evolve in step with the major societal developments induced by powerful change agents, such as Information Technology, even when the change induced is so pervasive as to reshape society and its core institutions substantially.

The results of this research support the proposition that government policy often fails to evolve in step with major societal evolutions induced by powerful change agents, such as Information Technology, even when the change is so pervasive as to reshape society and its core institutions.

The research validated what Schon described as an organization's attraction to "a stable state," which serves to protect individuals and organizations from the impact that change may have upon the core framework of their institutions and policies. The organization's inherent resistance to change, which manifests itself in active change resistance, is what Schon called "dynamic conservatism."[24]

A prime example of "dynamic conservatism" studied during this research effort was the Federal Government's battle over Encryption policy. Over a nearly eight-year period, the Clinton Administration expended considerable resources and energy in defending an encryption policy that by

all standards was overtaken by events before the Clinton Administration took office. Finally, on 16 September 1996, President Clinton himself reversed years of government stonewalling by directing an end to long-standing government prohibitions on the use, sale, and export of encryption products.

Proposition 8. The complexity and pervasive impact of a significant change agent, such as Information Technology, leads to the adoption of cooperative behavior and strategies between otherwise competing organizations.

Under certain cooperative strategies, the effective achievement of organizational goals is dependent on the exchange of commitments, sharing of power, and the reduction of potential uncertainty for both parties.[25] In such cases, a process of "dynamic adaptation" takes place at the boundary where policy gestation and administration meet. Organizational processes profoundly influence the kinds of policy that can be made, while policy shapes the internal mechanisms of organizations in ways that cannot be accounted for on the premise of organizational efficiency.[26]

Issues of policy are often decided through bargaining among policy makers seeking to achieve balance between personal needs and those of the collective. Individuals and organizations will adopt some form of cooperative strategy in order to reach effective closure on high-risk, technologically-complex Information Technology policy issues.

The results of this study suggest that in the Information Assurance policy arena, little overt cooperation occurred among agencies of the Federal

Government before adoption of ITMRA (PL 104-105) and issuance of Executive Order 13011. ITMRA mandated and EO 13011 forced the creation of a cooperative infrastructure within the Executive Branch to address Information Technology policy/policy implementation issues. Prior to this mandate, little voluntary cooperation was evident among the Departments and agencies of the Federal Government. Section 1 (d) of Executive Order 13011 directed the Executive Departments and agencies to:

> Cooperate in the use of Information Technology to improve the productivity of Federal programs and to promote a coordinated, interoperable, secure, and shared government-wide infrastructure that is provided and supported by a diversity of private sector suppliers and a well-trained corps of Information Technology professionals.[27]

Proposition 9. Policy issues devoid of political capital may elevate to the top of the agenda hierarchy through the advent of a series of catalyzing events.

Problems underlying policy issues often require the intervention of a catalyzing--or, to borrow from Kingdon, focusing--event, defined as a random happening that assumes the role of a powerful symbol associated with that specific issue, and which captures the attention of the general public and government decision makers.[28] These events create "condensation symbols," i.e., representations that evoke strong emotions associated with the event.[29] A catalyzing, or focusing event, is:

> An event that is sudden, relatively rare, can be reasonably defined as harmful or revealing the possibility of potentially greater future harm, inflicts harm or suggests potential harms that are or could be concentrated on a definable geographic

area or community of interest, and that is known to policy makers and the public virtually simultaneously.[30]

The efficacy of the catalyzing, or focusing event concept, and this proposition was probed by attempting to identify causalities between physical cyber-related events and specific Information Assurance policy-related reactions by the government. The results suggest that for Information Assurance, no catalyzing or focusing event of sufficient magnitude has occurred to elicit a specific, policy-related action on the part of the government. The candidate events included the Cuckoo's Egg, SOLAR SUNRISE, MOONLIGHT MAZE, the Melissa virus, and Love Bug virus, all of which are discussed in Chapter 4 of this study.

All of these events had a major financial, operational, legal and security impact on major sectors of the nation's infrastructure. While none of them constitute an "electronic Pearl Harbor," they all were considered very serious events. That these events either failed to qualify as a focusing event, or failed to evoke the level of response associated with a Kingdon or Birkland "focusing event," suggests at least two, possible explanations.

The first explanation is the possibility that none of these catalyzing events caused damage of sufficient magnitude, or adversely affected the general public enough, to gain the requisite notoriety to qualify as a focusing event. This explanation is rejected. Localized focusing events, affecting small numbers of people, have occurred that resulted in major impacts to government policy. The 1967 Ohio River Silver Bridge collapse that led to a

major change in the government's highway safety program is such an example.[31]

The second, more plausible explanation is that these events do not qualify as catalyzing or focusing because, to borrow from Kirlin, no Information Assurance, associated, language-based social constructions have evolved from genre to capture the public's attention. Since people do not share a common cognitive understanding of Information Assurance, they naturally do not share a common vernacular, or language, concerning Information Assurance issues. Since the general public does not share a common experience associated with Information Assurance, no social construction is possible; thus, no recognizable event focuses attention or catalyzes a policy response.

Research Question Four: Within the high-risk, high-technology national security policy arena, who exercises the greatest influence and leverage among policy makers and why?

Within the Information Assurance policy arena and during the eight years of the Clinton Administration, President Clinton and Vice President Albert Gore personally exercised by far the greatest amount of influence and leverage exercised among the policy makers. This leverage was exercised primarily through a Cabinet-level committee established by President Clinton through Executive Order 12881, dated 23 November 1993. This National Science and Technology Council (NSTC), which President Clinton personally

chaired, was the decision-making body that controlled ALL Clinton Administration technology policy and associated Federal investments.

The, "why," answer to this question is straightforward: both men had a strong, personal interest in Information Technology. The Clinton-Gore Team campaigned with Information Technology as a key tenet of its policy portfolio. Vice President Gore led the Administration's National Performance Review/Reinventing Government program, at the heart of which was Information Technology. Both the High-Performance Computing and Communications (HPCC) and the Next Generation Internet (NGI) programs were personally sponsored by and lobbied for by the President and Vice President. That Information Technology was important to both individuals was clearly validated through the level of personal attention and the amount of quality time each was willing to spend personally championing Information Technology issues for the Administration.

Proposition 10. Policy entrepreneurs are most effective in promoting policy or changes to policy within political arenas having a well-defined constituency.

Policy entrepreneurs are usually essential participants in the policy community. Entrepreneurs are often engaged within the policy community due to their unique technical expertise within the policy field, their political acumen and ability to facilitate the brokering of agreements and deals leading to new programs and policies, and due to their connection to a

problem as a representative of a particular constituency. Policy entrepreneurs are particularly important because they lead groups and coalitions that seek to use focusing events for their symbolic potential, thereby advancing issues on the agenda. [32]

Policy entrepreneurs as "people willing to invest their resources in return for future policies they favor."[33] Policy entrepreneurs are viewed in the Public Administration literature as essential to the success of a policy initiative. The ministrations and intervention of a skilled policy entrepreneur considerably enhances a policy issue's prominence on the decision agenda.[34]

Within the context of the Information Assurance policy field, none of the evidence collected supported the proposition that policy entrepreneurs, in the Kingdon or Birkland definitional sense, were key players in the evolution of Information Assurance policy. Industry-wide subject matter experts and retired flag officers of reputational note in the areas associated with Information Assurance, did serve, at the pleasure of President Clinton, on several Federal Advisory Commissions and special study committees. However, they did not serve as a means of advancing a particular agenda in return for securing a policy that they favored, or one that would benefit any particular focus group. Therefore, this proposition is rejected within the context of this study.

Proposition 11. The most influential group in the evolution of policy is not the collective professional bureaucracy, but the visible cluster of elected officials made up of the President, the prominent members of Congress, and senior members of their appointed staffs.

The results of this study strongly support the proposition that the most influential group in the evolution of Information Assurance policy is not the collective professional bureaucracy, but the visible cluster of elected officials made up of the president, the prominent members of Congress, and senior members of their appointed staffs. In fact, in this policy arena, there has been very little visibility on the parts of the professional staffs associated with the evolution of Information Assurance policy.

President Clinton and Vice President Gore both served as personal catalysts for, and engaged in, formulating and executing Information Assurance policy during the eight years of the Clinton Administration. On 23 November 1993, President Clinton issued Executive Order 12881, establishing a Cabinet-level committee, the National Science and Technology Council (NSTC), and for which he personally served as Chair. It was this council which directed all of the Clinton Administration technology policy and investments.

Associated with the NSTC were a handful of senior advisors, who also exerted significant influence on the policy process. They included Kenneth Kennedy and William Joy, Co-Chairs of the President's Information Technology Advisory Council (PITAC), Dr. Neal Lane, Assistant to the

President for Science and Technology, White House Office of Science and Technology Policy (OSTP), Dr. Jacob Lew, Director, OMB, Jamie Gorelick, former Deputy Attorney General, and Jack L. Brock, Jr., Director of the GAO's Governmentwide and Defense Information and Management Division.

Similarly, a small group of prominent legislators, considered by their peers to hold a significant pedigree as Information Assurance policy subject-matter experts, were influential in the Information Assurance policy process. In the Senate, they included: Senators Conrad Burns (R-MT), Fred Thompson (R-TN), William Frist (R-TN), Jon Kyle (R-AZ), John McCain (R-AZ), Orin Hatch (R-UT), and Patrick Leahy (D-VT). In the House of Representatives, they included: Congressmen James Sensenbrenner, Jr. (R-WI), Curt Weldon (R-PA), and Robert Goodlatte (R-VA). Of these legislators, Senator John McCain and Congressman James Sensenbrenner were clearly the most powerful in their respective Houses. Both were considered policy "gate keepers," i.e. they personally reviewed and determined whether a piece of Information Assurance legislation was, in their view, in the best interests of the country, ensuring that legislation would never leave the respective committee each chaired should that not be the case.

Proposition 12. Private sector participants in the evolution of high-risk, high-technology policies influence that policy through participation in organized interest groups, industry associations, and through

government-solicited participation on presidential commissions and committees.

In past Administrations, technical expertise within the Federal Government had been the purview of the professional bureaucracy. As Kingdon noted, the professional bureaucracy has a wealth of experience in administering current government programs, in dealing with the interest groups and the congressional politics surrounding these programs, and in planning possible changes in such programs. A final resource of the professional bureaucrat is their set of relationships and access to elected decision-makers and their key staff.[35]

Despite the credentials of the professional Federal bureaucracy, the Clinton Administration chose to draw upon both formally constituted standing and ad hoc Presidential Commissions or Councils as a key resource in evaluating the issues of importance to the Information Assurance political agenda. Rourke and Schulman postulated that commissions were created because of a President's "dissatisfaction with the way the ordinary executive agencies perform as policy-making institutions."[36] The research results suggest that Clinton Administration behavior in this matter supports Rourke's and Schulman's contention.

In the Clinton Administration and for this Information Technology/ Information Assurance policy issue, the professional Federal bureaucracy had very little influence or interaction with the Administration's decision makers. Instead, President Clinton extensively used the Federal Advisory

Commission Act to create over fifteen advisory Committees and Commissions, whose responsibilities were exclusively to support the evolution of Information Technology/Information Assurance policy (refer to Appendices C and D). This was in keeping with President's Clinton's strongly held belief that the private sector, not the public sector, should be responsible for the financing, evolution, construction, and operation of the National Information Infrastructure (NII). As such, the private sector was given a controlling interest by the Clinton Administration in decisions affecting the evolution of the NII. The FACA provided President Clinton with a mechanism to achieve that end.

Proposition 13. Successful policy gestation requires the strong advocacy of a policy "champion" of sufficient political stature and political leverage to carry the policy agenda through to a successful implementation.

President William Clinton and Vice President Albert Gore, Jr. served as their own Information Assurance "policy champions," personally engaged in formulating and executing Information Assurance policy during the past eight years. They served as the ultimate policy "champions" for Information Technology/Information Assurance policy throughout the Clinton Administration. Given the often-contentious nature of Information Technology/Information Assurance policy issues, it is unclear that this policy would have advanced without the personal attention of the Chief Executives.

An excellent example of this premise is found in Chapter Six. On 16 September 1999, the seminal event of the Clinton Administration's seven-year battle over encryption policy occurred with the publication of, "Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace." Co-signed by Secretary of Defense William Cohen, Attorney General Janet Reno, Secretary of Commerce William Daley, and OMB Director Jacob Lew, this policy document reversed four decades of United States Federal Government's encryption policy by removing virtually all prohibitions on the use, sale, or export of encryption products. In explanation, the preamble of the document set the stage in the following manner:

> The Federal Government has sought to maintain a balance between privacy and commercial interest on the one hand and public safety and national security concerns on the other by limiting the export of strong encryption software. Preserving the balance has become increasingly difficult with the clear need for strong encryption for electronic commerce, growing sophistication of foreign encryption products and the proliferation of software vendors, and expanded distribution mechanisms. In the process, all parties have become less satisfied with the inevitable compromises that have had to be struck. United States companies believe their markets are increasingly threatened by foreign manufacturers in a global economy where businesses, consumers, and individuals demand that strong encryption be integrated into computer systems, networks, and applications. National security organizations worry that the uncontrolled export of encryption will result in diversion of powerful tools to end users of concern. Law enforcement organizations see criminals increasingly adopting tools that put them beyond the reach of lawful surveillance.[37]

With this introduction, the national policy paper proposed a "new paradigm" to address the national security and privacy interests of the United States, based upon "three pillars--information security and privacy; a new framework for export controls; and updated tools for law enforcement."[38] This document, and the policy changes it defined, happened over the objections of each of its four signatories. It happened because President William J. Clinton personally ordered the change over the objections of four of his closest advisors.

Proposition 14. Balkanization of the Federal Information Assurance community results in an ineffective and fragmented policy.

The cohesiveness of relevant communities of policy and technical specialists within a given policy arena vary significantly. Kingdon observed that within some policy areas, the supporting communities of specialists and subject matter experts function through closed, almost fraternalistic interactions, even when individuals within the group represent many different organizations.[39] Conversely, other groups are much more diverse and fragmented.

The degree of fragmentation within such systemic groups is important because, as Kingdon noted, "the first consequence of system fragmentation is policy fragmentation."[40] The Federal Government, with its myriad of overlapping and often conflicted agencies and bureaucratic institutions,

would appear to be likely victims of a process where policy is developed and implemented in a very compartmentalized, organizationally-closed fashion.

In the case of Information Assurance, little or no "balkanization" was detected during this study. Information Assurance policy during the eight years of the Clinton Administration evolved directly from the Chief Executive, President William J. Clinton, retarding or eliminating the opportunity for balkanization to establish itself.

Research Question Five: Are existing decision-making frameworks (Classical Models) successful in determining and then addressing high-risk, technologically-complex questions of national security policy?

This research affirms the usefulness of the Classical Models of decision making in determining and then addressing high-risk, technologically-complex questions of national security. A framework is a useful approach in organizing and then systematically addressing the elements of complex decision making. However, given the complexity of the "system" of national security policy, there is no evidence from this research that would support the contention that Classical Models of decision making do more than loosely frame the decision space. They do not empirically address the complex, often nonlinear interactions among the constituent elements.

National security policy is a complex interaction of many constituent parts. Because of this complexity, it is difficult, perhaps impossible to model

the efficacy of that policy, when one or more of its constituent elements fails or fails to interact as predicted. There are, as yet, no analytical frameworks that can accurately predict the impact of such a change, leaving the policy maker with considerable uncertainty in his or her decision making.

Proposition 15. Rational choice and operations research models are useful in framing and quantitatively comparing alternatives in complex decision environments, offering optimal normative solutions to aid in the policy decision evolution.

This research affirms the usefulness of Rational Choice and Operations Research modeling in framing and quantitatively comparing alternatives in complex decision environments. However, this research cannot affirm that such tools offer "optimal normative solutions" to aid in the decision evolution.

During the course of this research, linear and integer programming and Monte Carlo predictability models were briefly used to experiment with a more analytical approach to address this complex national security issue and to determine whether an analytical component would be useful in this study. The analytical models were employed in an effort to probabilistically determine the chances of successfully executing a hypothetical Information Operation, either from an offensive or a defensive perspective.

Though the results for the offensive operations revealed a much higher probability of success than those for the defensive operations, a follow

up analysis indicated that the result obtained was attributable to randomness, which favors the offensive operation. This line of research was abandoned due to the constraints of the models. The limitations of the analytical tool used was in the mathematical definition of the problem set, which tended toward making the statement of the problem overly constrained, even in a base construct. This resulted in the calculated results having insufficient fidelity to be of use in this study. A brief summary of these efforts may be found in Appendix A of this research.

Proposition 16. A structured, system-engineered approach to problem analysis, decision making, and policy evolution is an effective alternative to political decision-making processes and models when dealing with high-risk, technologically-complex issues involving national security policy.

The research conducted indicates that neither the structured, analytical approach nor the political decision process alone are adequate in making an informed, intelligent decision when confronted by high-risk, technically-complex issues involving national security policy. The term "high-risk, technically complex," is not used here in reference to national security policy simply because it deals with a "system" having a tremendous number of simultaneously interacting elements. If national security policy decision making was merely a matter of sorting through such a maze of complexity, then the results of the research would have supported the proposition that a

structured, system engineering approach is superior to the political process in making national security policy decisions. It did not.

What this research affirmed is that the system of individual elements making up the decision space for high risk, technically complex national security policy cannot be modeled with certainty. That is because the interaction of the elements, these constituent parts and processes that make up policy, interact significantly, and often nonlinearly, with one another, creating outputs that are not empirically predictable in a systematic analysis of the decision space.

Prediction, and therefore decision making, is difficult in this environment, because the elements of choice that shape the future often act in this nonlinear way, rather than in an additive or linear manner. This suggests that even minor interactions in such a complex system can have dramatic impacts on the probabilities of other events happening in predictable ways.

In such cases, there seems to be value in what March, Cohen, and Olsen termed the "organized anarchies" within which the traditional models of decision making operate. These are characterized by the numerous activities competing for the attention of the organization simultaneously. They bound the decision space on a time-dependent basis. Temporal sorting, or time-dependent "binning" of the organizational elements converging on a decision, is a useful construct for comprehending the confusing picture of decision making within such organized anarchy.[41]

A structured, systems engineering approach offers an effective complement to the political process model approach by emphasizing performance-based policy making through the identification of specific policy functions and performance requirements, then defining and selecting from a set of candidate solution alternatives that best satisfy those requirements. And, it does serve as a framework for Kirlin's language-based social construction, contributing to the due process demanded of our democratic institutions.

Proposition 17. The PIES Model offers an effective alternate construct for theorizing about and framing high-risk, technologically-complex national security policy to the "Garbage Can" and "Streams" models.

This research validated the usefulness of the PIES model as a reasonably effective tool for mapping the elements and influences of policy in an integrated construct. The PIES model proved useful for tracing the interdependencies of constituent elements of the three policy components contributing to the evolution of Information Assurance policy. PIES' three dimensional, lifecycle framework suggests that, taken to its ultimate extension, PIES could prove effective in mapping the lifecycle components of a policy into a complex mosaic of incremental and evolutionary policy steps, supporting interdependency traceability throughout the policy lifecycle. This interdependency traceability could prove useful in helping to identify the elements of nonlinear interactions among policy elements. Perhaps the most

useful aspects of the model are its visualization aspects, which afforded this researcher multi-dimensional "lenses" for the study of the Information Assurance policy evolution process.

The application of PIES in this research cannot be used to endorse PIES definitively as being either a more-or-less effective analytical tool than traditional models of decision making. The PIES three-dimensional interdependency constructs do suggest usefulness in a future application, where such constructs can be computerized to greatly expand both the descriptive and interactive constructs and subsequent analyses of the policy elements.

SUMMARY OF THE FINDINGS

The results of this study suggest that Information Assurance policy makers exhibit predictable decision-making pathologies. In the presence of technical uncertainty and causal risk, the behavior of decision makers reinforces the policy status quo through a variety of organizational, procedural, and statutory means. Behavior that maintains the status quo extends all the way down to the operational, or executable, end of the policy continuum. Without the essential "top-down" push for change, those responsible for executing policy have little or no incentive in assuming the role of change agent or risk taker. Advocating for change, even necessary change, from the "bottom up" is often viewed as career-limiting behavior,

particularly in rigidly hierarchical organizations, such as the DOD, where such bottoms-up behavior is frowned upon institutionally.

Decision makers often receive an assist from policy gate keepers, who "buy" essential time for subject-matter specialists to organize and study policy-specific phenomena prior to their offering value-based recommendations to the decision maker. Policy gate keepers come in a variety of roles and identities. The more easily identified are highly respected scientists or engineers serving on Presidential Commissions. They are often highly placed members of a past or serving presidential administration. Or, as in the majority of the cases documented in this research, they are often influential members of Congress. Undeniably, however, the most powerful of the policy gate keepers is the President of the United States.

During the his Administration, President Clinton established the National Science and Technology Council (NSTC) as the conduit through which he personally exercised his gate keeping role over Information Assurance policy. At the same time, a small group of prominent legislators, considered by their peers as resident subject-matter experts in Information Assurance policy, served as policy gate keepers for the Federal Legislature. The results of this research found that high-risk, high technology national security policy discovery and recommendations were made by this select few.

Surprisingly, the organic bureaucracy, policy entrepreneurs, and even most key administrative appointees played minor roles in this process.

Extraordinary reliance was placed instead on the recommendations of elite subject-matter experts and industry executives recruited into Presidential Commissions under the auspices of PL 92-463, the Federal Advisory Committee Act (FACA). As a result, the influence exerted by the professional bureaucracy in evolving Information Assurance policy was negligible.

Over an eight-year period, this paradigm served as a catalyst in prompting the attrition of many senior-level subject matter experts from the ranks of the professional bureaucracy and into retirement or into employment within the private sector. The dismantling of the professional bureaucracy, through the erosion of its senior ranks, may have a significant debilitating effect on the policy-making apparatus of the George W. Bush Administration, early indications of which suggest it may not adopt the same "hands-on" policy making style of President Clinton, a self-described policy "wonk."

In the absence of catalyzing or focusing events, technical uncertainty and risk create opportunities for policy decision deferrals, rationalized as "bad decision" cost avoidances. Policy stagnation and even decision-making paralysis may result. This inertia is often overcome only through the direct and personal intervention of the President of the United States.

Finally, though ample evidence suggests that Information Technology tools and the growing realities of SIW pose a real threat to national security, it is the insider threat, not the threat from without, that continues to be the greatest threat to United States national security. The threat ranges from the

disaffected or disenfranchised insider, with access to sensitive national security information, to failures of the entrenched Federal bureaucracies to adopt and enforce even the most basic of information security techniques and behaviors within their own organizations. Social engineering weaknesses continue to be the best opportunity for successful penetration of the nation's information repositories. Investments in technology cannot overcome either willful or careless acts that expose United States critical information infrastructures to exploitation by those who would do harm to the United States and its national interests.

THEORETICAL PERSPECTIVES ON PUBLIC POLICY DECISION MAKING: POLICY AS AN INCREMENTAL EVOLUTIONARY SPIRAL MODEL

The PIES model offered in this dissertation was proposed as a potentially useful framework for operationalizing the theoretical perspectives of public policy decision making, while systematically addressing the host of organizational decision-making issues that affect the evolution of effective policy. PIES models the elements of policy making as interdependent, incremental decisions evolving through four stages, defined by the model as: Goals/Objectives Analysis; Functional Analyses/ Requirements Analyses; Alternatives Analyses/Selection, and; Validation/ Execution. These four stages represent the decision-making quadrants that exit within each of seven lifecycle policy phases identified in the model as: Conceptualization; Promotion; Initialization; Implementation; Sustainment; Exit/Termination; and

Post Analysis (Lessons Learned). Finally, six, off-setting decisional vectors are defined by the model as process forces that exert dynamic tension on the model's decision cycles. These vectors are defined as the: Problem Vector; Language/Cognitive Vector; Process Vector; the Participant Vector; Economic Vector; and the Political Vector

Each of these vectors was drawn from decision models by Allison (Rational Actor, Organizational Process, and Governmental Politics), March, Cohen, and Olsen (Garbage Can), Kingdon (Streams and Widows), Kirlin (Language-based Social Construction), Keeney and Raiffe (Rational Choice).

Within the context of the PIES mode, this dissertation has examined four intersecting policy vectors within the context of some of the rich legacy of the Organizational, Administrative, Decision-Making, Language-Based Social Construction, and Rational Choice Theory bases, probing for the balance between the qualitative judgments of political choice and the quantitative empiricism of rational choice.

While nothing substitutes for good judgment, the effective exercise of that decision making choice does demand as complete accounting of the facts as possible, at every stage of the decision lifecycle. The introduction of the PIES Model in this dissertation offers a construct for combining the major elements of the political and analytical decision-making processes into a single framework, bridging between the analytical elements of systems engineering and the decision-making judgment of the political purists.

This research partially validated the PIES model as a useful tool for mapping the elements and influences of policy into an integrated construct. The PIES model proved adept in mapping the interdependencies of constituent elements of the three policy components contributing to the evolution of the fourth policy constituent, Information Assurance policy. This interdependency traceability could prove useful in helping to identify the elements of nonlinear interactions among policy elements. The most useful aspects of the PIES construct for this study were its visualization aspects, which added dimensional views to the study of the Information Assurance policy evolution process.

The application of PIES in this research cannot be used to definitively endorse PIES as an effective tool for analyzing policy. Used as a template for a computer program, PIES might find useful employment beyond this study in an automated form. Further research would determine the usefulness of PIES beyond this study.

CONCLUSIONS AND SUGGESTIONS FOR FURTHER RESEARCH

This research was undertaken in recognition that the on-going Information Revolution and a growing dependence on vulnerable elements of the National Information Infrastructure (NII) are profoundly affecting the national security interests of the United States. The pervasive evolution and adoption of information technologies in most aspects of society present an

entirely new type of national vulnerability and policy-making complexity to those charged with "providing for the common defense."

The expansive growth and integration of interoperable computer-controlled information and communications systems form the foundation of the United States' Information Age-based economic vitality and quality of life. This information and communication systems infrastructure, comprised of the Public Telecommunications Network (PTN), the Internet, and millions of interconnected computers in private, commercial, academic, and government service, creates a virtual "electronic backbone," upon which all essential information and control services in the United States depend, i.e., transportation, energy production and storage, water, emergency services, government services, banking and finance, electrical power, and telecommunications. This unique set of interconnected infrastructures creates an entirely new dimension of strategic vulnerability and an Information Age challenge to the national security of the United States. The evolution of an effective Information Assurance policy is wholly dependent on the policy-making process of the United States Federal Government.

The United States' defense establishment and the nation's critical infrastructure are under assault from a series of well-orchestrated and sophisticated, computer-based, cyber attacks. The perpetrators of these attacks run the gamut of traditional nation-states hostile to the United States, geo-political entities, and a proliferating number of Non-Governmental Organizations (NGOs) or electronically networked terrorist groups.

Increasingly, the attacks are also traced to a growing number of disaffected individuals, who seek thrills in cyber gamesmanship and others, who consider themselves disenfranchised or otherwise wronged; they share intent to act in a malicious or destructive manner against the interests of the United States.

To defend against such cyber attacks, the United States is in need of an effective, long-term Information Assurance (IA) policy, the foundation of which must include the defense of United States' critical infrastructures, accomplished within a framework of an expanding Defense Information Infrastructure (DII), National Information Infrastructure (NII) and Global Information Infrastructure (GII). Such a policy requires a careful balancing between the imperatives of Information Assurance and critical infrastructure protection and the preservation of the civil liberties guaranteed by the 1st and 4th Amendments to the United States Constitution.

The results of this study strongly suggest that the United States lacks a coherent Information Assurance policy to protect its own critical national infrastructures leaves United States' critical information infrastructure vulnerable to Strategic Information Warfare (SIW) attack and the consequent disruption of essential societal services on a national scale. Further, the results of this writer's eight-year study strongly suggest that the Clinton Administration completely failed to affect a viable Information Assurance policy for the United States.

This dissertation has discussed the long-standing issues involving data encryption and the government's tight control of data encryption technology as the government's method of choice for preserving access control of worldwide electronic communications. Clinton Administration arguments for and, through force of statute and administrative order, control of data encryption products and technologies in the name of national security, instead exacerbated a growing vulnerability in the nation's critical information infrastructure. Civil libertarians and now, for the first time, the courts, have rejected the Federal Government's stated need for unrestricted access to private electronic communications in the name of national security.

Coupled with the Clinton Administration's oft-stated position that responsibility for the security of the nation's critical information infrastructure security lies with the commercial sector, the pendulum has swung in favor of the rights of individuals and organizations to the use of any products necessary to secure their private communications from compromise. The reversal at the end of the Clinton Administration of over three decades of restrictive Federal Government control of information assurance through encryption may have ended an era of unfettered government access to electronic communications, but it also made even more difficult the government's ability to "provide for the common defense."

In contending with these major national security issues during its eight years in office, the Clinton Administration largely ignored the role of the professional Federal bureaucracy in shaping policy in favor of elite groups

formed from hand-picked individuals from outside that standing bureaucracy. President Clinton's elites, comprised of highly-placed individuals within the Administration's inner circle, world-renowned subject matter experts, and industry leaders from the private sector, were selected and then formed into Federal Advisory Committees to provide counsel to the President on Information Assurance policy matters. The dismantling of the professional bureaucracy in favor of these elite groups has major implications for future administrations and is worthy of further study, drawing upon the literature on the sociology of elites to examine the impact of their widespread use by the Clinton Administration on mainstream democratic theory.

The dissertation has suggested that the Information Age, and with it, the Clinton Administration's National Performance Review, have presaged an evolving, new model of public-private partnering that has government evolving to serve as society's "facilitator" through electronic means. Information Technology-enabled government may evolve into society's ultimate mediating structure. In a growing demassified, electronic culture, Information Age private-sector entities might also assume the service provider role of government, providing a full range of electronic commerce services and information security functions for their constituents directly over networks and infrastructure regulated by government. The human interface would be left to the pluralistic venues and mediating structures of the local neighborhood, church, or semi-voluntary service organizations, where association and access is strictly voluntary.

Information Age technology promotes the automation of service provision in a way that, save for oversight and mediating disputes, affords government the opportunity to extricate itself completely from service provision. Government administration has within its power the ultimate outsourcing mechanism, courtesy of the Information Age, with the power to alleviate itself from a set of service provision tasks for which it was never intended, while promoting a full-time focus on supporting the governance function for which it was. Additional research into this paradigm change for administrative governance in the Information Age would also be appropriate.

As this dissertation has discussed, the accelerating "waves" of change surrounding society offers both unique opportunities for the society to evolve and grow in ways that can scarcely be comprehended, while at the same time creating new challenges in terms of security, inclusiveness, and equitable distribution. The Information Age, with all its wonders, has the potential to split wide the economic, educational, and employment opportunity gulfs that separate the members of the same society. There is serious research potential in this arena for consideration.

The rapidly accelerating vistas of the Information Age may be outstripping government's ability to evolve with it, perhaps into the mega-mediating structure suggested previously. The role that Public Administration has sought for itself in the modern era might be one of change agent and facilitator of the new paradigm. As Stone noted, every policy issue involves the distribution of something. An analysis of the emerging role of Public

Administration as a mega-mediating structure catalyzed through information automation could be the subject for additional, valuable research, as well.

[1] Norman Davis, "An Information Revolution in Military Affairs," in *In Athena's Camp: Preparing for Conflict in the Information Age. E*d. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corp., 1997), 79-98.

[2] Blank, Stephen J., "Preparing for the Next War: Reflections on the Revolution in Military Affairs," *In Athena's Camp: Preparing for Conflict in the Information Age, E*d. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corp., 1997), 62.

[3] Raoul Henri Alcala, "Guiding Principles for Revolution, Evolution, and Continuity in Military Affairs," as cited in Bracken and Alcala, *Whither the RMA: Two Perspectives on Tomorrow's Army* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1994), 27-29.

[4] The White House, The President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection,* October 1997, 17.

[5] Ibid., 4.

[6] Bruce D. Berkowitz, "Warfare in the Information Age," in *In Athena's Camp: Preparing for Conflict in the Information Age,* ed. John Arquilla and David Ronfeldt, 79-98 (Santa Monica, CA: RAND, 1997), 181.

[7] Ibid., 4-5.

[8] Roger C. Molander, et al, *Strategic Information Warfare Rising* (Santa Monica, CA: National Defense Research Institute, RAND, 1998), xi.

[9] Jan M. Lodal, Deputy Under Secretary of Defense for Policy, "Implications for National Defense," Proceedings from the Conference on National Security in the Information Age, ed. General James P. McCarthy, USAF [Ret](United States Air Force Academy, 28 February-1 March 1996), 97.

[10] Charles E. Lindblom and Edward J. Woodhouse, *The Policy-Making Process*, 3d ed. (Upper Saddle River, New Jersey: Prentice Hall, 1993), 62-63.

[11] Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: The Free Press, 1986), 136.

[12] United States General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (Washington, D.C.: GAO/AIMD-00-295), 6 September 2000, 1.

[13] Ibid., 2.

[14] Ibid., 27.

[15] James D. Thompson, *Organizations in Action* (New York: McGraw-Hill Book Company, 1971), 145.

[16] United States General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, D.C.: GAO/AIMD-96-84), 22 May 1996, 31.

[17] United States General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (Washington, D.C.: GAO/AIMD-00-295), 6 September 2000, 33.

[18] Ibid., 31.

[19] Ibid., 33.

[20] Ibid., 33.

[21] Public Law 104-106, Section 5125(a), 10 February 1996.

[22] Ibid., 275.

[23] Op.Cit., Section 5125(a).

[24] United States General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (Washington, D.C.: GAO/AIMD-00-295), 6 September 2000, 32.

[25] Thompson, 126-127.

[26] Phillip Selznick. *Leadership in Administration* (Berkeley, CA: University of California Press, 1984), 35-36.

[27] Ibid., 1 (d), 1.

[28] John W. *Kingdon, Agendas, Alternatives, and Public Policies* (New York: HarperCollins College Publishers, 94-95.

[29] Murray Edelman, *The Symbolic Uses of Politics* (Urbana, Illinois: University of Illinois Press, 1985), 6.

[30] Thomas A. Birkland, *After Disaster; Agenda Setting, Public Policy, and Focusing Events* (Washington, D.C.: Georgetown University Press, 1997), 22.

[31] Kingdon, 98.

[32] Ibid.,18.

[33] Kingdon, 204.

[34] Ibid., 205.

[35] Ibid., 33

[36] Francis Rourke and Paul Schulman, "Adhocracy in Policy Development," *Social Science Journal*, vol. 26, no. 2 (1989), 131-142.

[37] William Cohen, Janet Reno, William Daley, and Jacob Lew, *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace,* 16 September 1999, 5.

[38] Ibid., 5.

[39] Ibid., 118.

[40] Ibid., 119.

[41] James G. March and Johan P. Olsen, *Rediscovering Institutions* (New York, NY: The Free Press, 1989), 11.

BIBLIOGRAPHY

Ackoff, Russell. "The Future of Operations Research is Past." *Journal of Operational Research Society* 30.2 (1979): 90-104.

Adams, James. *The Next World War.* New York: Simon and Schuster, 1998.

Adler, Paul S., and Bryan Borys. "Two Types of Bureaucracy: Enabling and Coercive." *Administrative Science Quarterly* 41.1 (Mar. 1996): 61-89.

ADPA/NSIA. *CINCSPACE* Summer Study. *Commercial Industry Partnering With The Military To Achieve The United States Space Vision.* 25 Sept. 1997.

"Air Force Gets Infowar Assist." *Government Computer News* 23 Nov. 1998: 3.

Allen, Edward L. Letter to Barry Steinhardt. 10 Aug. 1998.

Allen, Thomas B. *War Games-The Secret World of the Creators, Players, and Policy Makers Rehearsing World War III Today.* New York: McGraw-Hill Book Company, 1987.

Allison, Graham. *Essence of Decision: Explaining the Cuban Missile Crisis.* Boston: Little Brown, 1971.

Andrews, Duane P. Letter to Dr. Craig I. Fields. 21 Nov. 1996.

Apple, James. Director, Systems Development Operations, TRW. Series of private discussions/emails, June 1998-Apr. 2000.

Arbel, A. *Exploring Interior-Point Linear Programming.* Cambridge, MA: MIT Press, 1993.

Arquilla, John, and David Ronfeldt. "Cyber War Is Coming!" *In Athena's Camp: Preparing for Conflict in the Information Age.* Ed. John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corp., 1997. 23-60.

---. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: RAND, 1997.

---. *The Advent of Netwar.* MR-789-OSD, 1996. 3-16.

---, and Michele Zanini. "Networks, Netwar and Information Age Terrorism." Ed. Ian O. Lesser, et al. *Countering the New Terrorism.* Santa Monica, CA: RAND, Inc., 1999.

Berger, Peter L., and Richard J. Newhouse. *To Empower People: The Role of Mediating Structures in Public Policy.* Washington, D.C.: American Enterprise Institute for Public Policy Research, 1977.

Berkowitz, Bruce D. "Warfare in the Information Age." *In Athena's Camp: Preparing for Conflict in the Information Age.* Ed. John Arquilla and David Ronfeldt. 79-98 Santa Monica, CA: RAND, 1997. 175-189.

Bernstein v. Department of State. 945 F. Supp. 1279. N.D. Cal. 1996.

Bernstein v. Department of State. 974 F. Supp. 1288. N.D. Cal. 1996.

Birkland, Thomas A. *After Disaster: Agenda Setting, Public Policy and Focusing Events.* Washington, D.C.: Georgetown University Press, 1997.

Blank, Stephen J. "Preparing for the Next War." *Strategic Review* 24.2 (Spring 1996): 17-25.

---. "Preparing for the Next War: Reflections on the Revolution in Military Affairs." *In Athena's Camp: Preparing for Conflict in the Information Age. E*d. John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corp., 1997. 61-78.

Boehm, Barry W. Software Engineering Economics. Upper Saddle River, NJ: Prentice-Hall, Inc., 1981.

Bracken, Paul, and Raoul Henri Alcala. *Whither the RMA: Two Perspectives on Tomorrow's Army.* Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1994. 27-29.

Brewer, Gary. "The Scope of the Policy Sciences." New Haven, CT: Mimeo course Syllabus, 1978; *Making and Managing Policy: Formulation, Analysis, Evaluation.* Ed. G. Ronald Gilbert. New York: Marcel Dekker, Inc., 1984. 13.

Brewin, Bob. "DOD Lays Groundwork for Network-Centric Warfare." Editorial. *Federal Computer Week Supplement* 10 Nov. 1997: 1.

Brock, Jack L., Jr. "Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations." Testimony before the Subcommittee on Technology, Terrorism and Government Information. Committee on the Judiciary. U.S. Senate. Washington, D.C.: GPO, 6 Oct. 1999.

Bronson, Richard. "Operations Research." *Shaum's Outline Series in Engineering.* New York: McGraw-Hill Book Company, 1982

Brown, Ronald H. "Putting the Information Infrastructure to Work." Gaithersburg, MD: National Institutes of Standards and Technology, 4 May 1994.

Brownstein, Charles N. "The Experimental Evaluation of Public Policy." *Public Policy Making in a Federal System.* Ed. Charles O. Jones and Robert D. Thomas. Beverly Hills, CA: SAGE Publications, Inc., 1976.

Caires, Greg. "Air Force Seeks Information Superiority Through New Battlelab." *Defense Daily* 30 July 1997: 1.

Calpin, James A. "The Tyranny of Moore's Law." *Proceedings* 126/2/1.164 (Feb. 2000): 64-66.

Campbell, Donald Draper. *Network Reliability and Interoperability Council (NRIC).* 15 Mar. 2000 <http://www.nric.org.>

Capen, Alan D. "Information Chiefs Join Federal Executive Teams." *SIGNAL* 51.1 (May 1997): 75-77.

---. "Its Vulnerability, Not Threat-Stupid!" *SIGNAL* 52.1 (Sept. 1997): 69-70.

Caruana, Patrick, Lt. Gen., USAF (Ret). Former Vice-Comander, United States Air Force Space Command. Vice President and SBIRS PDRR Program Manager, TRW Space and Electronics Group. Series of private discussions/emails, Aug. 1999-Apr. 2000.

Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare-Its Origins and Future." *Proceedings* U.S. Naval Institute 124/1/1.139 (Jan. 1998): 28-35.

Clausewitz, Carl von. *On War.* Ed. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Cleland, David I., and William R. King. *Systems Analysis and Project Management.* 3rd ed. New Delhi: McGraw-Hill Book Company, 1983.

Clinton, William Jefferson. "Presidential Memorandum on Electronic Commerce." Washington, D.C.: GPO, 1 July 1997. 1.

---. Letter to Mr. William T. Esprey. 7 July 1995.

Cobb, Roger W., and Charles D. Elder. *Participation in American Politics: The Dynamics of Agenda-Building.* Baltimore, MD: John Hopkins University Press, 1983.

Cohen, William, William Daley, Jacob Lew, and Janet Reno. "Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace." *A Report to the President of the United States.* Washington, D.C.: GPO, 16 Sept. 1999.

Computer Security Institute and the FBI International Computer Crime Squad, San Francisco Office. "Computer Crime and Security Survey." Department of Defense. National Security Agency. *The Insider Threat to United States Government Information Systems* (Draft). *Washington, D.C.: GPO,* Jan. 1999.

Conrow, Edmund C., and Patricia S. Shishido. "Implementing Risk Management on Software Intensive Projects." *IEEE Software* 14.3 (May-June 1997): 84-89.

Cooper, Jeffrey R. "Another View of the Revolution in Military Affairs." *Conference Proceedings of the Fifth Annual Conference on Strategy.* Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, Apr. 1994.

---. "Strategic Implications of the Information Age." *Proceedings from the Conference on National Security in the Information Age.* Ed. General James P. McCarthy. United States Air Force Academy, 28 Feb.-1 Mar. 1996. 71-93.

Copeland, Guy. Computer Sciences Corporation. Working Session Chair, Industry Executive Subcommittee, NSTAC. Series of discussions as participant in NDIA Summer Study. July-Oct. 1999.

Crippen, Dan. Letter to Congressman Henry Hyde. 21 Apr. 1999.

Critical Information Assurance Office. *Practices for Securing Critical Information Assets.* Washington, D.C.: CIAO, Jan. 2000.

Cronin, Thomas. *The State of the Presidency.* Boston: Little, Brown, 1975.

CSIS Panel on Terrorism. *Combating Terrorism: A Matter of Leverage.* Washington, D.C.: The Center for Strategic and International Studies, June 1986.

Danzig, G. *Linear Programming and Extensions.* Princeton, NJ: Princeton University Press, 1963.

Date, Shiruti. "House Speaker Hastert Sets Up Security Team of GOP Members." *Government Computer News* 13 Mar. 2000: 1.

---. "Security Issue Ignites Debate: Congress, GAO Want to See Better Security Planning." *Government Computer News* 20 Mar. 2000: 1.

Davis, Norman. "An Information-Based Revolution in Military Affairs." *In Athena's Camp: Preparing for Conflict in the Information Age. E*d. John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corp., 1997. 79-98.

Denhardt, Robert B. *Theories of Public Organizations.* Monterey, CA: Brooks/Cole Publishing Co., 1984.

Deutch, John M. "Foreign Information Warfare Programs and Capabilities." Testimony before the U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations. Washington, D.C.: GPO, 25 June 1996.

Diffie, Whitfield, and Susan Landau. *Privacy on the Line.* Cambridge, MA: The MIT Press, 1998.

"DOD Approves Information Technology Management Plan." *Government Computer News* 27 Mar. 1997: *C4I.*

Dorobek, Christopher J. "Defense Wants PKI Now." *Government Computer News* 4 May 1998: 1.

---. "Report: White House's Cyberdefense Too Close For Comfort." *Government Computer News* 23 Nov. 1998: 12.

Drogin, Robert. "Defense Shows Holes in Case Against Scientist." *Los Angeles Times* 19 Aug. 2000: A12.

---. "Yearlong Hacker Attack Nets Sensitive U.S. Data." *Los Angeles Times* 7 Oct. 1999: A1.

---. "U.S. Scurries to Erect Cyber-Defenses." *Los Angeles Times* 31 Oct. 1999: A1-A9.

Dupuy, T. N. *Understanding War-History and Theory of Combat.* New York: Paragon House, 1987.

Ecker, Rochelle B. "To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee." *University of Missouri at Kansas City Law Review* 63 (1994): 251-252.

Edelman, Murray. *The Symbolic Uses of Power.* Urbana, IL: University of Illinois Press, 1985.

Electronic Frontier Foundation. "'EFF DES Cracker' Machine Brings Honesty to Crypto Debate." *EFF Press Release* 17 July 1998: 2.

Electronic Frontier Foundation. "RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation." *RSA Data Security Conference.* San Jose, CA: 19 January 1999. 1

Electronic Industries Association. *EIA/IS-632, Systems Engineering.* Washington, D.C.: EIA Engineering Publications Office, 1994.

Elliott, Michael, et al. "Mission: Uncertain." *Newsweek* 5 Apr. 1999: 31.

---. "Special Report: The Cyberwar." *Newsweek* 12 Apr. 1999: 31.

Elster, Jon. *In Rational Choice.* Ed. Jon Elster. NY: New York University Press, 1986.

Esprey, William T. Letter to President William J. Clinton. 20 Mar. 1995.

Estes, Howell M., III. General, USAF (Ret). Former Commander in Chief, United States Space Command. Series of private discussions/emails, Apr. 1998-Feb. 2000.

Executive Order 12024. *Federal Advisory Committees.* Washington, D.C: GPO, 20 Nov. 1977.

--- --- 12333. *Collection Of Foreign Intelligence Data.* Washington, D.C: GPO, 1 Sept. 1981.

--- --- 12382. *President's National Security Telecommunications Advisory Committee.* Washington, D.C: GPO, 13 Sept. 1982.

--- --- 12472. *Assignment Of National Security And Emergency Preparedness Telecommunications Functions.* Washington, D.C: GPO, 3 Apr. 1984.

--- --- 12838. Termination And Limitation Of Federal Advisory Committees. Washington, D.C: GPO, 10 Feb. 1993.

--- --- 12864. *United States Advisory Council On The National Information Infrastructure.* Washington, D.C: GPO, 15 Sept. 1993.

--- --- 12881. *Establishment Of The National Science And Technology Council.* Washington, D.C: GPO, *23 Nov. 1993.*

--- --- 12882. *President's Committee Of Advisors On Science and Technology Policy.* Washington, D.C: GPO, 23 Nov. 1993.

--- --- 12924. *Declaration of National Emergency Under the International Emergency Economic Powers Act.* Washington, D.C: GPO, 19 Aug. 1994.

--- --- 12951. *Release Of Imagery By Space-Based National Intelligence Reconnaissance Systems.* Washington, D.C: GPO, 24 Feb. 1995.

--- --- 12974. *Continuance Of Certain Federal Advisory Committees.* Washington, D.C: GPO, 29 Sept. 1995.

--- --- 12981. *Administration of Export Controls.* Washington, D.C: GPO, 6 Dec. 1995.

--- --- 13010. *Critical Infrastructure Protection.* Washington, D.C: GPO, 15 July 1996.

--- --- 13011. *Federal Information Technology.* Washington, D.C: GPO, 17 July 1996.

--- --- 13020. *Amendment to Executive Order 12981.* Washington, D.C: GPO, 15 Oct. 1996.

--- --- 13026. *Administration Of Export Controls on Encryption Products.* Washington, D.C: GPO, 15 Nov. 1996.

--- --- 13035. *President's Advisory Committee On High-Performance Computing and Communications, Information Technology, and the Next Generation Internet.* Washington, D.C: GPO, 15 Feb. 1997.

--- --- 13038. *Continuance Of Certain Federal Advisory Committees.* Washington, D.C: GPO, 30 Sept. 1999.

--- --- 13062. *Continuance of Certain Federal Advisory Committees and Amendments to Executive Orders 13038 and 131054.* Washington, D.C: GPO, 27 Sept. 1997.

--- --- 13064. *Further Amendment To Executive Order 13010, As Amended, Critical Infrastructure Protection.* Washington, D.C: GPO, 14 Oct. 1997.

--- --- 13092. *President's Information Technology Advisory Committee, Amendments to Executive Order 13035.* Washington, D.C: GPO, 24 July 1998.

--- --- 13113. *President's Information Technology Advisory Committee, Further Amendments to Executive Order 13035, As Amended.* Washington, D.C: GPO, *11 Feb. 1999.*

--- --- 13130. *National Infrastructure Assurance Council.* Washington, D.C: GPO, 14 July 1999.

--- --- 13138. *Continuance Of Certain Federal Advisory Committees.* Washington, D.C: GPO, 30 Sept. 1999.

Ferster, Warren. "U.S. to Buy Private Imagery for Intelligence." *Space News* 12 Apr. 1999: 1.

Fesler, James W., and Donald F. Kettle. *The Politics of the Administrative Process.* Chatham, New Jersey: Chatham House Publishers, Inc., 1991.

Fialka, John J. "Pentagon Studies Art of 'Info War' to Reduce Its Systems Hackers." *The Wall Street Journal* 3 July 1995: A20.

Frederickson, H. George. "Comparing the Reinventing Government Movement with the New Public Administration." *Public Administration Review* 56.3 (May-June 1996): 263-270.

---. *The Spirit of Public Administration.* San Francisco: Jossey-Bass Publishers, 1997.

Frost, David. Vice Admiral, USN (Ret). Director, NDIA Study on Computer Network Defense. Series of discussions as participant in NDIA Summer Study. July-Oct. 1999.

Gaudin, Sharon. "Feds Allow 56-bit Encryption." *Computerworld* 21 Sept. 1998: 6.

---."Hackers Disrupt N.Y. Times Site." *Computerworld* 21 Sept. 1998: 6.

---."Hacks Gain in Malice, Frequency." *Computerworld* 12 Oct. 1998: 38.

Gohagan, John Kenneth. *Quantitative Analysis for Public Policy.* New York: McGraw-Hill Book Company, 1980.

Goldin, Daniel. Administrator, NASA. Former Vice President and General Manager, Space and Technologies Division, TRW. Briefing and follow-up interview, 15th Annual National Space Symposium. Broadmoor Hotel, Colorado Springs, CO. 8 April 1999.

Goldman, John J., and Usha Lee McFarling. "Man Accused of Hacking Into NASA Computers". *Los Angeles Times* 13 July 2000: A15.

Gomory, R. E. "An Algorithm for Integer Solutions to Linear Programs." *Recent Advances in Mathematical Programming. E*d. R.L. Graves and P. Wolf. New York: McGraw-Hill, 1963. 269-302.

Gosselin, Peter G. "Trade Controls on Computers No Easy Goal." *Los Angeles Times* 14 June 1999: A20.

--- "U.S. Computer Curbs on China May Ease." *Los Angeles Times* 2 July 1999: A4.

Green, Donald, and Ian Shapiro, *Pathologies of Rational Choice Theory: A Critique of Applications in Political Science.* New Haven, CT: Yale University Press, 1994. 20-28.

Grier, Peter. "In the Beginning, There Was ARPANET." *Air Force Magazine* 80.1 (Jan. 1997): 66-69.

Haass, Richard N. "Paradigm Lost." *Foreign Affairs* 74.1 (Jan.-Feb. 1995): 43-58.

"Hacker Invades EBay Online Auction Site." *Los Angeles Times* 20 Mar. 1999: C2.

Hall, Keith. Director, National Reconnaissance Office (NRO). Briefing and follow-up interview,14th Annual National Space Symposium. Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

Hammes, T. X. Colonel, USMC. "War Isn't a Rational Business." *United States Naval Institute Proceedings* 124/7/1.145 (July 1998): 22.

Hart, David K., and William Hart. Foreward. "The Organizational Imperative." *Administration and Society* 7.3 (Nov. 1975).

Haver, Richard. Former Deputy Director, Office of Naval Intelligence. Vice President and Director, Intelligence Programs, TRW System and Integration Technologies Group. Briefing and discussion on Information Assurance. TRW Space Park, Building R2/1094, 17 Aug. 1999.

"Hearings Reveal FBI Had Doubts Lee Was China Spy." *Los Angeles Times* 7 Mar. 2000: A22.

Herring, George C. "The Wrong Kind of Loyalty: McNamara's Apology for Vietnam." *Foreign Affairs* 74.3 (May-June 1995): 154-158.

Hoge, James F., Jr. "Media Pervasiveness." *Foreign Affairs* 73.4 (July-Aug. 1994): 136-144.

Howard, John D., and Thomas A. Longstaff. *A Common Language for Computer Security Incidents.* SAND98-866.7. Albuquerque, New Mexico: Sandia National Laboratories, Oct. 1998.

Hunker, Jeffrey. Senior Director for Critical Infrastructure Assurance. National Security Council. Briefing and lunch/interview as participant in NDIA Summer Study. Unisys Washington Corporate Offices, 27 Oct. 1999.

Hutchison, Daniel B. Colonel, USAF (Ret), Deputy Director, Office of Special Projects. United States Air Force. Deputy Program Manager, Space-Based Infrared System (SBIRS), Program Definition and Risk Reduction (PDRR), TRW. Series of private discussions/emails. Feb. 1998-Apr. 2000.

Implementation Task Force. *Network Reliability: The Path Forward.* Washington, D.C: GPO, Feb. 1996.

Jackson, William. "NIST OKs Crypto Products." *Government Computer News* 26 Oct. 1998: 3.

---. "Agencies Say Security is a Bigger Task Than Y2K." *Government Computer News* 10 May 1999: 6.

Jacobs, Lawrence, Eric Lawrence, Robert Shapiro, and Steven Smith. "Congressional Leadership of Public Opinion." *Political Science Quarterly* 113.1 (Spring 1998): 41.

Jenkins-Smith, Hank C. *Democratic Politics and Policy Analysis.* Pacific Grove, CA: Brooks/Cole Publishing, 1990.

"John Tukey; Coined the Words Software and BIT." *Los Angeles Times* 29 July 2000: B6.

Joint Security Commission. *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence from the Joint Security Commission.* Washington, D.C.: *GPO,* 28 Feb. 1994.

Kaplan, Abraham Kaplan. *The Conduct of Inquiry.* New York: Harper and Row Publishers, 1963.

Kaplan, Karen. "In Giveaway of 10,000 PCs, the Price Is Users' Privacy." *Los Angeles Times* 8 Feb. 1999: A1.

Karn v. Department of State. 925 F. Supp. 1. D.D.C. 1996.

Katz, Daniel, and Robert L. Kahn. *The Social Psychology of Organizations.* 2nd ed. New York: John Wiley and Sons, Inc., 1978.

Keegan, John. *The Second World War.* New York: Penguin Books USA Inc., 1990.

Keeney, Ralph L. *Value-Focused Thinking.* Cambridge, MA: Harvard University Press, 1992.

---, and Howard Raiffa. *Decisions with Multiple Objectives.* Cambridge, Eng.: Cambridge University Press, 1993.

Kelly, Rita Mae. "An Inclusive Democratic Polity, Representative Bureaucracies and the New Public Management." *Public Administration Review* 58.3 (May/June 1998): 201-207.

Kingdon, John W. *Agenda, Alternatives, and Public Policies.* 2nd ed. United States: HarperCollins College Publishers, 1995.

Kirlin, John J. "Policy Formulation." *Making and Managing Policy: Formulation, Analysis, Evaluation.* Ed. G. Ronald Gilbert. New York: Marcel Dekker, Inc., 1984. 13-23.

Klee, V., and G. J. Minty. "How Good is the Simplex Algorithm?" *Inequalities, III.* Ed. O. Sisha. New York: Academic Press, NY, 1972. 159-175.

Knowles, John. "IW Battlelab to Go Operational This Month." *Journal of Electronic Defense* 20.6 (June 1997): 26.

Kohut, Andrew, and Robert C. Toth. "Arms and the People." *Foreign Affairs* 73.6 (Nov.-Dec. 1994): 47-61.

Kornblum, Janet. "Federal Unit to Fight Hacking." 23 Mar. 1999: 1-4. *ABCNEWS.com.*<http://more.abcnews.go.com/sections/tech/CNET/cnet_hacking0227.html>.

Kruger, Ruth Gillie. "Analyzing American Social Policy: A Study of the Child Support Provisions of the Personal Responsibility and Work Opportunity and Reconciliation Act of 1996". Diss. U. of Southern California, 1998.

Lanchester, Frederick William. "Mathematics in Warfare." *The World of Mathematics.* Ed. James R. Newman. New York: Simon and Schuster, 1956.

Laswell, H. D. *A Pre-View of Policy Sciences.* New York: Elsevier, 1971; *Making and Managing Policy: Formulation, Analysis, Evaluation.* Ed. G. Ronald Gilbert. New York: Marcel Dekker, Inc., 1984. 13.

Lawlor, Maryann. "Congress, Industry Debate Proposed Encryption Laws," *SIGNAL* 52.1 (Aug. 1997): 66-67.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. *Countering The New Terrorism.* Santa Monica, CA: RAND, 1999.

Levy, Steven. "Courting a Crypto Win." *Newsweek* 17 May 1999: 85.

Lipsky, Michael. "Standing the Study of Public Policy Implementation on its Head." *American Politics and Public Policy.* Ed. Walter Dean Burnham and Martha W. Weinberg. Cambridge, MA: MIT Press, 1978.

Lindblom, Charles E. *Politics and Markets.* New York: Basic Books, 1977.

---, and Edward J. Woodhouse. *The Policy-Making Process.* 3rd ed. Upper Saddle River, New Jersey: Prentice Hall, 1993.

Lodal, Jan M. "Implications for National Defense." *Proceedings from the Conference on National Security in the Information Age.* Ed. James P.. McCarthy. United States Air Force Academy 28 Feb.-1 Mar. 1996. 95-105.

Loiko, Sergei L. "Chechnya: Dozens of Russians Killed." *Los Angeles Times* 4 July 2000: A6.

Luce, R. Duncan, and Howard Raiffa. *Games and Decisions.* 2nd ed. New York: Dover Publications, 1989.

Luttwak, Edward N. "Toward Post-Heroic Warfare," *Foreign Affairs* 74.3 (May-June 1995): 112-122.

Mandelbrot, Benoit B. *The Fractal Geometry of Nature.* 3rd ed. New York: W.H. Freeman and Company, 1983.

Maor, Moshe. "The Paradox of Managerialism." *Public Administration Review* 59.1 (Jan.-Feb. 1999): 5-18.

March, James G., and Johan P. Olsen. *Ambiguity and Choice in Organizations.* NY: Columbia University Press, 1982.

---. *Rediscovering Institutions.* NY: The Free Press, 1989.

Marsh, Robert T. General, USA (Ret.). Chairman, President's Commission on Critical Infrastructure Protection. Briefing and follow-up interview. Beverly Hilton Hotel, Beverly Hills, CA. 14 Nov. 1997.

May, J., and Aaron Wildavsky, eds. "The Policy Cycle." *Sage Yearbooks in Politics and Public Policy.* 5. Beverly Hills, CA: Sage Publishing, 1978; *Making and Managing Policy: Formulation, Analysis, Evaluation.* Ed. G. Ronald Gilbert. NY: Marcel Dekker, Inc., 1984. 13

Meier, Kenneth J. "Bureaucracy and Democracy: The Case for More Bureaucracy and Less Democracy." *Public Administration Review* 57.3 (May-June 1997): 193-199.

Melton, William. "Electronic Cash Transfers." *Proceedings from the Conference on National Security in the Information Age.* Ed. General James P. McCarthy. United States Air Force Academy 28 Feb.-1 Mar. 1996: 285-302.

Mihara, Robert M. Colonel, USAF (Ret). Deputy Director, Office of Special Projects. United States Air Force. Deputy Program Manager, Space-Based Infrared System (SBIRS), Program Definition and Risk Reduction (PDRR), TRW. Series of private discussions/emails. Mar. 1999-Apr. 2000.

Miller, Delbert C. *Handbook of Research Design and Social Measurement. 4th* ed. White Plains, NY: Longman, Inc., 1983. 72.

Mintzberg, Henry. "The Fall and Rise of Strategic Planning." *Harvard Business Review* 72.1 (Jan.-Feb. 1994): 23-38.

Moder, Joseph J., and Salah E. Elmaghraby, eds. *Handbook of Operations Research.* NY: Van Nostrand Reinhold Co., 1978.

Molander, Roger C., Peter A. Wilson, David A. Mussington, and Richard F. Mesic. *Strategic Information Warfare Rising.* Santa Monica, CA: National Defense Research Institute, RAND, 1998.

Money, Arthur L. Under Secretary of Defense for Acquisition and Technology. Dept. of Defense. Briefing and follow-up interview. Air Force 50th Anniversary Expo. Las Vegas Convention Center, Las Vegas, NV. 24 June 1997.

Morrow, James D. *Game Theory for Political Scientists.* Princeton, NJ: Princeton University Press, 1994.

Munro, Neil. "Pearl Harbor." Washingto*n Post* 16 July 1995: C3.

Myers, Richard. USAF, Commander in Chief, U.S. Space Command, Briefing and follow-up interview, 15th Annual National Space Symposium. Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

National Defense Panel. "National Security in the 21st Century: The Challenge of Transformation." *Joint Forces Quarterly* (Summer 1997): 18.

National Performance Review. "Creating a Government That Works Better and Costs Less: The Gore Report." Washington DC: GPO, 1993.

National Defense Industrial Association. 1998 NDIA Space Summer Study. *The Commercial Use of Space.* Washington, D.C.: GPO, Dec. 1998.

Nat. Def. Industrial Asso. 1999 NDIA Space Summer Study. *Computer Network Defense: An Industry Perspective.* Washington, D.C.: GPO, Oct. 1999.

Network Reliability and Interoperability Council. "Network Reliability: The Path Forward." Final Report of the Second Council. Washington, D.C.: GPO, Feb. 1996.

Network Reliability and Interoperability Council. "Network Interoperability: The Key to Competitiveness." Final Report of the Third Council. Washington, D.C.: GPO, 15 July 1997.

Neustadt, Richard E., and Ernest R. May. *Thinking in Time: The Uses of History for Decision-Makers.* NY: The Free Press, 1986.

Nigro, Felix A., and Lloyd G Nigro. *Modern Public Administration.* NY: Harper and Row, Publishers, Inc., 1973.

Oberg, James E. *Space Power Theory.* Interview. 14th Annual National Space Symposium. Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

Olson, Mancur, Jr. *The Logic of Collective Action.* 2nd ed. Cambridge, MA: Harvard UP, 1971.

---. *The Rise and Decline of Nations.* New Haven, CT: Yale UP, 1982.

Osborne, David, and Ted Gaebler. *Reinventing Government.* Reading, MA: Addison-Wesley Longman, Inc., 1992.

---, and Peter Plasttrik. *Banishing Bureaucracy.* Reading, MA: Addison-Wesley Publishing Company, Inc., 1997.

O'Sullivan, Elizabethann, and Gary R. Rassel. *Research Methods for Public Administrators.* NY: Longman, 1989: 30-34.

Ostrow, Ronald J. "U.S. Will Enlarge Its Computer Threat Team." *Los Angeles Times* 23 Mar. 1999: A17.

Padulo, Louis, and Michael A. Arbib. *System Theory.* Washington, D.C.: Hemisphere Publishing Corp., 1974.

"Pentagon Computers are Easy Prey for Hackers, GAO Warns." *Los Angeles Times* 23 May 1996: A1.

"Pentagon Official Denies Technology Aided China." *Los Angeles Times* 18 Sept. 1998: A25.

President's Blue Ribbon Commission on Defense Management. *A Quest for Excellence: Final Report to the President by the President's Blue Ribbon Commission on Defense Management.* Washington, D.C.: GPO, 1986.

President's National Security Telecommunications Advisory Committee. *Telecommunications Outage and Intrusion Information Sharing Report.* Washington, D.C.: GPO, Sept. 1998.

President's National Security Telecommunications Advisory Committee. *Legislative and Regulatory Group Report.* Washington, *D.C.: GPO,* Sept. 1998.

President's National Security Telecommunications Advisory Committee. *Legislative and Regulatory Group: National Services Subgroup White Paper.* Washington, D.C.: GPO, Sept. 1998.

President's National Security Telecommunications Advisory Committee. *Information Infrastructure Group Report.* Washington, D.C.*: GPO,* Sept. 1997.

President's National Security Telecommunications Advisory Committee. *Information Infrastructure Group Report.* Washington, D.*C.:* GPO, Sept. 1998.

President's National Security Telecommunications Advisory Committee. *Interim Transportation Information Risk Assessment Report.* Washington, D.C.: GPO, Dec. 1997.

President's National Security Telecommunications Advisory Committee. *Network Group Intrusion Detection Subgroup Report: Report on the NS/EP Implications of Intrusion Detection Technology Research and Development.* Washington, D.C.: GPO, Dec. 1997.

President's National Security Telecommunications Advisory Committee. *Network Group Report.* Washington, D.C.: GPO, Sept. 1998.

President's National Security Telecommunications Advisory Committee. *Operations Support Group Report.* Washington, D.C.: GPO, Sept. 1998.

President's National Security Telecommunications Advisory Committee. *Outage and Intrusion Information Sharing Report.* Washington, D.C.: GPO, Dec. 1998

President's National Security Telecommunications Advisory Committee. *Telecommunications Outage and Intrusion Information Sharing Report.* Washington, D.C.: GPO, Dec. 1998.

Presidential Decision Directive 62: *Combating Terrorism.* Washington, D.C.: GPO, 22 May 1998.

--- --- --- 63: *Protecting America's Critical Infrastructure.* Washington, D.C.: GPO, 22 May 1998.

Presthus, Robert. *The Organizational Society.* NY: St. Martin's Press, 1978.

Provan, Keith G., and H. Brinton Milward. "A Preliminary Theory of Interorganizational Effectiveness: A Comparative Study of Four Community Mental Health Systems." *Administrative Science Quarterly* 40.1 (Mar. 1995): 24.

Public Law 92-463.*Federal Advisory Committee Act.* Washington, D.C.: GPO, 5 Jan. 1973.

--- --- 94-409. *Government in the Sunshine Act.* Washington, D.C.: GPO, 12 Mar. 1977.

--- --- 105-153. *Federal Advisory Committee Acts Amendments of 1997.* Washington, D.C.: GPO, 17 Dec. 1997.

Ramos, Alberto Guerreiro. *The New Science of Organizations.* Toronto, Canada: University of Toronto Press, 1981.

Randolph, Bernard. General, USAF (Ret). Former Commander in Chief, United States Air Force Systems Command. Vice President, Space and Electronics Group, TRW. Series of private discussions/emails. Feb. 1993-Apr. 2000.

Reinsch, William A. Letter to Barry Steinhardt. 26 Aug. 1998.

Richter, Paul. "Need for Anti-Terrorism Chief Debated." *Los Angeles Times* 23 Jan. 1999: A11.

Robinson, Clarence A. "Orchestrating Standards Buoys Cooperative Combat Operations." *SIGNAL* 51.11 (July 1997): 55.

---. "Information Warfare Demands Battlespace Visualization Grasp," *SIGNAL* 51.6 (Apr. 1997): 17.

Rothrock, John. "Information Warfare: Time for Some Constructive Skepticism." *American Intelligence Journal* Spring-Summer 1999: 71-76.

Rourke, Francis, and Paul Schulman. "Adhocracy in Policy Development." *Social Science Journal* 26.2 (1989): 131-142.

Rusaw, A. Carol. *Transforming the Character of Public Organizations.* Westport, CN: Quorum Books, 1998.

Ryan, Michael. General and Chief of Staff, USAF. Briefing and follow-up interview. Beverly Hilton, Beverly Hills, CA. 14 Nov. 1997.

Salamon, Lester M. "Follow-ups, Letdowns, and Sleepers: The Time Dimension in Policy Evaluation." *Public Policy Making in a Federal System.* Ed. Charles O. Jones and Robert D. Thomas. Beverly Hills, CA: SAGE Publications, Inc., 1976.

---. "The Rise of the Nonprofit Sector." *Foreign Affairs* 73.4 (July-Aug. 1994): 109-122.

Samuelson, Robert J. "Puzzles of the 'New Economy'." *Newsweek* 17 Apr. 2000: 48.

Scharpf, Fritz W. *Games Real Actors Play: Actor-Centered Institutionalism in Policy Research.* Boulder, Colorado: Westview Press, 1997.

Schattschneider, E. E. *A Semi-Sovereign People.* NY: Holt, Reinhart, and Winston, 1960.

Schon, Donald A. *Beyond the Stable State.* NY: W.W. Norton & Company, 1971.

---. *The Reflective Practitioner.* NY: Basic Books, Inc., 1983.

Schwarzkopf, H. Norman, and Peter Petre. *It Doesn't Take a Hero.* NY: Linda Grey Bantam Books, 1992.

Scott, Richard W. *Organizations: Rational, Natural, and Open Systems.* Englewood Cliffs, NJ: Prentice-Hall, 1992.

Selznick, Phillip. *Leadership in Administration.* Berkeley, CA: U of California Press, 1984.

Shepsle, Kenneth A., and Mark S. Bonchek. *Analyzing Politics: Rationality, Behavior, and Institutions.* NY: W.W. Norton & Company, 1997.

Shiver, Jube Jr., and Charles Piller. "U.S. Role Hit as Latest Computer Bug Scare Fizzles." *Los Angeles Times* 20 May 2000: C1-C3.

Simon, Herbert A. "Administrative Decision Making." *Public Administration Review* (Mar. 1965): 35-36.

---. *Administrative Behavior.* 3rd ed. NY: The Free Press, 1976.

Slabodkin, Gregory. "Suit of Armor Fits 21st Century." *Government Computer News* 9 Mar. 1998: 45.

Smith, Daniel, Kevin Leyden, and Stephen Borrelli. "Predicting the Outcomes of Presidential Commissions: Evidence from the Johnson and Nixon Years." *Presidential Studies Quarterly* 28.2 (Spring 1998): 273-283.

Sokolski, Henry. Executive Director, The Nonproliferation Policy Education Center. Briefing and interview, 14th Annual National Space Symposium. Broadmoor Hotel, Colorado Springs, CO. 8 April 1998.

Steinhoff, Jeffrey C. Letter to Senator Robert F. Bennett (R-UT). Accompanying report GAO/AIMD-00-1: "Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences." Washington, D.C.: GPO, Oct. 1999.

Stoll, Cliff. *The Cuckoo's Egg.* NY: Pocket Books, 1990. 9.

Stone, Brad. "Bitten by Love." *Newsweek* 15 May 2000: 42.

Stone, Deborah. *Policy Paradox.* NY: W. W. Norton and Company, Inc., 1997.

Studeman, William O. Admiral, USN (Ret). Former Chief of Naval Intelligence. Former Deputy Director, CIA. Vice-President and Deputy General Manager, TRW Systems Integration and Technology Group. Series of private discussions/emails. Feb. 1997-Apr. 2000.

"Systems analysis." *Webster's New Collegiate Dictionary.* 3rd ed. 1983.

Tabacchi, Leonard. "Defense Information Infrastructure Master Plan." Appendix C: *Foundation-Technology Support.* 6 Nov. 1995: 1-4.

Taha, Hamdy A. "Linear Programming." *Handbook of Operations Research.* Eds, Moder, Joseph J. and Salah E. Elmaghraby. New York, NY: Van Nostrand Reinhold Co., 1978.

Taylor, James G. "An Introduction to Lanchester-Type Models of Warfare." *Proceedings of the Workshop on Modeling and Simulation of Land Combat.* Ed. L.G. Callahan. Atlanta, GA: Georgia Institute of Technology Research Institute, 1983.

Taylor, Mark Z. "Dominance Through Technology." *Foreign Affairs* 74.6 (Nov.-Dec. 1995): 14-20.

Thompson, Dennis F. "The Possibility of Administrative Ethics." *Public Administration Review* 45.5 (Sept.-Oct. 1985): 555.

Thompson, Fred. "Management, Control and the Pentagon: The Organizational Strategy-Structure Mismatch." *Public Administration Review* 51.1 (Jan.-Feb. 1991): 52-66.

Thompson, James D. *Organizations in Action.* NY: McGraw-Hill Book Company, 1967.

Tiboni, Frank. "Thompson Upbraids Agencies Over Systems Securities." *Government Computer News* 19 Oct. 1998: 9.

---. "In Turnabout, McCain Sponsors Bill to Ease Crypto Export Limits." *Government Computer News* 26 Apr. 1999: 6.

Toffler, Alvin, and Heidi Toffler. *The Third Wave.* NY: William Morrow and Company, Inc., 1980.

Toffler, Alvin. Toffler and Associates. Briefing and interview, 14th Annual National Space Symposium. Broadmoor Hotel, Colorado Springs, CO. 7 April 1998.

Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructure.* Washington, D.C.: GPO, July 1998.

United States Cong. *Rep.* Rick Boucher of Virginia. "National Information Infrastructure Act of 1993." *HR.*1767. 103rd Cong. 1st sess. *Cong. Rec.* 21 Apr. 1993: H5084-5094.

---, ---, Cong. House. Rep. George E. Brown, Jr., of California. "Information Infrastructure and Technology Act of 1992." *HR.*5759, 102nd Cong. 2nd sess. *Cong. Rec.* 4 Aug. 1992: E2358.

---, ---, Cong. House. Rep. George E. Brown, Jr., of California. "Encryption Standards and Procedures Act of 1994." *H.R. 5199.* 103rd Cong. 1st sess. *Bill Summary and Status for the 103rd Congress. Cong. Rec.* 6 Oct. 1994.

---, ---, Cong. House. Rep. Maria Cantrell of Washington. "Legislation to Amend the Export Control Act of 1979." *HR.* 3627, 103rd Cong. 1st sess. *Cong. Rec.* 24 Nov. 1993: E3110-E3112.

---, ---, Cong. House. Rep. William D. "Don" Edwards of California. "Communications Assistance for Law Enforcement Act." *HR.* 4922. 103rd Cong. 1st sess. *Cong. Rec.* 4 Oct. 1994: H10726, H10773-10783, H10917, S14660, H11435, S15225, H11563, D1259.

---, ---, Cong. House. Rep. Samuel Gejdenson of Connecticut. "The Export Administration Act of 1994." *HR.* 3937. 103rd Cong. 1st sess. *Bill Summary and Status for the 103rd Congress. Cong. Rec.* 2 Mar. 1994.

---, ---, Cong. House. Rep. Samuel Gejdenson of Connecticut. "The Export Administration Act of 1994." *HR.* 3937. 103rd Cong. 1st sess. *Cong. Rec.* 25 May-14 July 1994: H4089, H4653, H4720-4721, H5738-5740.

---, ---, Cong. House. Rep. Robert Goodlatte of Virginia. "Security and Freedom Through Encryption (SAFE) Act." *HR. 3011.* 104th Cong. 2nd sess. *Cong. Rec.* 5 Mar. 1996: E276-277.

---, ---, Cong. House. Rep. Robert Goodlatte of Virginia. "National Infrastructure Protection Act of 1996." *HR. 4095.* 104th Cong. 2nd sess. *Cong. Rec.* 17 Sept. 1996: H10524 [17SE].

---, ---, Cong. House. Rep. Robert Goodlattee of Virginia. "Security and Freedom Through Encryption (SAFE) Act." *H.R.850.* 106th Cong. 1st sess. *Cong. Rec.* House Report 106-117, Part III. 19 July 1999: H5838.

---, ---, Cong. House. Rep. Bart Gordon of Tennessee. "Providing for Consideration of H.R. 3937, Export Administration Act of 1994." *Cong. Rec.* 14 July 1994: H5731-5733.

---, ---, Cong. House. Rep. Porter J. Goss of Florida. "Encryption for the National Interest Act." *H.R. 2616.* 106th Cong. 1st sess. *Bill Summary and Status for the 106th Congress. Cong. Rec.* 27 July 1999.

---, ---, Cong. House. Rep. Porter J. Goss of Florida. "Encryption for the National Interest Act." *H.R. 2616.* 106th Cong. 1st sess. *Cong. Rec.* 27 July 1999: H6581.

---, ---, Cong. House. Rep. Doc Hastings of Washington. "Networking and Information Technology Research and Development Act." *HR.* 422. 106th Cong. 2nd sess. *Cong. Rec.* 15 Feb. 2000: H389-392.

---, ---, Cong. House. Rep. Henry Hyde of Illinois. Legislative Hearing on *H.R.850*, "Security and Freedom Through Encryption (SAFE) Act." 4 Mar. 1999. http://www.house.gov/judiciary/106-19.htm.

---, ---, Cong. House. Rep. Jim Saxton of New Jersey. "Expressing the sense of the Congress regarding Internet security and 'cyberterrorism'." *H. CON. RES. 285.* 106th Cong. 2nd sess. *Bill Summary and Status for the 106th Congress. Cong. Rec.* 15 Mar. 2000: 1-2.

---, ---, Cong. House. Rep. F. James Sensenbrenner, Jr., of Wisconsin. "Computer Security Enhancement Act of 1997." *H.R. 1903.* 105th Cong. 1st sess. *Cong. Rec.* 17 June 1997: E1231.

---, ---, Cong. House. Rep. F. James Sensenbrenner, Jr., of Wisconsin. "Next Generation Internet Research Act of 1998." *H.R.* 3332. 105th Cong. 2nd sess. *Cong. Rec.* 12 Nov. 1998: D1203-1204.

---,---, Cong. House. Representative F. James Sensenbrenner, Jr. of Wisconsin. "Network and Information Technology Research and Development Act." *H.R. 2086.* 106th Cong. 1st sess. *Cong. Rec.* 9 June 1999: E1186.

---, ---, Cong. House. Rep. F. James Sensenbrenner, Jr. of Wisconsin. "Computer Security Enhancement Act of 1999." *H.R. 2413.* 106th Cong. 1st sess. *Cong. Rec.* 1 July 1999: E1491.

---, ---, Senate. Senator Conrad Burns of Montana. "Promotion of On-Line in the Digital Era (Pro-CODE) Act of 1996." *S.1726.* 104th Cong. 2nd sess. *Cong. Rec.* 2 May 1996: S4624-4627.

---, ---, Senate. Senator Conrad Burns of Montana. "Promotion of On-Line in the Digital Era (Pro-CODE) Act of 1997." S.377. 105th Cong. 1st sess. *Cong. Rec.* 27 Feb. 1997: S1756.

---, ---, Senate. Senator William Frist of Tennessee. "The Next Generation Internet 2000 Act." *S. 2046.* Referred to the Committee on Commerce, Science, and Technology. 106th Cong. 2nd sess. *Cong. Rec. Daily Digest* 9 Feb. 2000: D370.

---, ---, Senate. Senator William Frist of Tennessee. "Next Generation Internet Research Act of 1998." *S.1609.* 105th Cong. 2nd sess. *Cong. Rec.* 4 Feb. 1998: S386.

---, ---, Senate. Senator William Frist of Tennessee. "The Next Generation Internet 2000 Act." *S. 2046.* 106th Cong. 2nd sess. *Cong. Rec.* 9 Feb. 2000: S546.

---, ---, Senate. Senator Albert Gore, Jr. of Tennessee. "The High-Performance Computing Act of 1991." *S.272.* 102nd Cong. 1st sess. *Cong. Rec.* 24 January 1991: S1159.

---, ---, Senate. Senator Albert Gore, Jr. of Tennessee. "Information Infrastructure and Technology Act of 1992." *S.2937.* 102nd Cong. 2nd sess. *Cong. Rec.* 1 July 1992: S7261.

---, ---, Senate. Senator Orrin G. Hatch of Utah. "Internet Integrity and Critical Infrastructure Protection Act of 2000." S.2448. 102nd Cong. 2nd sess. *Bill Summary and Status for the 106th Congress. Cong. Rec.* 13 Apr. 2000: 1-5.

---, ---, Senate. Senator Patrick Leahy of Vermont. "Electronic Rights for the 21st Century Act." *S.854.* 106th Cong. 1st sess. *Cong. Rec.* 21 Apr. 1999: S4042-4047.

---, ---, Senate. Senator Patrick Leahy of Vermont. "Internet Security Act of 2000." *S. 2430.* 106th Cong. 2nd sess. *Bill Summary and Status for the 106th Cong.* 13 Apr. 2000: 1-9.

---, ---, Senate. Senator Patrick Leahy of Vermont. *S. 2375*, 103rd Cong. 1st sess. *Cong. Rec.* 9 Aug. 1994: S11055-11062, S15176-15180.

---, ---, Senate. Senator Frank Leahy of Vermont. "The Encrypted Communication Privacy Act of 1997 (ECPA) Act of 1997. *S.376.* 105th Cong. 1st sess. *Cong. Rec.* 27 Feb. 1997: S1749.

---, ---, Senate. Senator John McCain of Arizona. "Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999." *S.798.* SEC. 103. 106th Cong. 1st sess. *Cong. Rec.* S3695. Washington, D.C.: GPO, 14 Apr. 1999.

---, ---, Senate. Senator John McCain of Arizona. Committee on Commerce, Science and Transportation. Hearing on Encryption. "Testimony, Department of Justice." *Cong. Rec.* 10 June 1999: S10388.

---, ---, Senate. Senator Jon Kyle of Tennessee. "National Infrastructure Protection Act of 1995/6." *S.982.* 104th Cong. 2nd sess. *Cong. Rec.* 8 Feb. 1996: S9554.

United States Department of Commerce. Federal Communications Commission, Network Reliability and Interoperability Council (NRIC). "Network Reliability: The Path Forward." *NRIC Report.* Washington, D.C.: GPO, Jan. 1996.

---, Dept. of Commerce. "Network Interoperability: The Key to Competition." *NRIC Report.* Washington, D.C.: GPO, 15 July 1997.

---, Dept. of Commerce. Critical Infrastructure Assurance Office. *Statement of John S. Tritak, Director, Critical Infrastructure Assurance Office before the Subcommittee on Technology, Terrorism and Government Information, Senate Judiciary Committee.* Washington, D.C.: GPO, 6 Oct. 1999.

---, Dept. of Commerce. *Statement by John S. Tritak, Director, Critical Infrastructure Assurance Office before the Subcommittee on Government Management, Information and Technology. House Government Reform Committee.* Washington, D.C.: GPO, 9 Mar. 2000.

---, Dept. of Commerce. National Institute of Standards and Technology. " Announcing Plans to Develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange." *Federal Register* 13 May 1997: 26294.

---, Dept. of Commerce. *Guide for Developing Security Plans for Information Technology Systems.* NIST Special Publication 800-18. Washington, D.C.: GPO, Dec. 1998.

---, Dept. of Commerce. Office of Public Relations. "Brown Releases Report Highlighting Benefits, Barriers of National Information Highway." Washington, D.C.: GPO, 4 May 1994.

United States Department of Defense. *Joint Doctrine for Information Operations.* Joint Pub. 3-13. Washington, D.C.: GPO, 9 Oct. 1998.

---, Dept, of Defense. *Public Key Infrastructure Roadmap for the Department of Defense.* Version 2.0, Revision C. Washington, D.C.: GPO, 28 Mar. 2000.

---, Dept. of Defense. Dept. of the Air Force. HQ ACC/DRC. *Air Force Modernization Planning: Theater Battle Management Mission Area Plan FY1996.* Washington, D.C.: GPO, 15 Nov. 1995.

---, Dept. of Defense. United States Air Force. "Global Engagement: A Vision of the 21st Century Air Force." Washington D.C.: GPO, 1997.

---, Dept. of Defense. HQ AFSPC/DO. *Information Superiority: Air Force Space Command's Vision for the 21st Century.* Washington, D.C.: GPO, 1 Dec. 1997.

---, Dept. of Defense. National Security Agency. *The Insider Threat to United States Government Information Systems* (Draft). Washington, D.C.: GPO, Jan. 1999.

---, Dept. of Defense. Office of the Under Secretary of Defense for Acquisition and Technology. Defense Science Board. *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield: October 1994.* Washington, D.C.: GPO, 3 Nov. 1994.

---, Dept. of Defense. *Defense Science Board Summer Study Task Force on Improved Application of Intelligence to the Battlefield: May-July 1995.* Washington D.C.: GPO, Sept. 1995.

---, Dept. of Defense. *Report of the Defense Science Board Task Force On Improved Application of Intelligence To The Battlefield: May-July 1996.* Washington, D.C.: GPO, 24 Feb. 1997.

---, Dept. of Defense. *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D).* Washington, D.C.: GPO, 25 Nov. 1996.

---, Department of Justice. Senate Committee on Commerce, Science and Transportation. *Hearing on Encryption.* Washington, D.C.: GPO, 10 June 1999.

---, Department of Justice. President's Working Group on Unlawful Conduct on the Internet. *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet.* Washington, D.C.: GPO, Mar. 2000.

---, Dept. of Justice. Computer Crime and Intellectual Property Section (CCIPS). *What Does CCIPS DO?* 16 Mar. 2000. <http://www.usdoj.gov/criminal/cybercrime/ccips.html>.

---, General Accounting Office, *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. Testimony of Jack L. Brooks, Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division. Before the Subcommittee on Technology, Terrorism and Government Information. Committee on the Judiciary, United States S. GAO/T-AIMD-00-72.* Washington, D.C.: GPO, 1 Feb. 2000.

---, General Accounting Office. *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences.* GAO/AIMD-00-1. Washington, D.C.: GPO, 1 Oct. 2000.

---, General Accounting Office. *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk.* GAO/AIMD-99-107. Washington, D.C.: GPO, 26 Aug. 1999.

--, General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* GAO/AIMD-96-84. Washington, D.C.: GPO, 22 May 1996.

---, *General Accounting Office. Information Security: Opportunities for Improved OMB Oversight of Agency Practices.* GAO/AIMD-96-110. Washington, D.C.: GPO, 24 Sept. 1996.

---, General Accounting Office. *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies.* GAO/AIMD-00-295. Washington, D.C.: GPO, 6 Sept. 2000.

---, General Accounting Office. *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk.* GAO/AIMD-98-92. Washington, D.C.: GPO, 23 Sept. 1998.

---, General Accounting Office. *Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. Statement of Joel C. Willemssen. Director. Civil Agencies Information Systems. Accounting and Information Management Division. GAO. Before the Subcommittee on Government Management. Information and Technology. Committee on Government Reform.* U. S. House. Washington, D.C.: GPO, 22 June 2000.

Van Inwegen, Earl S. Brigadier General, USAF (Ret). Former Director, TENCAP, USAF. Director, Air Force C4I Programs, TRW. Series of private discussions/ emails. Feb. 1996-June 1998.

"Vector." *Webster's Ninth New Collegiate Dictionary.* 1983.

Vistica, Gregory L. "Cyberwar and Sabotage." *Newsweek* 31 May 1999: 38.

---. "We're in the Middle of a Cyberwar." *Newsweek* 20 Sept. 1999: 52.

Webb, Helena. "Regulating Computer Exports." *Los Angeles Times* 14 June 1999: A20.

Weigley, Russell F. Rev. of *War and the Paradox of Technology* by Van Creveld. *International Security* (Fall 1989): 196.

Wehrfritz, George. "Raiding the 'Love Bug.'" *Newsweek* 22 May 2000: 44.

The White House. *A National Security Strategy For A New Century.* Washington, D.C.: GPO, May 1997.

---. *A National Security Strategy For A New Century.* Washington, D.C.: GPO, Dec. 1999.

---. Information Infrastructure Task Force. "The National Information Infrastructure: Agenda for Action." Section III. Washington, D.C.: GPO, 15 Sept. 1993.

---. Information Infrastructure Task Force. "A Nation of Opportunity: Realizing the Promise of the Information Superhighway." Washington, D.C.: GPO, 30 Jan. 1996.

---. Information Infrastructure Working Group. "Privacy and the National Information Infrastructure." Washington, D.C.: GPO, 6 June 1996.

---. *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63.* Washington, D.C.: GPO, May 1998.

---. Office of Management and Budget. OMB Circular No. A-130. *Management of Federal Information Resources.* 50 FR 52730. Washington, D.C.: GPO, 24 Dec. 1985.

---. Office of the Press Secretary. "Administration Updates Encryption Policy." Washington, D.C.: GPO, 16 Sept. 1998.

---. "Background on Clinton-Gore Administration's Next-Generation Internet Initiative." Washington, D.C.: GPO, 10 Oct. 1996.

---. "Export Controls on Computers." Washington, D.C.: GPO, 1 Feb. 2000.

---. *HR. 2086. Networking and Information Technology Research and Development Act.* Washington, D.C.: GPO, 15 Feb. 2000).

---. "Internet Initiative Press Release." 10 Oct. 1996.

---. "Press Briefing by The Vice President, Deputy Chief of Staff John Podesta, Principal Associate Deputy Attorney General Robert Litt, Assistant Director of the FBI Carolyn Morris, Under Secretary of Commerce William Reinsch, Deputy Secretary of Defense John Hamre, and Deputy National Security Advisor Jim Steinberg." Washington, D.C.: GPO, 16 Sept. 1998: 1.

---. "Proposed Implementation of the Government Paperwork Elimination Act." *Federal Register* 5 Mar. 1999.

---. "Statement by the President." Washington, D.C.: GPO, 1 Feb. 2000.

---. "Statement by the President on the Next Generation Internet Research Act of 1998." Washington, D.C.: GPO, 28 Oct. 1998.

---. "Statement by the Press Secretary on Export Control Reform." Washington, D.C.: GPO, 30 Mar. 1994.

---. "Strategic Planning Document-Information and Communications." Washington, D.C.: GPO, 15 Jan. 1994.

---. Office of Science and Technology Policy. "Statement of John H. Gibbons before the Committee on Science, Space, and Technology." U.S. House. Washington, D.C.: GPO, 27 Apr. 1993: 2-4.

---. Fact Sheet: "Combating Terrorism: Presidential Decision Directive 62." Washington, D.C.: GPO, 22 May 1998.

---. "FY2001 Interagency Research and Development Priorities." *Memorandum for the Heads of executive Departments and Agencies.* Washington, D.C.: GPO, 3 June 1999.

---. "Global Information Infrastructure." *The Global Information Infrastructure-Summary of Drafting Panel Discussion.* Washington, D.C.: GPO, 15 Apr. 1995.

---. Information *Technology Research and Development: Information Technology for the 21st Century.* Washington, D.C.: GPO, 21 Jan. 2000.

---. "President Clinton Names Robert Elliot Kahn to Serve on Information Technology Advisory Committee." Washington, D.C.: GPO, 24 July 1998.

---. *Testimony of The Honorable Neal Lane, Assistant to the President for Science and Technology before the Subcommittee on Science, Technology and Space, Committee on Commerce, Science, and Transportation.* U.S. Senate. Washington, D.C.: GPO, 1 Mar. 2000.

---. "The Global Information Infrastructure." *A White Paper Prepared for the White House Forum on the Role of Science and Technology in Promoting National Security and Global Stability.* Washington, D.C.: GPO, 30 Mar. 1995.

---. Office of the Vice President. *The Vice President's Task Force on Combating Terrorism. Letter from Vice President George Bush accompanying the release of the "Public Report of the Vice President's Task Force on Combating Terrorism.* Washington, D.C.: GPO, Feb. 1986.

---. *Reengineering Through Information Technology-Part 1, Executive Summary. Accompanying Report of the National Performance Review.* Washington, D.C.: GPO, 1 Sept. 1993.

---. *Reengineering Through Information Technology-Part3. Appendix B: Methodology. Accompanying Report of the National Performance Review.* Washington, D.C.: GPO, 1 Sept. 1993.

---. The President's Commission on Critical Infrastructure Protection. *Adequacy of Criminal Law and Procedure (Physical). 8.* Washington, D.C.: GPO, Dec. 1997.

---. *Privacy Laws and the Employer-Employee Relationship: A Legal Foundations Study. 9.* Washington, D.C.: GPO, Dec. 1997.

---. "Critical Foundations: Protecting America's Infrastructures." *The Report of the President's Commission on Critical Infrastructure Protection.* Washington, D.C.: GPO, 13 Oct. 1997.

---. *Information-Sharing Models. Special Study Report.* Washington, D.C.: GPO, 1997.

---. *Legal Foundations: Studies and Conclusions. 1.* Washington, D.C.: GPO, 1997.

---. *Privacy Laws and the Employer-Employee Relations. 9.* Washington, D.C.: GPO, 1997.

---. *Private Intrusion Response. Special Study Report. Washington, D.C.: GPO, 1997.*

---. *Research and Development: Recommendations for Protecting and Assuring Critical National Infrastructures.* Washington, D.C.: GPO, 1997.

---. The President's Working Group on Unlawful Conduct on the Internet. "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." Washington, D.C.: GPO, Mar. 2000.

Wiener, Daniel. Vice President, Unisys. Chair, Information Infrastructure Group (IIG), Industry Executive Subcommittee (IES), NSTAC. Chair, 1999 NDIA Summer Study on Information Assurance. Series of discussions as participant in NDIA Summer Study. July-Oct. 1999.

Wilkinson, Paul. *Terrorism and the Liberal State.* 2nd ed. Washington Square, NY: New York UP, 1986.

Wise, Charles R. "Public Service Configurations and Public Organizations: Public Organizations Design in the Post Privatization Era." *Public Administration Review* 50.152 (Mar./Apr. 1990): 142.

Witton, Richard T. Vice President and General Manager, Information Technologies Division, TRW. Series of private discussions/emails. Feb. 1997-Apr. 2000.

Wolanin, Thomas. *Presidential Advisory Commissions.* Madison: University of Wisconsin Press, 1975.

Yin, Robert K. *Case Study Research: Design Methods.* 2nd ed. Applied Social Research Methods Ser. 5. Thousand Oaks, CA: Sage Publications. 1994.

Zuckerman, M. J. "Hacker Pair Illustrate Pentagon's Vulnerabilities." *USA Today* 23 May 1996: A3.

APPENDIX A:
TOP-LEVEL ANALYSES OF RATIONAL DECISION MAKING MODELING FOR INFORMATION ASSSURANCE

Management decisions ultimately rest upon the issue of choice between alternative ways to allocate resources so as to optimize a result. Rational decision making selects that course of action which maximizes goal satisfaction or which promises to achieve closest to the desired result, given the environmental circumstances. When objective analyses of the decision domain are essential, the intelligence component of the decision process must gather quantitative information about the economic cost of alternative actions, as well as the price of meeting or failing to meet organizational goals.

Such methods allow an investigation of how rational participants in Information Assurance might frame, theorize about, and decide policy issues associated with preserving the critical information infrastructure of the United States against the effects of Strategic Information Warfare (SIW), Information Operations-Attack (IO-A), and related cyber war/terror activities. The of rational decision making is to understand the quantitative aspects of the cognitive elements and thought processes of the protagonists in a situation where opposing sides seek social, political, and economic advantage and leverage by attacking the United States or elements of the Global Information Infrastructure (GII).

Specifically, rational choice modeling requires that value choices be exercised by United States' Information Warfare-Defense (IW-D) forces in determining which elements of America's critical information infrastructure to defend and how best to protect them against attack by implementing any number of risk reduction defensive strategies. Conversely, Information Warfare-Offense (IW-O) forces face their own set of value choices regarding the selection of targets, methods of attack, and cost IW-O forces are willing to bear in order to press a successful offensive operation. Both the IW-D and the IW-O forces have limited resources. The problem for both antagonists is to maximize their respective utility functions, offensive in the case of IW-O terrorists and defensive in the case of the IW-D, while meeting their resource funding constraints.

IW-O cyber terrorists seek to achieve political advantage and leverage by attacking United States global interests and its citizens through denial of service attacks to the population in general, i.e., critical infrastructure attacks, or denial of income producing services to the economy, i.e., attacks on assets vital to United States' economic interests. United States global assets consist of physical plants, communication networks, financial, electrical power distribution systems, roads and highways, railroads, air transport, computer facilities and databases, agricultural and natural resources, water supplies, and other physical, electronic, financial, and symbolic assets. As most of these assets are critically dependent upon

Information Technology, they are also critically vulnerable to Information Technology-based attacks and disruptions.

As a corollary to the improvements in computer processing technology discussed previously, the Information Age has seen rapid advances in computational strategies for rational decision making. These strategies deal with hard tangibles: certainty, logic, and facts, i.e., the quantitative data gathered by the intelligence component of the decision process. In economic applications, these elements are intensely mathematical, or algorithmic, and are generally associated with branches in the fields of Operations Research (OR) and, sometimes, Artificial Intelligence (AI).

Mathematical Programming

The IW-O forces seek to maximize losses imposed on the defense as a result of a successful cyber attack mounted against selected critical information infrastructure targets, while the IW-D forces seek to minimize damage and maximize the survivability of critical infrastructure resources. In a general optimization problem, the forces seek to find extreme values, maxima or minima, of a specific quantity, called the objective, which depends on a finite number of decision variables, representing the choices available to the protagonists. These decision variables may be independent of one another, or they may be related through one or more constraints.

In Operations Research[1], a mathematical program is an optimization problem in which the objective and constraints are given as mathematical functions and functional relationships. The objective, for the n decision variables $(x_1, x_2, ..., x_n)$ is given by

$$L = L(x_1, x_2, ..., x_n)$$

subject to the constraints

$$\left.\begin{matrix} g_1(x_1, x_2, ..., x_n) \\ g_2(x_1, x_2, ..., x_n) \\ \cdots \\ g_m(x_1, x_2, ..., x_n) \end{matrix}\right\} \begin{matrix} \leq \\ = \\ \geq \end{matrix} \left\{\begin{matrix} c_1 \\ c_2 \\ \cdots \\ c_m \end{matrix}\right.$$

Each of the m constraint relationships involves one of the three signs:

$$\leq, =, \text{ or } \geq.$$

Given their financial resources, their asset base, and a level or disposition of expected assaults, the IW-D forces will implement defensive, risk reduction measures to maximize their surviving resources, i.e., to minimize the penalty inflicted by terrorist attacks. In a quantitative sense, risk is the probability that an asset is destroyed or rendered non-functional, given that it has been subjected to a terrorist attack. The purpose of these risk abatement measures is tactical warning of an attack, damage prevention and control, attack assessment, and restoration of service.

For IW-D, the value of the decision variable x_i, with $1 \leq i \leq n$, may be thought of as representing a decision to defend the i^{th} of n assets, i.e., taking $x_i = 1$ if the i^{th} asset is defended and $x_i = 0$ otherwise. However, for

the sake of simplicity, to reduce the number of decision variables, assume that IW-D assets can be grouped in classes, so the loss from a successful attack against each member of an asset-class is the same. Disruption or interruption of service at any major airport, as an example, might produce equal loss to the IW-D side regardless of the airport location. In this case, n denotes the number of asset-classes, and x_i is the number or fraction of defended assets in the i^{th} class.

Given the limitations of their financial resources, the IW-D asset base, and a level/disposition of protective resources, the IW-O cyber terrorists will allocate their offensive resources to maximize their notion of the penalty inflicted on the IW-D economy. In other words, the IW-O terrorists will seek to maximize a variant of the IW-D objective loss.

Linear Programming (LP) Problems

A mathematical program is called linear if the objective $L(x_1, x_2, ..., x_n)$ and each constraint $g_i(x_1, x_2, ..., x_n)$ for $i = 1, ..., m$ are linear in each of their arguments, i.e., if

$$L(x_1, x_2, ..., x_n) = a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_n \cdot x_n = \vec{a} \cdot \vec{x}$$

and

$$g_i(x_1, x_2, ..., x_n) = b_{i1} \cdot x_1 + b_{i2} \cdot x_2 + ... + b_{in} \cdot x_n = \vec{b}_i \cdot \vec{x},$$

where a_j and b_{ij} for $i = 1, ..., m$ and $j = 1, ..., n$ are known constants.

Assume the assets are grouped in n classes. In the IW-D decision problem, let us hypothesize that the defense assumes any undefended assets will be lost in a cyber attack. Let x_j be the fraction of the assets in the j^{th} class for which defenses are provided, so a_j is the total value of assets in the j^{th} class, $a_j \cdot x_j$ is the total value of assets in the j^{th} class surviving after an attack, and the IW-D forces will try to maximize

$$L(x_1, x_2, \ldots, x_n) = a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_n \cdot x_n$$

the total value of resources in all classes surviving the attack. The IW-D decision problem is constrained by the notional requirement that $0 \le x_j \le 1$ and the financial requirement that the total budget, c, available to implement risk abatement measures for IW defense of all classes not be exceeded, i.e.,

$$b_1 \cdot x_1 + b_2 \cdot x_2 + \ldots + b_j \cdot x_j + \ldots + b_n \cdot x_n \le c,$$

where b_j is the cost of defending all the assets in the j^{th} class.

The IW-O decision problem can be given a similar formulation, but the cyber terrorists might hypothesize that all attacked assets are lost and try to maximize the total value of resources succumbing to their attack. The financial constraints would reflect the cost of mounting an IW attack, rather than providing defense. Although functionally equivalent, the IW-D and IW-O forces in general would have their own resource constraints, cost coefficients, and objective coefficients.

Each constraint in the LP problem is a hyper-plane in decision space, and the feasible set of points satisfying these constraints is a bounded solid with vertices or corner points where line segments representing the boundaries intersect. The most important feature characterizing LP problems is that the solution is always found at a vertex. Consequently, we need only look at corner points to find the optimum.

The simplex method for solving LP problems was invented by George Dantzig of Leland Stanford, Junior University in 1947.[2] It searches along the edges of the constraint/visualization solid to find the best answer. Computational implementation involves: (1) finding a feasible solution to start the process; (2) improving this feasible solution by finding the adjacent vertex that yields the largest improvement in the objective, and; (3) repeating Step 2 until there is no longer an adjacent vertex yielding an improvement.

Klee and Minty have constructed worst-case examples where the elementary simplex method does not have polynomial-time complexity but rather requires an exponential number of steps, but such cases seem never to be encountered in practical applications.[3]

In recent years, alternatives to the simplex method have been developed which use projections out from the interior of the feasible region to find he optimal point on the boundary. Commonly known as Karmarkar's algorithm, the interior-point technique is proving especially powerful for the

solution of large-scale linear programming problems, with better performance bounds than the simplex algorithm.[4]

To provide a simple IW example, Figure 1 illustrates the constraint boundaries, cost c and objective L as functions of the decision variables x_1 and x_2 for an IW participant with two asset-classes. This particular graphic is drawn to show the situation when $b_1 > b_2$; symmetric results apply when $b_1 < b_2$, but the x_1 and x_2 axes are interchanged. The structure of the optimal policy has four decision regions.

For Region I, $c \geq b_1 + b_2$, with the optimum at the edge of the constraint square $x_1 = 1$ and $x_2 = 1$, and objective value $L = a_1 + a_2$. For an IW-D problem, the funding completely equips both asset-classes with impenetrable defenses. Conversely, for an IW-O problem, the funding is sufficient to completely subject both asset-classes to irresistible cyber terrorist attack.

In Region II, $b_1 \leq c < b_1 + b_2$, the objective is maximized when one of the two asset-classes is fully funded and the residual is applied to the other asset-class. The objective is maximized at the upper vertex where

$$x_1 = (c - b_2)/b_1 \text{ and } x_2 = 1$$

or at the side where

$$x_1 = 1 \qquad \text{and } x_2 = (c - b_1)/b_2 .$$

By substitution into the objective, it can be shown that the top of the square, the upper vertex, with $x_2 = 1$, is optimal when $a_2 / b_2 > a_1 / b_1$. Otherwise, $x_1 = 1$ is optimal.

In Region III, $b_2 \leq c < b_1$, the objective is maximized when the second asset-class is fully funded, with the residual is applied to the first asset-class, or when the second asset-class is not funded at all and the funds are applied to the first asset-class. The objective is maximized at the upper vertex where

$$x_1 = (c - b_2) / b_1 \text{ and } x_2 = 1$$

or at the bottom vertex where

$$x_1 = c / b_1 \text{ and } x_2 = 0.$$

Again, by substitution into the objective, it can be shown that the top of the square, the upper vertex, with $x_2 = 1$, is optimal when $a_2 / b_2 > a_1 / b_1$. Otherwise, no resources should be spent on the second asset-class. The first asset-class is partially funded in both cases.

In Region IV, $0 \leq c < b_2$, the objective is maximized when the second asset class is partially funded, with nothing applied to the first asset-class, or when the second asset-class is not funded at all and the funds are applied to the first asset-class. The objective is maximized at the left vertex where

$$x_1 = 0 \text{ and } x_2 = c / b_2$$

or at the bottom vertex where

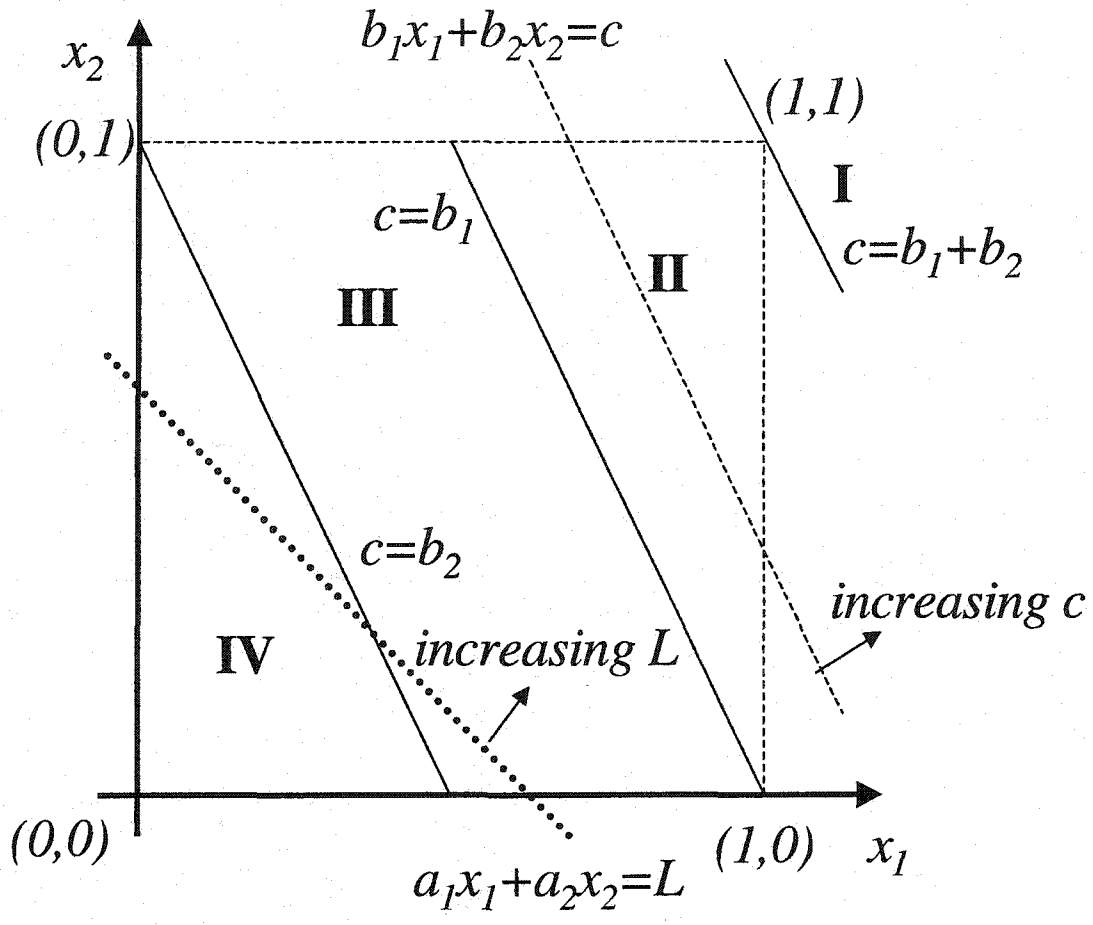


Figure A-1: Linear Programming Decision Space for Two Asset Classes

$$x_1 = c/b_1 \text{ and } x_2 = 0.$$

Again, by substitution into the objective, it can be shown that the left side of the square is optimal when $a_2/b_2 > a_1/b_1$.

Note that a_1/b_1 and a_2/b_2 are figures of merit measuring return per unit cost. Thus, our IW example shows the preferred asset-class is always associated with the most "bang for the buck."

Because IW-D forces assume an attack is inevitable, they have time to deploy at least some risk reduction measures before the IW-O terrorist strike. The IW-O decision depends on how much is known about the IW-D capabilities, strategy, and asset deployment. If the IW-O forces are totally ignorant of the defense, they would assume the assets are not defended by measures sufficient to resist their offense and they would organize their attack accordingly, using the type of analysis shown above.

On the other hand, if the IW-O cyber terrorists were totally knowledgeable of the IW-D defenses, they would only attack undefended assets and/or, to the extent possible, develop technically superior methods of attack to overcome those defenses. In attacking only undefended assets, the IW-O terrorists would simply delete the defended assets from the asset pool and re-optimize their strategy as described above.

A theoretically interesting situation occurs when the IW-O terrorists have partial knowledge of the defensive deployment, i.e., they know that the IW-D assets are only partially defended, but they don't know exactly which assets are defended and their resources will not allow them to attack everything. This leads to a stochastic type problem, where the objective represents the expected return to the IW-O forces from "kills." On the IW-D side, let x_{Di} represent the fraction of the i^{th} asset-class for which defensive measures are provided, so $0 \le x_{Di} \le 1$. On the IW-O side, if x_{Oi} is the fraction of assets in the i^{th} asset-class attacked by terrorists, then the

expected fraction of all assets that are undefended and attacked, and therefore destroyed, is $x_{Oi} \cdot (1 - x_{Di})$. If a_{Oi} is the terrorist gain for the total destruction of the i^{th} asset-class, the expected gain over all asset-classes for the IW-O cyber terrorists is:

$$\overline{L}_D = \sum_{i=1}^{n} x_{Oi} \cdot a_{Oi} \cdot (1 - x_{Di}),$$

where n is again the total number of asset-classes. This is the same LP problem solved previously for the IW-O forces, except that a_{Oi} has been replaced by $a_{Oi} \cdot (1 - x_{Di})$.

Integer Programming (IP) Problems

Integer programming (IP) is the domain of mathematical programming and optimization in which some or all of the decision variables have integer constraints. In formulating the IP problem for IW analyses, the decision variables represent the fraction of the assets in each asset class defended or attacked. In fact, each asset class contains an integer number of assets. An IW-D defender is not allowed to protect a fractional asset, nor can an IW-O terrorist decide to attack a fractional asset. These are all or nothing decisions. The IW decision problem must be reformulated so the n decision variables $(x_1, x_2, ..., x_n)$ can have only integer values. This can be done in one of two ways: we can let the decision variables represent the number of assets in each class defended or attacked, or we can let the decision

variables represent the decision to attack or defend, regardless of asset class.

In the first integer linear programming (ILP) formulation, let x_j be the number of assets in the j^{th} class defended or attacked, so a_j is the unit value of each asset in the j^{th} class. Again, $a_j \cdot x_j$ is the total value of assets in the j^{th} class surviving or destroyed after an attack, and the forces will try to maximize

$$L(x_1, x_2, \ldots, x_n) = a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_n \cdot x_n$$

The total value of resources in all classes surviving or destroyed by the attack. The IW decision problem is constrained by the financial requirement that the total budget c available to implement IW defense or attack measures not be exceeded, i.e.,

$$b_1 \cdot x_1 + b_2 \cdot x_2 + \ldots + b_j \cdot x_j + \ldots + b_n \cdot x_n \leq c,$$

where b_j is the cost of defending or attacking all the assets in the j^{th} class. The decision variables must also be greater than zero and satisfy the additional constraints $0 \leq x_j \leq n_j$, where n_j is the total number of assets in the j^{th} class.

If the LP solution happens to produce integers, then this is the optimal solution to the original problem. Otherwise, the LP solution is only a first approximation. The LP solution can be rounded to the nearest integer values to obtain a second approximation. This is particularly useful when the

number of assets in each asset class is large, but it can prove inaccurate when the numbers are small.

Generic ILP problems, where the LP decision variables are all required to have integer values, are open to two fundamental methods of solution[5]: direct enumeration, including branch and bound algorithms, and the Gomory cutting plane algorithm.

If an LP solution to an ILP problem has non-integer values, say x_i^*, then $j < x_i^* < j+1$ for some positive integer j. Augmenting the original program with the constraint $x_i \leq j$ or the constraint $x_i \geq j+1$ creates two new LP problems. This process is called branching and has the effect of limiting the region of feasible solutions in a way that eliminates the current non-integral solution but still preserves all possible integral solutions to the original problem.

Branching continues until an integral first approximation is obtained. The value of the objective for this first integral solution becomes a bound for the problem. If the objective is to be maximized, all programs whose first approximations yield values of the objective function smaller than this bound are discarded. Branching continues from those solutions having non-integral first approximations that give values of the objective function greater than the lower bound. If a new integral solution is uncovered having a value of the objective function greater than the current lower bound, then this value becomes the new lower bound. Branching continues until there are no

programs with non-integral firs approximation under consideration. At this point, the current lower-bound solution is the optimal solution to the original integer program.

At each stage of branching in the branch and bound algorithm, the current feasible region is cut into two smaller regions by the imposition of two new constraints derived from the first approximation to the original program. The splitting is such that the optimal solution to the current program must show up as the optimal solution to one of the two new programs.

In 1958, R. E. Gomory developed a systematic way of generating implied constraints and a corresponding algorithm.[6] The Gomory cut algorithm operates in essentially like fashion, the only difference being that a single now constraint is added at each stage, whereby the feasible region is diminished without being split. There are no theoretical reasons for choosing between Gomory cut algorithms and branch-and-bound algorithms. The branch and bound algorithm is newer and appears to be favored slightly among practitioners.

The second ILP formulation does not employ the concept of an asset-class. Given a total of n assets, let $x_j = 0$ if the j^{th} asset is not attacked or defended and $x_j = 1$ otherwise. Thus, a_j represents the value of the j^{th} asset, and $a_j \cdot x_j$ is the total value of the j^{th} asset after an attack. The forces will again try to maximize

$$L(x_1, x_2, \ldots, x_n) = a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_n \cdot x_n$$

the total value of resources surviving or destroyed by the attack. The IW decision problem is constrained by the financial requirement that the total budget c available to implement IW defense or attack measures not be exceeded, i.e.,

$$b_1 \cdot x_1 + b_2 \cdot x_2 + \ldots + b_j \cdot x_j + \ldots + b_n \cdot x_n \leq c,$$

where b_j is the cost of defending or attacking all the j^{th} asset. This ILP formulation with 0-1 variables is a special case of the well known "knapsack problem," where a hiker/camper must fit various goods of known utility and weight/volume into a container of limited capacity.

Policy-space concepts from our two asset-class formulation of the LP problem suggest the following approximate solution to ILP problems for IW:

1. Evaluate the maximum possible cost, allowing each decision variable to achieve its maximum value, $x_j = n_j$ for the j^{th} asset-class or $x_j = 1$ for the j^{th} asset. If this maximum cost is within budget, the problem is solved.
2. Otherwise, rank order the assets or asset-classes according to their figures of merit, a_j / b_j, expressing return per unit cost.
3. Allocate resources against the budget giving preference to assets or asset-classes based on their figure of merit until the budget is exhausted.

Models, Simulations, and War Games

A model is a logical description of how a system, process, or component behaves. Modeling is a powerful tool. It is employed to analyze, design, and operate complex systems. Models are used to assess real-world processes too complex to analyze via spreadsheets or flow charts. Models test hypotheses at a fraction of the cost of interacting with the real system. Models may be static or dynamic.

Dynamic modeling, or simulation, is a software representation of the time-based behavior of a system. Static models ignore time dependent variations. While a static model involves a single computation of an equation, dynamic modeling is iterative, using finite difference equations or differential equations to determine system behavior. A dynamic model constantly updates its equations as time changes. The increased computational power and speed of today's computers, coupled with the need for more exact answers, has made dynamic modeling the method of choice.

Dynamic modeling can predict the outcomes of possible courses of action and can account for the effects of randomness. While random events cannot be controlled, dynamic modeling can predict their likelihood and consequences.

Dynamic modeling tools greatly facilitate the model-building process. They range from general purpose to specialized applications and from simulation languages to graphical simulators, where predefined components

are represented by icons, which are inserted into the simulation model and connected via a graphic user interface.

For IW, models are used to estimate the cost benefit and susceptibility to attack of each asset or asset-class. Full-scale economic simulations would cover multiple assets and asset-classes. The cost-benefit data from the simulation are the objective coefficients for each asset or asset-class in LP and ILP problem formulations. These assume the objective is a linear function, first order and additive, of the decision variables. The immediate goal of using models and simulations to support IW analyses is to derive values for objective coefficients. The next step is to look for non-linear characteristics, e.g., quadratic and/or cross terms in the objective; cross terms are significant when destruction of one asset or asset-class element has a deleterious effect on a second asset or asset class element. Finally, non-linear models and simulations are used to evaluate the optimality of solutions derived from linear assumptions.

War gaming is a special form of modeling. The goal of war gaming is to simulate war. James G. Taylor describes a spectrum of wargaming beginning with flesh and blood military exercises, continuing through games involving players and computers, and ending with analytic models.[7] In order of decreasing operational realism and increasing degree of abstraction, convenience, and accessibility, are:

- Military field exercises

- Military field experiments
- Map exercises
- War games
- Computer simulations
- Analytical models.

Thomas B. Allen has explored the historical, political, social, and moral aspects of modern wargaming. Wargaming establishes political-military policy, plans operations, defines contingency procedures, and supports crisis management.[8] Because of the widespread use of wargaming, the DoD Defense Advanced Research Projects Agency (DARPA) created the following formal definitions for some of the terms we have been using:

- *Gaming:* A gaming exercise employs human beings acting as themselves or playing roles in an environment that is either actual or simulated.
- *War gaming:* A war game is defined by the Department of Defense as a simulated military operation involving two or more opposing forces and using rules, data, and procedures designed to depict an actual or hypothetical real-life situation.
- *Simulation:* The representation of a system or organism by another system or model designed to have a relevant behavioral similarity to the original.

- *Model:* A representation of an entity or situation by something else that has the relevant features or properties of the original.

Trevor Dupuy has raised wargaming from an art to a scientific theory of combat by exploring the quantitative aspects of military war games[9]. Modern wargaming is pervaded with Dupuy's ideas, from board games in hobby shops to Pentagon planning games. His Quantified Judgement Model (QJM) formula for the combat power P of a force,

$$P = S \cdot V_f \cdot CEV,$$

is a refinement of Clausewitz's Law of Numbers[10]. Here, S represents force strength, V_f is a composite of operational and environmental factors, and CEV is the combat effectiveness value.

In the Clausewitz concept of battle, the relative combat power of the two forces determines the outcome. The force with the greater combat power usually wins, except for elements of chance or luck, especially the random interactions of hundreds or thousands of troops. Furthermore, absolute accuracy in developing factors to represent the variables affecting the circumstances of a battle is impossible to achieve.

The force strength S takes into account the firepower and mobility of modern weapons, comparing lethality and effectiveness. The measure of weapon effectiveness used by Dupuy is the Operational Lethality Index (OLI). This compares relative weapon lethality in casualties per hour against a theoretical array of unarmored soldiers standing in formation on an infinite

plane surface, each occupying one square meter of space; this theoretical figure is adjusted to account for weapon performance and relative troop density. Once an OLI has been calculated for each weapon, individual weapons values are scaled to account for weapon effect factors and added to provide aggregate scores for units and forces.

In the QJM, circumstantial variables, represented by V_f, are divided into three major groups: environmental (terrain, weather, season), operational (posture, mobility, vulnerability, fatigue, surprise, and air superiority), and the tangible aspects of human behavior (leadership, training, experience, morale, and manpower quality).

Intangible behavioral considerations are combined into a single fudge factor, CEV, representing a relative combat effectiveness value. Dupuy employs CEV to explain the difference between the theoretical outcome and actual outcome of a battle based on the relative power ratios of the opposing forces.

In October 1914, Frederick William Lanchester wrote an article entitled "The Principle of Concentration," in the British journal *Engineering*. That article, offering differential equations for the rate of change of force strength, has had a profound effect on the evolution of a mathematical, scientific theory of combat. Lanchester explained:

> If ... we assume equal individual fighting value, and the combatants otherwise ... on terms of equality, each man will in a given time score, on the average, a certain number of hits that are effective; consequently, the number of men knocked

out per unit time will be directly proportional to the numerical strength of the opposing force. [11]

When the opposing sides know precise locations of targets and can concentrate fire, Lanchester gives the "aimed fire" equations:

$$\frac{dD}{dt} = -c \cdot A$$

$$\frac{dA}{dt} = -C \cdot D,$$

where A and D are the attacking and defending force strengths and dA/dt and dD/dt are the casualty rates of the opposing sides. The condition for equal fractional decrease in numerical strength is:

$$\frac{1}{D} \cdot \frac{dD}{dt} = \frac{1}{A} \cdot \frac{dA}{dt}$$

or

$$c \cdot A^2 = C \cdot D^2,$$

which is Lanchester's square law. Dupuy has modified Lanchester's differential equations to fit the QJM approach. [12]

QJM analysis of more than 200 engagements between 1913 and 1973 reveal patterns establishing ranges for more than forty model parameters to within ±20%. Dupuy notes, "While this is not rigorous precision, it is better than educated guesses, which are probably accurate to within ±100%."[13] Extending Dupuy's analysis to IW wargaming remains a topic for future research.

Impediments to Rational Decision Making

Given implementation of the mathematical programming methods discussed here on a widely available and affordable spreadsheet software program, the primary impediment to rational decision making appears to be lack of quantitative data or the IW case, the lack of the ability by IW forces to formulate policy, rather than algorithmic complexity. Barry Boehm describes the need for financial ways to express goals and constraints. He concludes, however, "that these quantitative methods, although often helpful," ... are..."insufficient for dealing with the critical irreconcilable or unquantifiable goals which often confront us.[14]

Boehm discusses two main problems in coping with such goals: (1) finding techniques for presenting analysis results to decision makers in ways which will enhance their ability to absorb all the factors and to make satisfactory decisions based on the information presented; and, (2) finding techniques for achieving group consensus on decisions involving irreconcilable criteria.

Summary

Rational choice theory and Operation Research tools and techniques offer a wide variety of useful mechanisms for deriving empirical data in support of decision making. While not an exact science, Operations Research provides the decision maker with an approximation of a

mathematically precise choice. As data become more refined, that mathematical precision becomes greater and greater, with a theoretical approximation approaching that of 1.0.

The risk to the decision maker is an over reliance on statistical results that are derived from imperfect data. Given the complexities and uncertainties associated with the SIW problem discussed in this Appendix, it is difficult to reach an absolute conclusion concerning the viability of rational choice approaches to Information Assurance policy decisions. Based upon the sheer number of unknowns associated with such SIW modeling, it was determined that a further pursuit of this line of research would not yield sufficiently qualifiable results to be of empirical use to this research. The rational choice/Operations Research effort was therefore abandoned.

[1] Hamdy A. Taha, "Linear Programming," in *Handbook of Operations Research*, Moder, Joseph J. and Salah E. Elmaghraby, eds.(New York, NY: Van Nostrand Reinhold Co., 1978), 85-119.

[2] G. Danzig, *Linear Programming and Extensions* (Princeton, NJ: Princeton University Press, 1999), 1-648.

[3] V. Klee and G. J. Minty, "How Good is the Simplex Algorithm?", in *Inequalities III*, O. Shisha, ed. (. New York, NY: Academic Press, 1972), 159-175.

[4] Ami Arbel, *Exploring Interior-Point Linear Programming* (Cambridge, MA: MIT Press, 1993), 1-208.

[5] Richard Bronson, "Operations Research," *Shaum's Outline Series in Engineering* (New York, NY: McGraw-Hill Book Company, 1982) 54-69.

[6] R. E. Gomory, "An Algorithm for Integer Solutions to Linear Programs," in *Recent Advances in Mathematical Programming,* Graves, R. L. and P. Wolf, eds. (New York, NY: McGraw-Hill Book Company, 1963), 269-302.

[7] James G. Taylor, "An Introduction to Lanchester-Type Models of Warfare," in *Proceedings of the Workshop on Modeling and Simulation of Land Combat*, L.G. Callahan, ed. (Atlanta, GA: Georgia Institute of Technology Research Institute, 1983), 112-136.

[8] Thomas B. Allen, *War Games-the Secret World of the Creators, Players, and Policy Makers Rehearsing World War III Today* (New York, NY: McGraw-Hill Book Company, 1987), 59-78.

[9] T. N. Dupuy, *Understanding War-History and Theory of Combat* (New York, NY: Paragon House, 1987), 81-89.

[10] Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 1-732.

[11] Frederick William Lanchester, "Mathematics in Warfare," reprinted in Newman, James R., ed., *The World of Mathematics* (New York, NY: Simon and Schuster, 1956), 2138-2157.

[12] Op Cit, 221-235.

[13] Op Cit, 266.

[14] Barry W. Boehm, *Software Engineering Economics* (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1981), 265-277.

Appendix B:
Major 20th Century Initiatives to Improve the United States Federal Government

Dates:	Administration:	Name of Body:	Accomplishment:
1905-1909	Theodore Roosevelt	Keep Commission	Established comprehensive vocabulary of terms and concepts to be applied to public administration
1910-1913	Robert Taft	President's Commission on Economy and Efficiency	Recommended comprehensive changes in human resources, business, and financial management; proposed creating a national executive budget.
1921-1924	Warren Harding	Joint Committee on Reorganization	Established the president as the manager (CEO) of the executive branch.
1936-1937	Franklin Roosevelt	President's Committee on Administrative Management	Established concept of hierarchical executive organization with clear lines of authority and accountability; held that responsibility for policy and standards resided with the president and departmental secretaries.
1947-1949	Harry Truman	First Hoover Commission	Reviewed economy and efficiency of the executive branch; recommended hierarchical administration renewal.
1953-1955	Dwight Eisenhower	Second Hoover Commission	Attempted to reduce the functions of the federal government.
1953-1968	Dwight Eisenhower, John Kennedy, and Lyndon Johnson	Study Commissions on Executive Reorganization	Variety of commissions made recommendations regarding change, policy planning, evaluation, and making departments/ agencies more responsive to the president.
1969-1971	Richard Nixon	Ash Council	Concluded that a fundamental restructuring of the executive branch was needed; recommended that traditional, constituency-oriented departments be replaced by broader, functional departments.

Dates:	Administration:	Name of Body:	Accomplishment:
1977-1979	Jimmy Carter	Carter Reorganization Effort	Rejected most principles of public administration; failed in bottoms-up, process-oriented reorganization
1969-1971	Richard Nixon	Ash Council	Concluded that a fundamental restructuring of the executive branch was needed; recommended that traditional, constituency-oriented departments be replaced by broader, functional departments.
1977-1979	Jimmy Carter	Carter Reorganization Effort	Rejected most principles of public administration; failed in bottoms-up, process-oriented reorganization
1982-1984	Ronald Reagan	Grace Commission	Argued that public-private sectors are alike; should be judged on same set of economic variables and managerial principles; focused on cutting fraud, waste & abuse by government.
1993-2000	William Clinton	National Performance Review (NPR)	Effort to "reinvent government" along entrepreneurial lines (smaller, more agile organizations; empowered staffs); drive decision-making to lowest levels; customer-oriented operations much in a business-centric approach to administration.

Appendix C:
Summary of Relevant Statutes, Executive Orders, Decision Directives, & Circulars

Name:	Issued By:	Date Issued:	Function/Charter:
NSCID No. 9: National Security Council Intelligence Directive No.9	President Harry Truman	24 Oct 1952	Establishes the National Security Agency to collect, process, and disseminate intelligence information from foreign electronic signals for national foreign intelligence/ counterintelligence purposes and to support military operations.
Presidential Memorandum: Establishment of a National Communication System	President John Kennedy	21 Aug 1963	Establishes the National Communication System (NCS), whose mandate includes linking, improving, and extending communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability.
Presidential Directive: Establishment of the Central Security Service	President Richard Nixon	5 May 1972	Creates the Central Security Service (CSS) under the NSA; unified cryptologic effort for all U.S. military; NSA Director serves as Chief of CSS.
PL 92-463: Federal Advisory Committee Act ("FACA"), as amended by **PL 94-409**: Government in the Sunshine Act [Section 5(c)] (5 U.S.C, app. I) and by **PL 105-153**: FACA Amendments of 1997.	92nd Congress of the United States	5 Jan 1973; amended, 12 Mar 1977; amended, 17 Dec 1997	Establishes a Committee Management Secretariat to provide Government-wide oversight of advisory committees; establishes framework covering the creation, management, operation, and termination of all advisory committees reporting to the executive branch; establishes term limits on executive and agency advisory committees to maximum of two years (renewable).

EO 12024: Federal Advisory Committees	President Jimmy Carter	20 Nov 1977	Transfers all functions of the President under the FACA to the Administrator of General Services.
PD 53(PD/NSC-53): National Security Telecommunications Policy	President Ronald Reagan	21 Aug 1981	Establishes roles and responsibilities for secure telecommunications networks in time of war.
EO 12333: Collection of Foreign Intelligence Data	President Ronald Reagan	1 Sep 1981	Authorizes agencies of the intelligence community to collect and produce foreign intelligence and foreign counterintelligence consistent with applicable law.
EO 12382: President's National Security Telecommunications Advisory Committee	President Ronald Reagan	13 Sep 1982	Establishes the National Security Telecommunications Advisory Committee of 30 members to provide technical advice to the president.
EO 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions	President Ronald Reagan	3 April 1984	During national non-wartime emergencies: directs the FCC to investigate violations of pertinent law and regulations and initiation of appropriate enforcement actions; directs the NSC to coordinate planning, policy development, programs and standards for use of telecommunications resources during national emergency; expands NCS from 6 to 23 Fderal Departments/agencies.
NSDD-145: National Policy on Telecommunications and Automated Information Systems Security	President Ronald Reagan	17 Sep 1984	National Security Decision Directive aimed at safeguarding automated information systems with a special focus on protecting those Federal systems accessed via (and dependent on) network communications.

NTISS No.2: National Telecommunications Information Systems and Secuirty Policy Directive No.2	National Security Advisor, Admiral John Poindexter	29 Oct 1986	This directive added a new "sensitive but unclassified" category of Federal information, setting a new criteria of Federal information and the stage for the classification of masses of new data previously deemed unclassified. Poindexter's successor, Frank Carlucci, rescinded NTISS Directive No. 2 on 16 March 1987, following negotiations with the committees having jurisdiction over H.R. 145, which became PL 100-235.
PL 100-235: Computer Security Act of 1987 (40 U.S.C. 759)	100th Congress of the United States	8 Jan 1988	Establishes a computer standards program within the National Bureau of Standards; provides for Government-wide computer security; provides for the training of Federal employees in computer security.
PL 100-503: Computer Matching and Privacy Protection Act of 1988	100th Congress of the United States	18 Oct 1988	Amended title 5 of the United States Code to ensure privacy, integrity, and verification of data for computer matching; establishes Data Integrity Boards within Federal agencies.
PL 102-194: High Performance Computing Act of 1991 (105 U.S.C. 1595)	102nd Congress of the United States	9 Dec 1991	Authorizes $1B, multi-agency research and development program for next generation high performance computers/ network; requires the president to establish an advisory committee to provide advice and information on high-performance computing and communications.
EO 12838: Termination and Limitation of Federal Advisory Committees	President William Clinton	10 Feb 1993	Requires each executive department & agency of the Federal Government to reduce the number of advisory committees

			subject to FACA by minimum of 1/3 by the end of FY 1993; committees will be formed after 1993 only as a result of statute, EO, or OMB approval.
OMB Circular A-130, App. III: Security of Federal Automated Information Resources	Office of Management and Budget (OMB)	25 June 1993	Establishes the policy framework for the management of Federal information resources under auspices of OMB.
PL 103-62: Government Performance and Results Act (GPRA) of 1993	103rd Congress of the United States	3 Aug 1993	Establishes performance metrics and efficiency measures for agency performance of mission and practices.
EO 12864: United States Advisory Council on the National Information Infrastructure	President William Clinton	15 Sep 1993	Establishes within the DOC the United States Advisory Council on the National Information Infrastructure, the purpose of which is to advise SecCom on matters related to the development of the NII, including national security and emergency preparedness.
EO 12881: Establishment of the National Science and Technology Council	President William Clinton	23 Nov 1993	Establishes the National Science and Technology Council chaired by the President of the United States; functions to coordinate the science and technology policy-making process for the United States; to ensure that science and technology policy decisions are consistent with the stated goals of the President; and to ensure that agency science and technology programs and budgets are coordinated and consistent with the President's policies.

EO 12882: Establishment of the President's Committee of Advisors on Science and Technology (PCAST)	President William Clinton	23 Nov 1993	Establishes 18 member Presidential Advisory Committee, 16 of whom are to be "distinguished individuals from the nonfederal sector;" led by the Assistant to the President for Science and Technology; duties are to advise the President through the APST on matters involving science and technology and assist the National Science and Technology Council (NSTC) in securing private sector involvement in its activities.
EO 12924: Declaration of National Emergency Under the International Emergency Economic Powers Act (IEEPA)	President William Clinton	19 Aug 1994	Declares national state of emergency with respect to the lapse of the Export Administration Act of 1979 and the system of controls maintained under that Act; invokes Presidential IEEPA authority to continue functions of EEA under emergency conditions.
EO 12951: Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems	President William Clinton	24 Feb 1995	Directs declassification and public release of Historical Intelligence Imagery from the Corona, Argon, and Lanyard systems; establishes procedure for declassifying future release of national intel imagery.
PDD 39: Counterterrorism Policy	President William Clinton	21 June 1995	Establishes criteria for interagency coordination to prevent and manage the consequence of terrorism in all its forms, including matters related to nuclear, biological, or chemical (NBC) terrorism or threats to the nation's infrastructure.
PL104-13: Paperwork Reduction Act of 1995 (44	104th Congress of the United	1 Oct 1995	Establishes efficiency measures for agencies to

U.S.C. 35)	States		maximize the use/reuse of information collected; minimize public burden for data requested.
EO 12981: Administration of Export Controls	President William Clinton	6 Dec 1995	Establishes DOC as Federal authority to regulate exports; removes authority from State and Defense for export control; provides for formal depart-ment/agency reviews as requested, not to exceed 30 day time window; establishes internal Federal Advisory Committee on Export Policy (ACEP). Establishes Operating Committee with representatives from DOS, DOD, DOC, DOE, and the ACDA to review all export license applications on which reviewing departments or agencies disagree; appeals to ACEP.
PL 104-104:Telecommunica-tions Reform Act of 1996	104th Congress of the United States	8 Feb 1996	First major overhaul of the Nation's telecommunications policy since the Telecommunications Act of 1934; redefined competition and regulation across all sectors of the communications industry.
PL 104-106 (Division E): Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)	104th Congress of the United States	10 Feb 1996	Shifts responsibility for managing all Federal information technology procurement, investment and security from GSA to OMB; ties technology investment and funding to agency operating goals and ROI; establishes CIO position within each agency.

EO 13010: Critical Infrastructure Protection	President William Clinton	15 July 1996	Establishes President's Commission on Critical Infrastructure Protection to examine vulnerabilities in key national infrastructures, such as banking and finance, telecommunications, emergency services, etc.
EO 13011: Federal Information Technology	President William Clinton	17 Jul 1996	Establishes executive branch agency and department Information Technology policy; directs appointment of agency CIOs with agency authority over all IT investments; makes CIOs and agency chiefs responsible for agency IT performance and measurable returns on investment; echoes PL 104-106 assignment of IT responsibility from GSA to OMB.
EO 13020: Amendment to Executive Order 12981	President William Clinton	15 Oct 1996	Establishes reporting requirement by Export Control Operating Committee to departments and agencies of majority voting results on any satellite or hot section jet engine technology export license requests. Departments may appeal OC decisions through the Advisory Committee on Export Policy (ACEP) and on to the SecCom, who has final appeal authority.
EO 13026: Administration of Export Controls on Encryption Products	President William Clinton	15 Nov 1996	Transfers encryption products from the United States Munitions List regulated by DOS to DOC Commerce Control List subject to DOC Export Administration Regulations (EAR). Rescinds provisions of the Export Administration Act (EAA) and EAR relating to availability of

			comparable products of foreign origin; establishes strict export controls on encryption products and software. Amends EO 12981 by establishing formal reviews for DOS, DOD, DOE, DOJ and the ACDA for requests for encryption product export licenses.
EO 13035: President's Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet	President William Clinton	15 Feb 1997	Establishes the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet; Committee to provide technical advice to the president concerning the development and implementation of High-Performance Computing and the NGI.
EO 13062: Further Amendment to EO13010, As Amended, Critical Infrastructure Protection	President William Clinton	29 Sep 1997	Continues the NSTAC and President's Committee on Science and Technology Policy through 30 September 1999. Revokes charter for the United States Advisory Council on the National Information Infrastructure NII).
PDD 62: Combating Terrorism	President William Clinton	22 May 1998	Establishes a wide range of government policies and programs to defeat terrorism; creates National Coordinator for Security, Infrastructure Protection, and Counter terrorism to oversee programs/policies to combat terrorism.

PDD 63: Protecting America's Critical Infrastructure	President William Clinton	22 May 1998	Establishes national goal to eliminate any significant vulnerabilities to critical infrastructures by 2003 through govt/ industry partnership; establishes National Infrastructure Protection Center (NIPC); establishes Critical Information Assurance Office (CIAO).
EO 13092: President's Information Technology Advisory Committee, Amendments to Executive Order 13035	President William Clinton	24 July 1998	Changes the name of the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet to the President's Information Technology Advisory Committee (PITAC); increases membership from 25 to 30.
PL 105-277: Government Paperwork Elimination Act (GPEA), Title XVII.	105th Congress of the United States	21 Oct 1998	Provides for Federal agencies, by 21 October 2003, to provide individuals required to submit or disclose information to the government the right to do so electronically and to use electronic authentication (signature) method to verify the identity of the sender and the authenticity of the electronic content.
PL 105-305: Next Generation Internet Research Act of 1998	105th Congress of the United States	28 Oct 1998	Amends the High-Performance Computing Act of 1991 by authorizing appropriations for FY99-00 for the Next Generation Internet program; requires Advisory Committee on High-Performance Computing and Communications, Information Technology,

			and the Next Generation Internet; President's Information Technology Advisory Committee (PITAC) to monitor and give advice to the president and the Congress over development and implementation of the NGI.
EO 13113: *President's* Information Technology Advisory Committee, Further Amendments to Executive Order 13035, As Amended	President William Clinton	11 Feb 1999	Expands to 26 members the renamed President's Information Technology Advisory Committee (PITAC) in response to PL 102-194.
EO (unnumbered): Further Amendment to Executive Order 12981, As Amended	President William Clinton	31 Mar 1999	Amends EO 12981 by removing the Arms Control and Disarmament Agency from the formal review process for export license for encryption products.
EO 13130: National Infrastructure Assurance Council	President William Clinton	14 July 1999	Establishes National Infrastructure Assurance Council (NIAC) composed of 30 private sector leaders to enhance public-private partnership of critical infrastructure protection; encourage private sector to perform periodic self-risk assessments.
EO 13133: *Working Group* on Unlawful Conduct on the Internet	President William Clinton	6 Aug 1999	Established to (1) determine extent to which current Federal law provides a sufficient basis for investigation and prosecution of Internet-based crime; (2) extent to which new technology/ tools may be required to affect (1); and, (3) potential for new or existing tools to educate/ empower teachers and parents to prevent or minimize risk from unlawful conduct involving use of Internet.

EO 13138: Continuance of Certain Federal Advisory Committees	President William Clinton	30 Sep 1999	Continues until 30 Sep 2001 the PCAST (EO 12882) and NSTAC (EO 12382, as amended). Abolishes PCCIP (EO 13010).
Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue	President William Clinton	7 Jan 2000	Initial release of core Federal plan for strengthening the nation's defense against cyber-threats to public/private sector information systems critical to the nation's economic/social well-being; shifts burden to private sector.

Appendix D:
Federally-Sponsored Commissions and Organizations Having an Information Assurance Focus

Name:	Authority:	Date Created:	Membership/Charter:
President's National Security Telecommunications Advisory Committee (NSTAC)	EO 12382: President's National Security Telecommunications Advisory Committee	13 Sep 1982	35 CEO's of America's leading telecommunications industries appointed by the President to two-year terms. Provides industry-based analyses and recommendations on national security and emergency preparedness telecommunications.
President's Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet	High Performance Computing Act (PL 102-194); EO 13035	9 Dec 1991	25 member technical advisory committee to provide advice and information to the President on high-performance computing and communication and networking.
President's Advisory Council on the National Information Infrastructure	EO 12864: United States Advisory Council on the National Information Infrastructure	15 Sep 1993	25 member private-sector advisory committee selected by SecCom to provide technical advice on establishing the NII.
President's Information Infrastructure Task Force (IITF)	White House Memorandum, President William Clinton	18 Sep 1993	Chaired by SecCom, task force composed of high-level Federal agency representatives to work with Congress and the private sector to accelerate development of a National Information Infrastructure (NII); staff work and administrative support for the IITF provided by DOC's National Telecommunications and Information Administration (NTIA).

National Science and Technology Council	EO 12881: Establishment of the National Science and Technology Council	23 Nov 1993	Chaired by the President and consisting of department and key agency heads and science advisors; role is to coordinate science and technology policy-making across the Federal Government, ensuring that policy decisions and implementations are consistent with President's stated goals.
President's Committee of Advisors on Science and Technology (PCAST)	EO 12882	23 Nov 1993	18 member PCAST created to advise the President on matters involving science and technology, and to assist the National Science and Technology Council in securing private sector involvement in its activities.
Critical Infrastructure Working Group (CIWG)	Presidential Directive	June 1995	Inter-agency working group sponsored by the DOJ and chaired by then Deputy Attorney General Jamie Gorelick; includes representatives from the Defense, Intelligence, and national security communities; identified both physical and cyber threats to the nation's critical infrastructure and recommended the formation of a Presidential Commission (PCCIP) to address these concerns.
President's Commission on Critical Infrastructure Protection (PCCIP)	EO 13010	15 July 1996	PCCIP - Administration focal point for examination of key infrastructure vulnerabilities; recommends ways of addressing them.

Chief Information Officers Council (CIOC)	EO 13011	17 July 1996	CIO Council established as the principal interagency forum to improve agency practices on the design, modernization, use, sharing and performance of agency information resources.
Office of Computer Investigations and Infrastructure Protection (OCIIP)	Directive, FBI Director Louis Freeh	July 1996	In July 1996, the Director of the FBI established the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) as a single point of coordination for all criminal, counterintelligence, and counterterrorism computer intrusion matters and cases involving threats to critical infrastructure. In August 1997, the Director upgraded the status of this coordination function by creating the OCIIP.
Government Information Technology Services Board (GITSB)	EO 13011	17 July 1996	GITSB is responsible for collecting and disseminating information on Information Technologies best practices for the Federal Government.
President's Information Technology Advisory Committee (PITAC)	Next Generation Internet Research Act of 1998 (PL 105-305) EO 13035/EO 13113	15 Feb 1997	Established to provide guidance and advice to the Clinton Administration on all areas of high performance computing
National Infrastructure Protection Center (NIPC)	PDD-63	15 Feb 1998	Based within the FBI; fuses efforts of FBI, DOD, USSS, DOE, DOT, the Intelligence Community, and private sector in joint threat/risk information sharing. NIPC is the principal means of facilitating and

			coordinating a Federal response to an incident, mitigating attacks, investigating threats and affecting reconstitution.
Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism	PDD-62	22 May 1998	Staffed under the NSC, Executive Director of the NIAC. Creates single focal point for Federal activities in combating physical and cyber terror.
Critical Infrastructure Coordination Group (CICG)	PDD-63	22 May 1998	Chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, and made up of sector Liaison Officers and Functional Coordinators of the Federal Lead Agencies, responsible for coordinating the implementation of PDD-63 across government.
Critical Information Assurance Office (CIAO), ex-National Plan Coordination Staff	PDD-63	22 May 1998	Government focal point for the development of a national plan for protecting the nation's critical infrastructure and to coordinate plan implementation efforts.
National Infrastructure Protection Center (NIPC)	PDD-63	Origin: 8 Feb 1998; Expanded: 22 May 1998	PDD-63 authorizes the FBI to expand its fledgling organization to a full-scale national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity, the National Infrastructure Protection Center.
President's Information Technology Advisory Committee (PITAC)	EO 13092 (Amendment to EO 13035)	24 July 1998	Changes the name of the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet to the President's Information Technology Advisory

			Committee (PITAC); increases members from 25 to 30.
National Infrastructure Assurance Council (NIAC)	PDD-63; EO 13130	14 July 1999	Council of up to 30 private-sector executives, appointed by the president to two year terms; purpose of the Council is to enhance partnership between the public and private sectors in protecting the nation's critical infrastructure.
Network Reliability and Interoperability Council (NRIC)	Telecommunications Act of 1996 (47 U.S.C.); also know as the Klinger-Cohen Act	14 July 1999	In AT&T post-divestiture era, advises FCC on best practices to coordinated network and National Services planning by service providers.