THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION SHARING/CRITICAL INFRASTRUCTURE PROTECTION TASK FORCE REPORT

MAY 2000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Following the 22nd meeting of the President's National Security Telecommunications Advisory Committee (NSTAC), the NSTAC's Industry Executive Subcommittee (IES) charged the Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force with the following tasks—

- Develop recommendations leading to significant advances toward the goals of Presidential Decision Directive (PDD) 63[1], including mechanisms and processes for protected, operational information sharing to achieve these goals and for furthering the role of the National Coordinating Center for Telecommunications (NCC) as an Information Sharing and Analysis Center (ISAC) for telecommunications.
- Continue interaction with Government leaders responsible for PDD-63 implementation.

The IS/CIP Task Force examined information that would advance operational information sharing by focusing on the historical and Year 2000 (Y2K) experiences of the NCC, including the experiences of the Government and the NSTAC Network Security Information Exchanges (NSIEs). Additionally, operational and real-time data from industry was harvested from the 16 years of experience with joint industry/Government information sharing in the NCC. The NSIEs provided a rich source of data on industry's network security experiences and its willingness to share those experiences.

Among the lessons learned, the IS/CIP Task Force recognized that the increased level of information sharing that appears to be necessary for CIP will require overcoming operational and perceived impediments. Remedies such as information sharing agreements and exemptions from Freedom of Information Act (FOIA) need to be explored further.

The IS/CIP Task Force addressed PDD-63 goals embodied in the National Plan for Information Systems Protection and the Partnership for Critical Infrastructure Security through a detailed evaluation of the Plan, including the impact of the Plan on industry; an assessment of the value that industry could provide Government; and finally, through meetings with Government officials in which the IS/CIP Task Force provided a clear assessment of industry's added value. Recommendations for several principles for inclusion in the National Plan were also provided to the Government. Information and lessons learned in securing the Public Network from cybercrime and disaster were shared at a variety of meetings that took place across industry sector infrastructures.

[1] Protecting America's Critical Infrastructures: PDD-63

The IS/CIP Task Force paid specific attention to efforts that further positioned the NCC as an ISAC for telecommunications. An analysis of the NCC considered what information is collected, how it is shared, and what the value added is for industry and for Government. The IS/CIP Task Force recognized that the telecommunications industry's long history of supporting national security and emergency preparedness efforts enabled the NCC to be positioned as the first joint industry/Government ISAC partnership. The NCC ISAC function is being developed through a phased approach in which participation, outreach, external relationships, and other issues will be addressed.

NSTAC Recommendation to the President

Recommend that the President support legislation similar to the Y2K Information and Readiness Disclosure Act that would protect CIP information voluntarily shared with the appropriate departments and agencies from disclosure under FOIA and limit liability.

NSTAC Recommendations to the IES for Consideration in the NSTAC XXIV Work Plan

- Continue to observe and collaborate in the development of the NCC ISAC function and make appropriate recommendations.
- Continue outreach efforts to support implementation of PDD-63 related initiatives.
- Continue to actively engage in a dialogue with the Federal Government to provide telecommunications industry input to subsequent versions of the National Plan.

1.0 INTRODUCTION & CHARGE

Following the 22nd meeting of the President's National Security Telecommunications Advisory Committee (NSTAC), the NSTAC's Industry Executive Subcommittee (IES) tasked the Operations Support Group (OSG) to examine lessons learned from the Year 2000 (Y2K) experiences of the National Coordinating Center for Telecommunications (NCC), industry, and other Government entities that interacted with the NCC for application in critical infrastructure protection (CIP). The OSG was also tasked to continue to monitor the NCC in its role as an information sharing and analysis center (ISAC); future enhancements to the NCC; and implementation of the NCC indications, assessment, and warning (IAW) function. In addition, the Information Infrastructure Group (IIG) was tasked, following the NSTAC XXII cycle, to address Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures* industry/Government partnership issues and the National Plan for Information Systems Security.

The Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force was created in September 1999 following a reevaluation of the NSTAC working groups. A majority of the tasks assigned to the OSG and the PDD-63-related tasks assigned to the IIG were assumed by the IS/CIP Task Force and addressed throughout the NSTAC XXIII cycle. The IS/CIP Task Force was charged with the following tasks for the NSTAC XXIII cycle:

- Develop recommendations leading to significant advances toward the goals of PDD-63, including mechanisms and processes for protected, operational information sharing to achieve these goals and for furthering the role of the NCC as an ISAC for telecommunications.
- Continue interaction with Government leaders responsible for PDD-63 implementation.

The IS/CIP Task Force approached its assigned tasks by focusing on three levels of CIP information sharing efforts: telecommunications sector, national, and cross-sector level. IS/CIP Task Force telecommunications sector level efforts focused specifically on examining NCC operational information sharing experiences in the context of NCC implementation of the ISAC function. Through continued outreach to Government officials responsible for implementing PDD-63 initiatives at the national and cross-sector level, the IS/CIP Task Force shared expertise and lessons learned from the NSTAC and the telecommunications industry.

Specifically, at the national level, the IS/CIP Task Force focused its efforts on the National Plan for Information Systems Security (Version 1.0). IS/CIP Task Force outreach efforts at the national level also included dialogue with the Critical Infrastructure Assurance Office (CIAO) and the Chief Information Officer Council's Security, Privacy, and Critical Infrastructure Committee and subcommittees. Providing support to—on an individual company basis—and

monitoring the development of the Partnership for Critical Infrastructure Security was the focus of cross-sector level IS/CIP Task Force efforts.

2.0 RESULTS

2.1 Operational Information Sharing

Through several initiatives, industry and Government continue to work to ensure the security of the Nation's critical infrastructures. Existing information sharing forums such as the NCC and the Government and the NSTAC Network Security Information Exchanges (NSIEs), having evolved over time, are positioned to successfully support CIP efforts. In addition, information sharing initiatives called for in PDD-63 and the National Plan are being established that will further support CIP, including the development of ISACs and the establishment of the National Infrastructure Assurance Council (NIAC). The IS/CIP Task Force, through examination of NCC historical and Y2K-related experiences, developed an understanding of the benefits to participants of information sharing and identified potentially significant barriers to information sharing.

2.1.1 Benefits of Information Sharing

Historically, information sharing has taken place in a trusted environment benefiting the entities involved in the information sharing process. As trust builds, participants in information sharing forums may make more detailed information available. This information is beneficial in helping both industry and Government participants build on lessons learned by others. It is believed that with such information both industry and Government can strengthen security and prevent or mitigate the damage caused by future incidents or attacks. The process may also facilitate information sharing with other critical infrastructures.

Partnering with Government may allow industry to obtain more detailed threat information. Conversely, Government is better able to determine the nature of the threat facing the Nation's critical infrastructures today and in the future through joint industry/Government information sharing initiatives. By combining private sector information about the type of incidents and attacks that are experienced with information obtained through intelligence and law enforcement sources, Government participants may develop warnings and advisories that can also assist other departments and agencies in the Federal, State, and local governments, the critical infrastructures, and security organizations to protect their own systems and respond to incidents.

As Government provides to the private sector indications and warnings and information on specific threats facing the Nation, companies may develop a better understanding of the threats facing their particular infrastructure and may be willing and able to take further action to protect the sector. Access to Government threat-related information through information sharing initiatives may increase the opportunity for the private sector to determine where it will get the "most bang for its security buck."

2.1.2 Historical Experiences

The IS/CIP Task Force examined three questions when considering historical examples of information sharing:

- What information is shared?
- How information is shared?
- What the utility of information sharing is for industry and for Government?

IS/CIP Task Force efforts focused on understanding the context in which information sharing has positioned the NCC to function as an ISAC.

2.1.2.1 National Coordinating Center for Telecommunications

Under the framework of Executive Order 12472, *Assignment of National Security and Emergency Preparedness (NS/EP) Telecommunications Functions,* the NCC, a joint industry/Government body, was established in 1984 to assist the National Communications System (NCS) in accomplishing its mission to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency. The NCC mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities. Information sharing in the NCC has traditionally focused on these areas.

In 1998, the NCC's mission was expanded to include the development of an IAW capability. The NCC conducted a 120-day trial of the IAW Center pilot in 1998. The IAW Center pilot focused on the reporting of "cyber"-related activities that deviated from a company or agency's normal thresholds of operational activity. Following the IAW Center pilot, the NCC decided to fully incorporate the IAW function into its operations.[1]

In June 1999, the NSTAC concluded that the NCC today performs the primary functions of an ISAC for the telecommunications sector as outlined in PDD-63.[2] On January 18, 2000, the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism signed a memorandum agreeing with the conclusion and supporting the decision by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to designate the NCC as an ISAC for telecommunications. The NCC ISAC is one of the first two ISACs to be recognized by the Federal Government.[3] Continuing the telecommunications industry's long

[1] The Operations Support Group Report to NSTAC XXII provides additional information on the IAW Center pilot.
[2] National Security Telecommunications Advisory Committee, Operations Support Group Report to NSTAC XXII, June 1999.
[3] A Financial Services ISAC has also been established; however, participation is limited to the private sector.

history of supporting NS/EP efforts, the NCC ISAC is the first joint industry/Government ISAC partnership. As such, the NCC ISAC is a model to be considered by other infrastructures.

The ISAC function is being developed through a phased approach. The initial phase represents an initial operating capability, which closely mirrors existing NCC operations. Subsequent phases will further address industry and Government participation, sharing agreements, outreach, reporting, and external relationships. NCC relationships with external organizations such as the National Infrastructure Protection Center (NIPC), the Computer Emergency Response Team (CERT) Coordination Center, and the Department of Defense (DOD) Joint Task Force–Computer Network Defense increase the flow of information among industry, Government, and the public sector and should be further examined during implementation of the ISAC function. Efforts are also under way to further develop the relationship between the NCC and the NSIEs to facilitate information sharing among the bodies.

As ISAC activities become more and more defined, participants will have to continue to review NCC ISAC draft policy guidance and procedures to determine the level of participation each is able to commit to the ISAC effort. Through the ISAC function, information will be received and analyzed, and the results sanitized and disseminated. One new tool to facilitate information sharing is the NCC-developed Y2K information sharing and analysis system, which was modified for CIP.[4]

During the initial phase, participation in the ISAC will include existing and pending NCC members.[5] The IS/CIP Task Force agreed with the conclusion made previously by the OSG during the NSTAC XXII cycle that participation in the ISAC should be expanded during subsequent phases to include a broader spectrum of information and communications industry companies. Participation in the ISAC should include providers and operators of wireless services, Internet services, data transmission services, cable services, and providers of database and gateway services to infrastructure operators. The increased level of information sharing that appears to be necessary for CIP will require additional legal protections than those currently available. It appears that initial steps may include a requirement for information sharing agreements and protection of CIP information from disclosure under the Freedom of Information Act (FOIA).

[4] The Y2K system was developed in coordination with the Y2K Telco Forum for collecting and monitoring the status of the telecommunications infrastructure throughout the United States during the Y2K roll-over period.

[5] Existing NCC resident and nonresident members are: AT&T, COMSAT, GTE, ITT Industries, MCI WorldCom, National Telecommunications Alliance, Sprint, and US Telecom Association. Pending NCC members are: Cisco Systems, Computer Sciences Corporation, Electronic Data Systems, Nortel Networks, and Science Applications International Corporation.

2.1.2.2 Network Security Information Exchanges

There are two NSIEs: the NSTAC NSIE and Government NSIE. Although each have separate charters and memberships, they meet jointly about every 2 months to share information. NSIE members are expected to voluntarily share information on—

- new intrusion activities or updates to previously discussed activities,
- vulnerabilities with the potential to result in intrusions or put systems at risk,
- vulnerabilities with the potential to allow authorized users to exceed permission or unintentionally damage a system, its information, or performance,
- significant new malicious code,
- hacker skills, tools, or new methods of attack,
- threats to the public networks,
- security policies, processes, and procedures found to be useful in mitigating significant security risks,
- problems with the potential to affect the availability, confidentiality, or integrity of infrastructure systems, and
- new or ongoing law enforcement cases regarding intrusions into communications and information system networks.

NSIE member organizations sign nondisclosure agreements, and all representatives must have Secret security clearances. The sharing of NSIE information is categorized in three levels: N-1, N-2, and N-3. At Level N-1, information can be shared only with other NSIE representatives. At Level N-2, information can be shared with other individuals within member organizations who have a need to know as determined by their NSIE representative. At Level N-3, information can be shared beyond NSIE member organizations. Although nondisclosure agreements and different levels of information sharing provide members with some protection when sharing information, it is the development of trusted relationships between individuals that allows the sharing of information to take place freely within the NSIEs.

The NSIEs conduct analysis of shared incidents and maintain a database of known network security vulnerabilities. Although the NSIEs primary focus is post-incident sharing and analysis, through the use of e-mail, NSIE members have developed an informal, quasi-"real-time" information sharing capability. NSIE members who experience a "cyber"-related incident (i.e., virus, hacker attack, or security vulnerability) may share their observations and any identified solutions via e-mail on an informal basis as events occur. Such near real-time communication allows industry and Government participants to collaborate to rapidly contain, respond to, and recover from an incident, thus saving response time and human and financial

resources. Future NCC ISAC implementation phases will examine relationships between the NSIEs and the NCC and opportunities for the two bodies to share information.

2.1.3 Year 2000 Information Sharing Experiences

During the Y2K roll-over, the NCC served as a central ISAC for the telecommunications industry and Government. The NCC relied on the efforts of the Y2K Telco Forum, Canadian Telecommunications Industry Forum, International Telecommunication Union, Federal Communications Commission (FCC), General Services Administration (GSA), Defense Information Systems Agency, and multiple divisions of the NCS throughout the year for preparation, coordination, and activation of the NCC Operations Center for Y2K activities. Using its Y2K information sharing system, the NCC was able to provide a mechanism for real-time information sharing.

The Y2K system facilitated information sharing. Eighty-two companies in forty-one countries reported the status of their networks at a minimum of 10 scheduled intervals over the roll-over period. Specific criteria were established by the NCC that companies were required to meet to participate in the Y2K system. The system was designed to meet the needs of a diverse group with varying requirements. Y2K system participants were partitioned into domestic and international sharing groups and granted different levels of database privileges. In addition to industry participants, Government agencies (i.e., GSA, FCC, Department of State, and DoD) participated in the Y2K system. Based on received information, the NCC posted reports every 4 hours on the status of networks domestically and internationally.

The relative success of the NCC Y2K coordination effort was attributed in large part to the trust previously established between industry and Government within the NCC. In addition, the following factors associated with Y2K information sharing were critical to the success of NCC Y2K efforts—

- a universally recognized threat,
- a fixed deadline for mitigating the risk and preparing contingencies,
- highly visible and focused Government leadership,
- compelling business and political reasons for industry participation,
- legislation to protect information and the provider of the information,
- Government-funded centers to support the process,
- a database developed to industry and Government specifications,
- documented information sharing agreements between industry and Government participants, and

- an understanding that the process had a finite life span and that the data would be deleted.

The development of agreements on the exchange of certain proprietary information between each participant and the Office of the Manager, NCS, acting on behalf of itself and the NCC were necessary for the success of Y2K information sharing. The agreements assured participants that recipients of their proprietary information would treat it as such and not disclose it beyond the sharing group. The agreements also provided that proprietary information received by the NCC would be considered a confidential trade secret and commercial or financial information exempt from mandatory agency disclosure under FOIA. In addition, Y2K legislation enacted to protect Y2K information from disclosure under FOIA also enabled the process to be successful.

Y2K provided the NCC with an opportunity to test mechanisms for sharing information among the telecommunications sector in real-time. The experiences and lessons learned will help shape the development of the NCC as it makes the transition to CIP and becomes fully operational as an ISAC for telecommunications. The systems developed and enhancements made to existing NCC resources for Y2K are being adapted to fulfill the ISAC function. The trust built between industry and Government throughout the history of the NCC and further developed in preparation for Y2K sets the foundation for building trust among ISAC participants to facilitate information sharing.

2.1.4 Impediments to Information Sharing

Despite the success of Y2K information sharing efforts and information sharing forums such as the NCC and the NSIEs, several impediments to information sharing may limit the amount and type of information that industry is willing to share. The IS/CIP Task Force identified three categories of impediments to information sharing: perceived, operational, and legal.[6]

2.1.4.1 Perceived Impediments

Y2K information sharing, as noted previously, was successful largely because both industry and Government recognized the threat and faced a fixed deadline by which time action had to be taken. This is not the case with CIP. Industry believes that it understands and is adequately mitigating the threat. Government refers to an increased threat to the critical infrastructures; however, this threat is unclear. Without a clear and present danger, it is difficult for industry to justify spending additional dollars to protect systems that may never be attacked or from threats not identified by industry. Government must make the case in economic terms that an immediate

[6] The NSTAC's Protecting Systems Task Force (PSTF) also examined barriers to information sharing as they related to network security. The PSTF identified technological, cultural, and human factors, and legal and regulatory barriers.

threat to the critical infrastructures exists if it would like industry to share more information than is being shared.

Operational Impediments

Industry shares information using several channels. Providing the same information to multiple entities places demands on corporate resources. By designating one forum as a repository for information related to telecommunications, the demands placed on a company for information sharing should be reduced. As an ISAC for telecommunications, the NCC is positioned to serve as that forum through which industry and Government can share telecommunications IAW information. Optimally, NCC ISAC participants should be able to share information through only one body: the NCC. The NCC, as a coordinating entity, should forward information, in an agreed-on form, to other appropriate bodies (i.e., NIPC, CERT, other ISACs) as permitted under information sharing agreements.

2.1.4.3 Legal Impediments

Over the past year and a half, Congress has shown an interest in developing measures to ensure that the critical infrastructures can be protected under law.

- The Senate Special Committee on the Y2K Technology Problem requested that the General Accounting Office prepare a report on CIP.
- The Senate Armed Services Committee heard testimony from the U.S. Commission on National Security in the 21st Century (Hart-Rudman Commission) regarding the potential for attacks on U.S. information systems.
- The Technology, Terrorism, and Government Information Subcommittee of the Senate Judiciary Committee heard testimony on critical information infrastructure protection.

In addition, several pieces of legislation related to infrastructure protection issues were to be considered by the 106th Congress. Appendix B summarizes proposed legislation for the 106th Congress.

Although Congress is considering CIP-related legislation, legal issues continue to present challenges to CIP information sharing. Foremost among the legal impediments to information sharing is FOIA. FOIA provides the public with access to records maintained by Government departments and agencies. A number of exemptions prevent the disclosure, under FOIA, of specific information; however, none of the exemptions cover CIP information. On behalf of the IS/CIP Task Force, the Legislative and Regulatory Working Group (LRWG) was tasked to examine FOIA as it related to information sharing. Appendix C contains the LRWG background paper prepared for the IS/CIP Task Force on perspectives on FOIA.

In 1997, the President's Commission on Critical Infrastructure Protection recognized the need for voluntary information sharing and identified FOIA as a barrier to information sharing.[7] Congress, at the urging of industry and Government, recognized that FOIA might also be a barrier to voluntary information sharing in preparation for and during the Y2K roll-over. Congress passed the Y2K Information and Readiness Disclosure Act to protect information shared voluntarily with the Government as part of a "special data gathering" request from disclosure under FOIA. PDD-63 calls for long-term voluntary information sharing between industry and Government to achieve CIP. Both PDD-63 and the Y2K experience have raised awareness about the sensitivities of information-sharing processes. Critical infrastructures are being asked to share information for a longer duration and under less defined conditions than previously experienced during Y2K. For PDD-63 information sharing initiatives to be fully implemented, protection of voluntarily shared information from disclosure under FOIA must be provided.

A Critical Infrastructure Information Sharing Drafting Group was convened by the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and the Department of Justice (DOJ) to consider a nondisclosure provision that would protect "security-related" information voluntarily shared with the Government from disclosure under FOIA. The draft nondisclosure provision was an attempt to address concerns of the private sector and to eliminate or reduce the impact an impediment such as FOIA has on information sharing between industry and Government. Through a dialogue with DOJ and CIAO representatives, the IS/CIP Task Force and the LRWG shared concerns about FOIA and the need for legislation to address such concerns.

In addition, concerns about antitrust and liability laws may be a barrier to information sharing, which without a legal remedy, may prevent cooperation.[8] An effort is also under way within DOJ to address such concerns. DOJ has solicited input from the private sector regarding concerns associated with CIP information sharing and antitrust and liability and is working on developing acceptable legal remedies.

Although legal remedies could alleviate some of the concerns associated with FOIA, antitrust, and liability, alleviating potential impediments to information sharing will be more difficult. The IS/CIP Task Force recognizes the proactive actions being taken by DOJ to address FOIA concerns and antitrust and liability issues and welcomes future opportunities to share private sector concerns about legal impediments to information sharing. At the same time that legal remedies are being developed, joint industry/Government efforts should be taken to clarify issues that slow or inhibit the sharing of CIP information. Doing so would require both industry and Government to reconsider traditionally held values, processes, and organizational

[7] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures, 1997.*

[8] The NCC Charter was vetted through the FCC and the Antitrust Division of DOJ to ensure that NCC operations do not violate antitrust laws.

responsibilities. Traditional information sharing entities and channels may need to be reenergized to meet CIP goals as outlined in PDD-63.

2.1.5 Conclusions

The NCC is developing an ISAC function. This function will increase voluntary information sharing beyond that which has traditionally been accomplished in the NCC. Issues such as participation, sharing agreements, reporting procedures, and external relationships will be addressed through the phased implementation of the ISAC function. Further examination of the relationship between the NCC and the NSIEs and the leveraging of relationships with other external entities will promote information sharing within the telecommunications sector and provide benefits to NCC ISAC participants. In addition, electing to share information through the NCC ISAC should be sufficient to ensure that the information will be shared with other Government bodies and ISACs through one body, the NCC.

Overcoming legal, operational, and perceived impediments is a challenge. However, legal and operational remedies must be achieved for increased, widespread information sharing between industry and Government to take place. Experience with the NCC and the NSIEs has shown information sharing to be worthwhile. In addition, the nine factors identified by the IS/CIP Task Force that facilitated Y2K information sharing do not universally apply to CIP. Therefore, in-depth CIP information sharing may not be achieved as rapidly as the Y2K effort was implemented.

2.1.6 NSTAC Recommendation to the President

Recommend that the President support legislation similar to the Y2K Information and Readiness Disclosure Act that would protect CIP information voluntarily shared with the Government from disclosure under FOIA and limit liability.

2.1.7 NSTAC Recommendation to the IES for Consideration in the NSTAC XXIV Work Plan

Continue to observe and collaborate in the development of the NCC ISAC function and make appropriate recommendations.

2.2 PDD-63 Related Initiatives

Throughout the NSTAC XXIII cycle, the IS/CIP Task Force conducted outreach with Government leaders responsible for the implementation of initiatives outlined in PDD-63. IS/CIP Task Force activities focused on both national and cross-sector level CIP-related efforts. Outreach included providing input to the National Plan and sharing experiences and lessons learned with the Partnership.

2.2.1 National Plan for Information Systems Protection

Building on work conducted by the IIG during the NSTAC XXII cycle, the IS/CIP Task Force continued to provide input to the National Plan. Members of the IS/CIP Task Force frequently met with the Director, CIAO, to recommend for inclusion in the National Plan a number of principles identified by the NSTAC. Some of these principles were incorporated into Version 1.0 of the National Plan, which was released on January 7, 2000. In addition, the DOD Infrastructure Assurance Plan, part of the National Plan, specifically mentions the NSTAC as an industry/Government "partnership" model for exchanging information. The NSTAC is also further cited as an example of "industry commitment to ... the public good," and of how industry can partner with Government to improve information security.[9]

Focused on three broad objectives—prepare and prevent, detect and respond, and build strong foundations—10 programs are outlined in the National Plan. Among the 10 programs are two initiatives—the creation of both ISACs and the Partnership—which the IS/CIP Task Force have monitored. The National Plan encourages the private sector and State and local governments to create ISACs. The IS/CIP Task Force and the OSG actively supported the designation of the NCC as an ISAC for the telecommunications sector. The National Plan does not, at this time, specifically address the formation of the NCC ISAC. Appendix D provides the NSTAC recommended input to the National Plan regarding the NCC ISAC.

2.2.2 Partnership for Critical Infrastructure Security

As part of IS/CIP Task Force PDD-63-related outreach efforts, members, representing their individual companies, provided support to the Partnership, a collaborative effort of industry and Government to address risks to the Nation's critical infrastructures and assure the delivery of essential services over those infrastructures.

The Partnership was envisioned to provide a forum for the critical infrastructures to exchange views on interdependencies, threats, work-force development, standards and best practices, technology, research and development (R&D), risk management, international matters, legal and regulatory matters, and other areas of mutual concern. In addition, the Partnership would facilitate industry participation in the National Plan process and provide a vehicle for coordinating industry contribution to the work of the NIAC, which was to be established to advise the President on infrastructure assurance and Partnership issues.

Several NSTAC member companies were represented on the steering group organized to provide advice and help facilitate CIAO efforts to form the Partnership. By leveraging the positive experience of the NSTAC, NSTAC members helped shape this new initiative. NSTAC member

[9] U.S. White House, *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0 An Invitation to Dialogue*, 2000, p. 106.

companies were instrumental in developing the message tailored to areas of importance to industry—fiduciary responsibility and market influences—that eventually became the foundation of the Partnership. In addition, NSTAC member companies worked to increase awareness throughout industry regarding the Partnership.

The initial Partnership event was held at the World Trade Center, New York, on December 8, 1999. Ninety-one attendees representing more than 55 companies and 7 Government organizations joined together to begin a collaborative effort to ensure the delivery of essential services over the Nation's critical infrastructures. Sixteen NSTAC member companies participated. Several pertinent industry points of view were shared with Government, and awareness of network security issues was raised among all eight of the critical infrastructure sectors identified in PDD-63.

Following the initial event, an *ad hoc* organizing committee was formed to accomplish the coordination of a working meeting to discuss further organizational issues and develop a plan of action. Five working groups with membership anticipated from all the sectors have been created.[10] The NSTAC was considered to be a valuable source for attendees from the Information and Communications (I&C) sector and for studies and recommendations developed over its 18-year history.

2.2.3 Conclusions

Outreach in support of PDD-63 implementation efforts is an ongoing activity. The National Plan Version 1.0, subtitled "An Invitation to Dialogue," is considered a work in progress. Subsequent versions of the National Plan should consider both cyberspace and physical security plans for industry and Federal, State, and local governments; defined roles for industry, State, and local government partnerships with the Federal Government; international issues; and personal privacy and civil liberties. Industry should continue to engage in a dialogue with the Government and provide input to subsequent versions of the National Plan.

The Partnership initiative provides a forum for the eight critical infrastructures to potentially share information across sectors and work issues of interest to both industry and Government to ensure the security of the Nation's critical infrastructures. NSTAC member companies may have an opportunity to share expertise, experiences, and lessons learned through the NSTAC with the Partnership to promote information sharing across sectors. Continued support of the Partnership and participation in working groups by individual NSTAC member companies should ensure that the I&C sector is adequately represented.

[10] The five working groups are Interdependency Risk Management and Vulnerability Assessment; Information Sharing, Awareness & Outreach; Legislation and Public Policy Development; R&D and Workforce Development; and, Organization and Public-Private Cooperation Issues.

Efforts by industry and Government departments and agencies to promote outreach and awareness across the critical infrastructures with an emphasis on the I&C sector should be continued to ensure that—

- timely dissemination of physical and cyber information takes place,
- R&D programs are undertaken to develop infrastructure protection tools and techniques to counter emerging cyber threats, and
- technological leadership is provided to safeguard America's critical infrastructures through assessments of NS/EP requirements in the evolving information environment.[11]

2.2.4 NSTAC Recommendations to the IES for Consideration in the NSTAC XXIV Work Plan

- Continue outreach efforts to support implementation of PDD-63 related initiatives.
- Continue to actively engage in a dialogue with the Federal Government to provide telecommunications industry input to subsequent versions of the National Plan.

[11] President William J. Clinton, Letter to Mr. William T. Esrey, July 7, 1995.

APPENDIX A

TASK FORCE MEMBERS AND OTHER CONTRIBUTORS

TASK FORCE MEMBERS

GTE	Mr. Lowell Thomas, Chair
SAIC	Mr. Hank Kluepfel, Vice-Chair
AT&T	Mr. Gordy Bendick
Boeing	Mr. Bob Steele
Cisco Systems	Mr. Ken Watson
COMSAT	Mr. Ernie Wallace
CSC	Mr. Guy Copeland
EDS	Mr. Bob Donahue
ITT	Mr. Joe Gancie
Lockheed Martin	Mr. Michael Collins
Nortel Networks	Dr. Jack Edwards
NTA	Mr. Bob Burns
Raytheon	Mr. Bob Tolhurst
Rockwell	Mr. Ken Kato
TRW	Mr. Bob Lentz
USTA	Mr. Paul Johnson
U S WEST	Mr. Jon Lofstedt

OTHER CONTRIBUTORS

AT&T	Mr. Harry Underhill
COMSAT	Dr. Jack Oslund
CSC	Ms. Sheila Andahazy
GTE	Ms. Ernie Gormsen
Unisys	Dr. Dan Wiener

GOVERNMENT PARTICIPANTS

GSA	Mr. Tom Sellers
NCC	Mr. Bernie Farrell
NTIA	Mr. Bill Belote
NTIA	Mr. Irv Pikus

APPENDIX B

PROPOSED LEGISLATION OF THE 106TH CONGRESS

PROPOSED LEGISLATION OF THE 106TH CONGRESS

The following four sections summarize pending legislation before the 106th Congress. This information is not meant to be a complete list of pending bills; rather, it presents those bills related to the mission of the Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force. Also relevant to the IS/CIP Task Force are various authorization and appropriation bills that reference infrastructure protection, information assurance, and information sharing issues. A majority of those bills were enrolled and sent to the President.

I. INFRASTRUCTURE PROTECTION ISSUES

Although the following bills do not examine CIP issues from a national security and emergency preparedness (NS/EP) perspective, they are useful in providing a gauge with which to measure CIP awareness.

S.1993 Government Information Security Act of 1999
Sponsor*:* Senator Fred Thompson.
Latest Major Action: 11/19/99, referred to the Senate Committee on Governmental Affairs.
Official Title: A bill to reform Government information security by strengthening information security practices throughout the Federal Government.
Further Explanation: Prompted by hearings within the Governmental Affairs Committee, this bill was introduced to protect the integrity, confidentiality, and availability of information on Government computers. The bill builds on the existing information security framework by defining specific roles for Federal agencies. The bill would require that a Government-wide set of information security controls be established under the auspices of the Office of Management and Budget. Such a shift would bifurcate the existing information security system, in which the National Security Agency (NSA) is responsible for securing classified information, and the National Institute of Standards and Technology (NIST) is responsible for securing non-classified information. The bill would also require an annual independent evaluation of agencies' information security practices and mandate that agencies follow best-practices guidelines established by the Government Accounting Office.

H.R.2630 National Telecommunications and Information Administration (NTIA) Reauthorization Act of 1999
Sponsor: Representative Billy Tauzin.
Latest Major Action: 7/29/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection; 7/29/99, forwarded by subcommittee to full committee (amended) by voice vote.
Official Title: To reauthorize the NTIA, and for other purposes.
Further Explanation: (Sec. 8) Authorizes the Secretary [of Commerce], under the Telecommunications and Information Infrastructure Assistance Program, to make grants to

eligible entities to assist in the development of a national telecommunications and information infrastructure. Requires grant funds to be used only for projects to: (1) expand or augment telecommunications networks or information technology systems for health care providers, educational institutions, research facilities, libraries, museums, State and local governments, and other social service and public information providers; (2) enhance the ability of such entities to have access to existing and new sources of information; (3) make universally available and utilize an advanced telecommunications and information infrastructure, especially for traditionally under-served populations; and (4) demonstrate and improve the efficiency and effectiveness of the delivery of social services, such as education and health care, to the American people.

H.R.115 National Infrastructure Development Act of 1999
Sponsor: Representative Rosa DeLauro.
Latest Major Action: 1/6/99, referred to Committees on Transportation and Infrastructure, Banking and Financial Services, and Ways and Means; 2/12/99, referred to House subcommittees.
Official Title: To facilitate efficient investments and financing of infrastructure projects and new job creation through the establishment of a National Infrastructure Development Corporation (NIDC), and for other purposes.
Further Explanation: Establishes as a wholly owned Government corporation: (1) the NIDC, which shall make new sources of financing available (including public benefit bonds) for the development of infrastructure facilities; and (2) the National Infrastructure Insurance Corporation (NIIC), which shall be a subsidiary of NIDC, issuing insurance, reinsurance, and related undertakings with respect to obligations for development of such facilities. Requires NIDC and NIIC to conduct their respective businesses as self-supporting entities.

H.R.866 Critical Infrastructure Communications Act of 1999
Sponsor: Representative Walter Jones, Jr.
Latest Major Action: 3/16/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection.
Official Title: To amend the Communications Act of 1934 to protect critical infrastructure radio systems from interference and to promote efficient spectrum management of the private land mobile radio bands, and for other purposes.
Further Explanation: Directs the Federal Communications Commission (FCC) to adopt rules to ensure the ongoing protection and promotion of radio spectrum used by electric, gas, and water utilities and natural gas and petroleum pipelines against interference from other users of spectrum and consistent with provisions of the Communications Act of 1934.

II. INFORMATION ASSURANCE ISSUES

Computer security and information assurance goes hand in hand. The following three bills address information assurance through either training venues or encryption policy reform. The latter two bills examine computer security and NS/EP implications.

S.1314/H.R.2816 Computer Crime Enforcement Act
Sponsor: Senator Patrick Leahy / Representative Matt Salmon.
Latest Major Action: 7/1/99, referred to Senate Judiciary Committee; 9/17/99, referred to the House Judiciary Committee's Subcommittee on Crime.
Official Title: A bill to establish a grant program to assist State and local law enforcement in deterring, investigating, and prosecuting computer crimes.
Further Explanation: Directs the Office of Justice Programs to make a grant to each State, subject to the availability of appropriations, which shall be used to: (1) assist State and local law enforcement agencies in enforcing State and local criminal laws relating to, and educating the public to prevent and identify, computer crime; (2) assist in educating and training State and local law enforcement officers and prosecutors to conduct investigations and forensic analyses of evidence and prosecutions of computer crime; (3) assist State and local law enforcement officers and prosecutors in acquiring computer and other equipment to conduct investigations and forensic analysis of evidence of computer crimes; and (4) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer crimes with State and local law enforcement officers and prosecutors, including the use of multi-jurisdictional task forces.

H.R.2413 Computer Security Enhancement Act of 1999
Sponsor: Representative James Sensenbrenner, Jr.
Latest Major Action: 10/20/99, forwarded by House Subcommittee on Technology to full Committee on Science.
Official Title: To amend the NIST Act to enhance the ability of the NIST to improve computer security, and for other purposes.
Further Explanation: Amends the NIST Act to require the NIST, in fulfilling its responsibilities under the computer standards program, to: (1) upon request from the private sector, assist in establishing voluntary interoperable standards, guidelines, and associated methods and techniques to facilitate and expedite the establishment of non-Federal public key management infrastructures that can be used to communicate with and conduct transactions with the Federal Government; and (2) provide assistance to Federal agencies in the protection of computer networks, and coordinate Federal response efforts related to unauthorized access to Federal computer systems.

Requires the Institute to perform evaluation and tests of: (1) information technologies to assess security vulnerabilities; and (2) commercially available security products to determine their suitability for use by Federal agencies for protecting sensitive information in computer systems.

(Sec. 8) Revises specified requirements, including authorizing (currently, requiring) the Institute, for the purposes of performing research and conducting studies, to draw upon computer system security guidelines developed by NSA.

(Sec. 9) Amends the Computer Security Act of 1987 to revise requirements regarding Federal computer system security training to require such training to include emphasis on protecting sensitive information in Federal databases and Federal computer sites that are accessible through public networks.

(Sec. 12) Directs the Under Secretary of Commerce for Technology (Under Secretary) to: (1) promote the more widespread use of cryptography applications and associated technologies to enhance the security of the Nation's information infrastructure; (2) establish a central clearinghouse for the collection by the Federal Government and dissemination to the public of information to promote awareness of information security threats; (3) promote the development of the national, standards-based infrastructure needed to support commercial and private uses of encryption technologies for confidentiality and authentication.

H.R.850 Security And Freedom through Encryption (SAFE) Act
Other Titles: Protection of National Security and Public Safety Act; Encryption for the National Interest Act.
Sponsor: Representative Bob Goodlatte.
Latest Major Action: After being reviewed and amended by the House Select Committee on Intelligence and the House Judiciary, Commerce, Armed Service and International Relations Committees and various subcommittees, the bill was labeled as prepared for the House floor on 7/23/99.
Official Title: To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.
Further Explanation: Directs the President to control the export of all dual-use encryption products. Authorizes the President to deny the export of any encryption product on the basis that its export is contrary to U.S. national security interests. Provides that any decision made by the President or his designee regarding the export of encryption products under this Act shall not be subject to judicial review.

III. PRIVACY

Privacy issues sometimes seem contrary to the Administration's policies, especially CIP and NS/EP policies. The following bills have been introduced with the intention of protecting individuals' identities and personal information.

H.R.313 Consumer Internet Privacy Protection Act of 1999
Sponsor: Representative Bruce Vento.
Latest Major Action: 4/12/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection.
Official Title: To regulate the use by interactive computer services of personally identifiable information provided by subscribers to such services.
Further Explanation: Prohibits an interactive computer service from disclosing to a third party any personally identifiable information provided by a subscriber without the subscriber's informed written consent. Permits the subscriber to revoke such consent at any time and requires the service to cease disclosing such information.

H.R.367 Social Security On-line Privacy Protection Act of 1999
Sponsor: Representative Bob Franks.
Latest Major Action: 1/29/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection.
Official Title: To regulate the use by interactive computer services of Social Security account numbers and related personally identifiable information.
Further Explanation: Prohibits an interactive computer service from disclosing to a third party an individual's social security number or related personally identifiable information without the individual's prior informed written consent. Defines interactive computer service as one providing computer access to multiple users via modem or other means of telecommunication to the Internet or any other on-line network. Requires such service to permit an individual to revoke any consent at any time, upon which revocation such service shall cease disclosing such number or information to a third party.

H.R.514 Wireless Privacy Enhancement Act of 1999/Wireless Privacy Bill
Sponsor: Representative Heather Wilson.
Latest Major Action: 3/3/99, referred to Senate Commerce Committee.
Official Title: To amend the Communications Act of 1934 to strengthen and clarify prohibitions on electronic eavesdropping, and for other purposes.
Further Explanation: Amends the Communications Act of 1934 to prohibit modifying any electronic communication device, equipment, or system in a manner that causes it to fail to comply with regulations governing electronic eavesdropping devices.

H.R.1685 Internet Growth and Development Act of 1999
Sponsor: Representative Rick Boucher.
Latest Major Action: 5/25/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection; 5/5/99, referred to House Judiciary Committee, hearings held on 6/30/99.
Official Title: To provide for the recognition of electronic signatures for the conduct of interstate and foreign commerce, to restrict the transmission of certain electronic mail advertisements, to authorize the Federal Trade Commission (FTC) to prescribe rules to protect the privacy of users of commercial Internet sites, to promote the rapid deployment of broadband Internet services, and for other purposes.

IV. OTHER

The following bills address various "hot topics" of the 106th Congress. Some of these bills might prove relevant to analyses undertaken by the National Security Telecommunications Advisory Committee.

S.1125 Telecommunications Merger Review Act of 1999
Sponsor: Senator John McCain.
Latest Major Action: 5/26/99, referred to Senate Commerce Committee.
Official Title: A bill to restrict the authority of the FCC to review mergers and to impose conditions on licenses and other authorizations assigned or transferred in the course of mergers or other transactions subject to review by the Department of Justice or the FTC.

H.R.1686 Internet Freedom Act
Sponsor: Representative Bob Goodlatte.
Latest Major Action: 5/25/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection; 5/5/99, referred to House Judiciary Committee, hearings held on 6/30/99.
Official Title: To ensure that the Internet remains open to fair competition, free from government regulation, and accessible to American consumers.
Further Explanation: Amends the Federal criminal code to provide criminal penalties against anyone who intentionally: (1) and without authorization initiates the transmission of a bulk unsolicited electronic mail message to a protected computer with knowledge that such message falsifies an Internet domain, header information, or other identifier; or (2) sells or distributes any computer program designed primarily to conceal the source or routing information on such mail, has only limited commercially significant purpose or use, or is marketed by the violator or another person acting in concert with the violator with the violator's knowledge of such use.

Provides that inter-LATA services shall not include services that consist of or include the transmission of any data or information by means of the Internet or any other network that

employs Internet Protocol-based or other packet-switched technology. Prohibits a Bell operating company or its affiliate from providing, by the Internet or similar network employing such technology, two-way voice-only inter-LATA telecommunications services originating in any of its in-region States until the FCC approves the application of such company for such State.

H.R.1714 Electronic Signatures in Global and National Commerce Act
Sponsor: Representative Tom Bliley.
Latest Major Action: Passed House, as amended; 11/19/99, referred to Senate Commerce Committee.
Official Title: To facilitate the use of electronic records and signatures in interstate or foreign commerce.
Further Explanation: Title I: Validity of Electronic Records and Signatures for Commerce. Enumerates principles governing the use of electronic signatures in international transactions. (Sec.105) Provides that in any commercial transaction affecting interstate commerce, a contract shall not be denied legal effect or enforceability solely because an electronic signature or record was used in its formation. Sets forth procedural guidelines affecting: (1) electronic signatures and records; (2) electronic record retention; and (3) interaction of electronic agents.

Title II: Development and Adoption of Electronic Signature Products and Services. Directs the Secretary to: (1) report to Congress on the results of an inquiry regarding impediments to commerce in electronic signature products and services; and (2) promote the practice of electronic signatures in interstate and foreign commerce.

Title III: Use of Electronic Records and Signatures Under Federal Securities Law. Amends the Securities Exchange Act of 1934 to reflect the provisions of this Act regarding the use of electronic records and signatures. Authorizes the Securities and Exchange Commission to: (1) prescribe implementing regulations following certain guidelines; (2) require that records be filed in electronic format; and (3) require manual signatures in certain circumstances to deter fraud.

H.CON.RES.182 (House Concurrent Resolution)
Sponsor: Representative Thomas Davis.
Latest Major Action: 10/6/99, referred to House Committee on Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection.
Official Title: Outlining a vision to shape congressional information technology policy into the next century to promote and preserve the successes, leadership, and uniqueness of the United States information technology sector.
Further Explanation: Requires Congress, in addressing issues of information technology and electronic commerce policy, to: (1) focus on a broad spectrum of issues essential to the evolution and strength of the American information technology industry; (2) ensure that it plays an enabling and not inhibiting role in supporting the movement of industry and people into the

Information Age; (3) incorporate a principle of minimal and predictable government regulation; and (4) refrain from actions that would enshrine or favor specific technologies or standards.

APPENDIX C

LEGISLATIVE AND REGULATORY WORKING GROUP

BACKGROUND PAPER: PERSPECTIVES ON THE FREEDOM OF INFORMATION ACT

BACKGROUND PAPER:
PERSPECTIVES ON THE FREEDOM OF INFORMATION ACT (FOIA)[1]

FOIA has been viewed as one of the more visible impediments to information sharing under Presidential Decision Directive (PDD) 63. A Government drafting group comprising representatives of the Department of Justice, Department of Defense, Federal Aviation Administration, U.S. Coast Guard, Security Policy Board, and the Critical Infrastructure Assurance Office was formed to prepare FOIA-related draft legislation to overcome this barrier to information sharing.

In anticipation of this draft legislation, the Legislative and Regulatory Group (LRG) of the President's National Security Telecommunications Advisory Committee (NSTAC) examined various FOIA issues related to PDD-63 information sharing. Following the reorganization of the NSTAC working groups in September 1999, the LRG was renamed the Legislative and Regulatory Working Group (LRWG). The LRWG remains dormant until an individual task force tasks it to advise and provide input on legal and regulatory aspects of current issues being addressed by the NSTAC. The LRWG was tasked by the Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force to complete the FOIA-related work prepared by the LRG. This paper provides the IS/CIP Task Force with general reference information for use in assessing the Administration's proposed FOIA-related legislation.

The LRG *Outage and Intrusion Information Sharing Report* identified several information-sharing forums with which the telecommunications industry shares or will share information (Attachment 1). The report also outlined several barriers to information sharing, including the confidentiality of information. Attachment 2 serves as a supplement to the report, highlighting the presence of nondisclosure agreements and the information-sharing forums' exposure to FOIA and State freedom of information statutes. A separate but related issue is a revision to Office of Management and Budget (OMB) Circular A-110 made pursuant to Public Law 105-277, which requires Federal agencies to ensure that all data produced under a Federal grant or award made to institutions of higher education, hospitals, and non-profit organizations will be made available to the public through procedures established under FOIA. Where appropriate, the potential impact of this revision has been noted.

Attachment 3 provides a partial list of laws and executive orders (E.O.), in addition to FOIA exemptions, that protect national security and emergency preparedness and law enforcement information from disclosure. These authorities can be consulted when draft FOIA legislation is

[1] This background paper was prepared by the LRWG for the IS/CIP Task Force to use as reference material when considering draft provisions to protect voluntarily shared critical infrastructure protection information from disclosure under FOIA. Additional information on FOIA can be found at the following sites: http://www.usdoj.gov/oip/foi-act.htm and http://www.foia.com/foiahelp.html

being evaluated, to prevent the inaccurate identification of shortfalls in the draft legislation. The draft language might intentionally not address items that are already covered by other authorities.

The Year 2000 (Y2K) Information and Readiness Disclosure Act includes language that provides FOIA relief for special Y2K data-gathering requests. Attachment 4 provides the relevant text. The legislation applies to all Federal agencies, entities, and authorities, rather than to a particular agency or department. In addition, the Act identifies specific dates on which provisions within the Act regarding statements and disclosures no longer apply. Other examples of language designed to protect information shared with the Government also exist, such as that contained in House Resolution 2885 (Statistical Efficiency Act of 1999). The IS/CIP Task Force might wish to consider the language used in the Y2K Information and Readiness Disclosure Act as a positive example of FOIA relief that could be applied to information sharing in the PDD-63 context. Other language protecting shared information might also be considered.

Attachment 5 summarizes FOIA. Exemptions that are most relevant to the protection of information shared under the national security and emergency preparedness umbrella are highlighted for emphasis.

General Observations:

From these attachments, some general observations can be made and some related issues identified:

- Individual Government departments and agencies determine whether existing FOIA exemptions (i.e., trade secrets or law enforcement) are applicable for withholding requested information. Decisions will likely be made on a case-by-case basis, depending on the specific information requested and the department or agency responding to the request.
- An information-sharing forum (e.g., Agora[2]) might not be subject to FOIA; however, individual Government departments and agencies (e.g., U.S. Secret Service) participating in the information-sharing forum might be subject to FOIA requests. Will Government departments and agencies that receive information through their participation in an entity not subject to FOIA protect the information from disclosure under FOIA?
- Information-sharing forums that are composed entirely of private sector participants are not subject to FOIA; however, if information is provided to the Government, it may then be subject to FOIA requests. Liability and antitrust issues may present additional barriers to information sharing. For example, the Financial Services Information Sharing and Analysis Center (ISAC) overcame antitrust concerns by

[2] See Attachment 2 for a description of Agora.

selecting the Department of Treasury to serve in an advisory role. Although this action alleviates antitrust concerns, information in the possession of Treasury that has been obtained through the ISAC is subject to FOIA requests. Moreover, despite approaches for overcoming these potential barriers, antitrust and liability issues continue to be concerns of companies involved in information-sharing forums.

- There might be FOIA implications for information that one agency determines to be exempt but that is shared with another agency. Normally, decisions on whether to disclose records are made by the agency that originally created or received the record. However, individual agencies may make decisions without consulting the originating or receiving agency (especially if the document is not properly marked), thereby resulting in one agency releasing records that another agency may try not to release. For example, if the National Infrastructure Protection Center (NIPC) has in its possession a record(s) that is exempt and it shares the record(s) with another Government agency, such as the Department of Commerce, will that agency also consider the record(s) to be exempt from disclosure under FOIA?
- Although companies have FOIA-related concerns, most, if not all, Industry Executive Subcommittee (IES) member companies are participating or are planning to participate in information-sharing forums that are identified in the LRG *Outage and Intrusion Information Sharing Report* and that are subject to FOIA requests. Can comparisons be made between existing information-sharing arrangements and those proposed by PDD-63 that would be useful in assessing the draft FOIA legislation?
- The level of detail of information expected to be shared under the PDD-63 framework is different from the level of detail routinely shared in existing information-sharing forums. Traditionally, most information sharing has dealt with incidents caused by human error, natural events, or physical attacks. As outages caused by unauthorized electronic intrusions increase, companies are being asked to share more detailed information than was previously shared. Possible Government disclosure of detailed information under FOIA, shared under PDD-63 initiatives, raises concerns such as competitive disadvantage, liability, and erosion of customer trust among industry. Information requested by the Government from industry needs to be limited to only that needed to understand the vulnerability and intrusion with as little proprietary information disclosed as possible.
- Although companies may legally discuss information associated with being the victim of a crime, in reality law enforcement usually will instruct a company not to share information, to prevent jeopardizing an ongoing investigation. Law enforcement's presence in an information-sharing forum might not necessarily prevent the sharing of information. However, industry continues to be concerned about the disclosure under FOIA of information shared with law enforcement.

Other Industry Concerns:

In addition to the foregoing general observations regarding FOIA, a number of other issues should be addressed when examining information sharing in a larger context than FOIA. Until convinced of the following, industry might not be comfortable sharing more information than it currently shares in existing information-sharing forums.

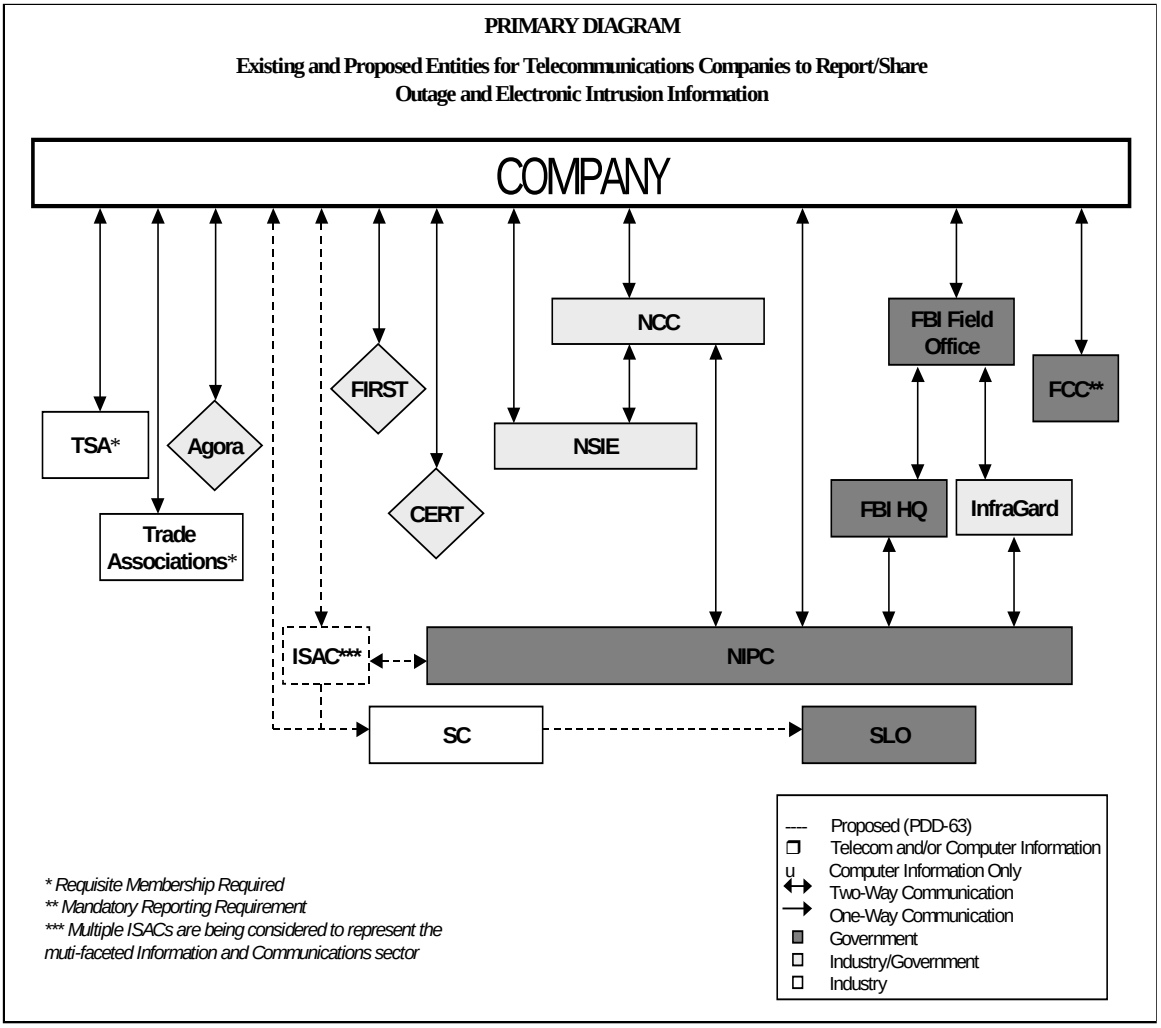
- Information sharing is in the national interest, and it is the right thing for a corporate citizen to do.
- All carriers, or at least the major ones, will participate equally and in good faith.
- The carrier will benefit from participating.
- The benefit will outweigh the cost of participation.
- Information will not be used for competitive advantage.
- Information will be protected and not available to the public.
- Information will not be used by the Government to penalize the provider.
- The carrier will incur no liability for providing inaccurate information.
- Providing the information is not in conflict with law enforcement requirements.[3]

Although outside the scope of FOIA, these are important issues to keep in mind when considering the draft FOIA legislation and the larger context of information sharing.

It is the intent of the LRWG that this document provide the IS/CIP Task Force and IES members with a basis for commenting on the draft FOIA exemption legislation for consideration by the Government. This discussion paper is not intended to serve as a policy paper or to commit any NSTAC member company to a position regarding the draft FOIA legislation. A more targeted analysis of issues related to PDD-63 information-sharing processes would depend on the specific focus and scope of the task force's examination of operational information sharing.

[3] Government and NSTAC Network Security Information Exchange, *The 1999 NSIE Risk Assessment of the Public Network*, April 1999.

ATTACHMENT 1
LEGISLATIVE AND REGULATORY GROUP
OUTAGE AND INTRUSION INFORMATION SHARING REPORT
PRIMARY DIAGRAM



ATTACHMENT 2
OUTAGE AND INTRUSION
INFORMATION SHARING REPORT SUPPLEMENT [4]

NONDISCLOSURE AND FOIA EXPOSURE

- **Agora[5]**

  - Nondisclosure agreement.
  - Not subject to FOIA (not an agency of the executive branch of the Federal Government).
  - Agora membership includes 45 Government agencies (e.g., the Federal Bureau of Investigation, the U.S. Secret Service, and the U.S. Customs Service), which are subject to FOIA. Information shared with these agencies through Agora might be covered by FOIA exemptions (b)(4) or (b)(7).[6] Individual Government agencies would be responsible for determining whether material is exempt.
  - Agora is sponsored by the Regence Group, an affiliate of the Pacific Northwest's largest health plans (Regence Blue Cross Blue Shield of Oregon, Regence BlueShield, Regence BlueShield of Idaho, and Regence BlueCross BlueShield of Utah). It is not federally funded.

- **Computer Emergency Response Team Coordination Center (CERT/CC)**

  - Information specific to a site is kept confidential unless the site gives permission to release that information. Sites reporting incidents are asked to state clearly in CERT's incident reporting form whether CERT is authorized to release information to other sites involved, other computer security incident response teams, or law enforcement.
  - Not subject to FOIA (not an agency of the executive branch of the Federal Government).
  - The revision to OMB Circular A-110 would likely make data collected by CERT/CC subject to FOIA. CERT/CC is part of the Software Engineering Institute, a federally funded research and development center sponsored by the Department of Defense at Carnegie Mellon University.

[4] FOIA applies to records in the Government's possession and not verbal communications. See Attachment E for a summary of FOIA.
[5] Agora is a forum for members to voluntarily and confidentially share sensitive information on computer security issues. Based in Seattle, Washington, it is composed of more than 300 people representing about 100 companies and 45 Government agencies.
[6] (b)(4) applies to information, such as trade secrets and commercial or financial information obtained from a person on a privileged or confidential basis. (b)(7) applies to investigatory records, release of which could constitute an unwarranted invasion of the personal privacy of others, disclose the identity of a confidential source, disclose investigative techniques and procedure, or endanger the life or physical safety of a law enforcement officer.

- **Federal Bureau of Investigation (FBI) / InfraGard**

  – Membership agreements signed between InfraGard members and the FBI outline disclosure terms.
  – Subject to FOIA. Proprietary information is shared with the FBI. Exemption (b)(4) protects this information from disclosure. Unsanitized InfraGard reports become part of law enforcement files, which would be protected from disclosure by exemption (b)(7).

- **Federal Communications Commission (FCC)**

  – Reporting of outage information is required by law.
  – Subject to FOIA.

- **Forum of Incident Response and Security Teams (FIRST)**

  – As part of FIRST's operational framework, all FIRST participants must adhere to the dissemination constraints specified by the originating source. Information that has no specific dissemination instructions cannot be disseminated further. If a member obtains information subject to a nondisclosure agreement, no rights to that information may be assumed by other members.
  – Not subject to FOIA (not an agency of the executive branch of the Federal Government).
  – Individual Government members of FIRST, such as the Department of Energy's Computer Incident Advisory Capability or the U.S. Air Force Computer Emergency Response Team, would be subject to FOIA.

- **Information and Communications Sector Liaison Official (SLO)**

  – Information in the possession of the SLO, an individual designated from the National Telecommunications and Information Administration (NTIA), would be subject to FOIA.

- **Information and Communications Sector Coordinator (SC)**

  – The SC is a private sector representative identified by the SLO to represent the sector and implement PDD-63 initiatives. Information in the possession of the SC would not be subject to FOIA.

- **Information Sharing and Analysis Centers (ISAC)**

  – The question of whether information would be subject to FOIA depends on the nature of the ISAC. If the ISAC is a Government agency, then the information will be subject to FOIA. However, exemptions might apply, such as FOIA exemption (b)(4). If the ISAC

is not a Government agency but receives Federal funding, it might be subject to FOIA disclosure under the revision made to OMB Circular A-110.

- **National Coordinating Center for Telecommunications (NCC)**

  – Memoranda of agreement made with the Secretary of Defense, as Executive Agent for the National Communications System (NCS), or his designee provide the method of participation in the NCC.
  – Subject to FOIA. Proprietary information shared with the NCC would be exempt from FOIA disclosure under FOIA exemption (b)(4).

- **National Infrastructure Protection Center (NIPC)**

  – Subject to FOIA. Exemptions (b)(4) and (b)(7) might cover most if not all information shared with the NIPC.

- **Network Security Information Exchanges (NSIE)**

  – Nondisclosure agreement.
  – Subject to FOIA. Proprietary information shared with the NSIE would be exempt from FOIA disclosure under FOIA exemption (b)(4).

STATE FREEDOM OF INFORMATION STATUTES

With the exception of Agora, no entities identified by the LRG's *Outage and Intrusion Information Sharing Report* are subject to State freedom of information statutes. Individual public agencies (e.g., State or local police departments) in Alaska, Idaho, Oregon, Montana, and Washington that are Agora members might be subject to State freedom of information statutes as follows.

Alaska's Public Record Act (A.S. 09.25.110, *et seq*.) provides that the public records of all public agencies are open to inspection by the public. A number of exemptions limit inspection of particular public records. The most relevant is the exemption regarding records or information compiled for law enforcement purposes. The exemption applies to information that—

- could reasonably be expected to interfere with enforcement proceedings;
- would deprive a person of a right to a fair trial or an impartial adjudication;
- could reasonably be expected to constitute an unwarranted invasion of the personal privacy of a suspect, defendant, victim, or witness;
- could reasonably be expected to disclose the identity of a confidential source;

- would disclose confidential techniques and procedures for law enforcement investigations or prosecutions;
- would disclose guidelines for law enforcement investigations or prosecutions if the disclosure could reasonably be expected to risk circumvention of the law; or
- could reasonably be expected to endanger the life or physical safety of an individual.

Idaho law on evidence and public writings (Idaho Code, Title 9, Chapter 3, sec. 9-337–9-350) exempts from disclosure certain records in the possession of State agencies. Any public record exempt from disclosure by Federal or State law or Federal regulation to the extent specifically provided for by such a law or regulation is exempt. In addition, investigatory records of a law enforcement agency are exempt from disclosure.[7] Trade secrets, including those contained in response to public agency requests for proposal, clarification, information, and similar requests, are exempt from disclosure.[8]

Montana Code 2-6-102 provides public citizens with the right to inspect and copy public writings of the State. Library and burial records are the only exceptions called out in that section. However, Montana Code 44-5-303 does limit the dissemination of confidential criminal justice information.[9] Dissemination of confidential criminal justice information is restricted to criminal justice agencies, to those authorized by law to receive it, and to those authorized to receive it by a district court upon a written finding that the demands of individual privacy do not clearly exceed the merits of public disclosure.

Oregon's Public Record Act also provides for public inspection of public records held by public agencies. Particular public records are exempt from disclosure under ORS 192.410–192.505. These records include trade secrets and investigatory information compiled for criminal law purposes.[10] Investigatory information compiled for criminal law purposes can be exempt from disclosure if there is a clear need to delay disclosure in the course of a specific investigation,

[7] Investigatory records are defined as information with respect to an identifiable person, group of persons, or entities compiled by a public agency pursuant to its statutory authority in the course of investigating a specific act, omission, failure to act, or other conduct over which the public agency has regulatory or law enforcement authority.

[8] A trade secret refers to information, formula, pattern, compilation, program, computer program, device, method, technique, process, or unpublished or in progress research that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

[9] Confidential criminal justice information means criminal investigative information, criminal intelligence information, fingerprints and photographs, criminal justice information or records made confidential by law, and any other criminal justice information not clearly defined as public criminal justice information.

[10] Trade secrets in this context may include but are not limited to any formula, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information that is not patented, that is known only to certain individuals in an organization and that is used in a business it conducts, having actual or potential commercial value, and that gives its user an opportunity to obtain a business advantage over competitors who do not know or use it.

including the need to protect the complaining party or the victim. Exempt from disclosure are those records pertaining to specific operational plans in connection with an anticipated threat to individual or public safety for deployment and use of personnel and equipment, prepared and used by a law enforcement agency, if public disclosure thereof would endanger the life or physical safety of a citizen or law enforcement officer or jeopardize the law enforcement activity involved.

Washington's Public Records Act provides the public with access to public records. A number of exemptions apply, limiting disclosure of information. Specific intelligence information and investigative records, compiled by investigative, law enforcement, and penology agencies, and state agencies vested with the responsibility to discipline members of any profession, the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy, are exempt. Once an investigation is complete, the records can be made available. Specific records of completed investigations can be withheld if their disclosure would jeopardize witnesses or discourage potential sources of information from coming forward in the future.

SUMMARY MATRIX

The following matrix summarizes information highlighted in the previous sections. Under the FOIA column, the reference to exemptions refers to those exemptions specified in FOIA and discussed above, where appropriate, under each organization, such as exemption (b)(4) and (b)(7).

Organization	Voluntary or Required	FOIA	State Freedom of Information Statutes
AGORA	Voluntary	N	Y (public agencies)
CERT	Voluntary	N	N
FCC	Required	Y	N
FIRST	Voluntary	N	N
NCC	Voluntary	Y (exemptions)	N
NSIE	Voluntary	Y (exemptions)	N
Associations	Voluntary	N	N
PDD-63 Entities:			
ISAC	Voluntary	Y*	N
I&C SLO	Voluntary	Y	N
I&C SC	Voluntary	N	N
InfraGard	Voluntary	Y (exemptions)	N
NIPC	Voluntary	Y (exemptions)	N

* If an ISAC is a Government agency, then it is subject to FOIA.

ATTACHMENT 3
LAWS AND EXECUTIVE ORDERS (E.O.) PROTECTING NATIONAL SECURITY AND EMERGENCY PREPAREDNESS AND LAW ENFORCEMENT INFORMATION

The following is a partial list of the laws and E.O.s protecting NS/EP and law enforcement.[11]

Code of Federal Regulations–Title 47 Chapter 1 Part 0 Subpart C
47CFRO.459 provides that any person submitting information or materials to the FCC may submit a request that such information not be made routinely available for public inspection. Each request must be accompanied by a statement explaining the reasons for withholding the materials from inspection.

Executive Order 12958–National Security Information
E.O. 12958 prescribes a uniform system for classifying, declassifying, and safeguarding national security information. Information cannot be classified under E.O. 12958 unless its disclosure reasonably could be expected to cause damage to national security.[12] Information to be considered for classification includes—

- military plans, weapons systems, or operations;
- the vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security;
- foreign government information;
- intelligence activities, intelligence sources or methods, or cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to national security; and
- United States Government programs for safeguarding nuclear materials or facilities.

In addition, information that has not been disclosed previously to the public may be classified or reclassified after an agency has received a request for it under FOIA or the Privacy Act of 1974 if such classification meets the requirements of E.O. 12958 and is accomplished personally and on a document-by-document basis by the agency head, deputy agency head, senior agency official designated to direct and administer an agency's information security program, or an official with original Top Secret classification authority.

[11]This document presents some of the more relevant laws/executive orders related to disclosure of information and national security/law enforcement. It is not intended to include all laws related to privacy or disclosure of information.
[12] Information means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or under the control of the United States Government.

Computer Fraud & Abuse Act
The Computer Fraud & Abuse Act makes unauthorized computer access a Federal criminal offense. Among other things, the Act makes it an offense subject to a fine and/or imprisonment to obtain, via unauthorized computer access, any information that has been determined by the Government pursuant to an E.O. or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations. In addition, obtaining information from any department or agency or any protected computer is considered an offense subject to a fine and/or imprisonment if the conduct involved an interstate or foreign communication.

Economic Espionage Act of 1996
The Economic Espionage Act of 1996 makes the theft of trade secrets a Federal criminal offense. The Act specifically makes it a Federal criminal act for any person to convert a trade secret to the economic benefit of anyone other than the owner, intending or knowing that the offense will injure any owner of the trade secret.[13] Persons and organizations violating the Act are subject to a fine and/or imprisonment. In addition, property is subject to forfeiture.

Uniform Trade Secrets Act (UTSA)
UTSA was drafted by the National Conference of Commissioners on Uniform State Laws (amended 1985) in an effort to make protection of trade secrets uniform throughout the States. UTSA covers the misappropriation or acquisition of trade secrets through other improper means, including theft, bribery, breach of duty to maintain secrecy, or espionage (electronic or other). UTSA calls for injunctive relief and damages for persons or organizations in violation. Forty states have adopted various statutes modeled after UTSA.

Privacy Act of 1974
The Privacy Act of 1974 provides that no agency shall disclose any record that is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains.

[13] Trade secret is defined as all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if the owner thereof has taken reasonable measures to keep such information secret, and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public. (This definition is built upon the trade secret definition used in UTSA.)

ATTACHMENT 4
Y2K INFORMATION AND READINESS DISCLOSURE ACT
FOIA-RELATED PROVISION[14]

Public Law 105-271

Section 4. Protection for Y2K Statements.
(f) Special Data Gathering.

(1) In general. – A Federal entity, agency, or authority may expressly designate a request for the voluntary provision of information relating to Y2K processing, including Y2K statements, as a special Y2K data gathering request made pursuant to this subsection.

(2) Specifics. – A special Y2K data gathering request made under this subsection shall specify a Federal entity, agency, or authority, or with its consent, another public or private entity, agency, or authority, to gather responses to the request.

(3) Protections. – Except with the express consent or permission of the provider of information described in paragraph (1), any Y2K statements or other such information provided by a party in response to a special Y2K data gathering request made under this subsection—

(A) shall be exempt from disclosure under subsection (b)(4) of section 552 of title 5, United States Code, commonly known as the "Freedom of Information Act";

(B) shall not be disclosed to any third party; and

(C) may not be used by any Federal entity, agency, or authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law.

(4) Exceptions. –

(A) Information obtained elsewhere. – Nothing in this subsection shall preclude a Federal entity, agency, or authority, or any third party, from separately obtaining the information submitted in response to a request under this subsection through the use of independent legal authorities, and using such separately obtained information in any action.

(B) Voluntary disclosure. – A restriction on use or disclosure of information under this subsection shall not apply to any information disclosed to the public with the express consent of the party responding to a special Y2K data gathering request or disclosed by such party separately from a response to a special Y2K data gathering request.

[14] The full text of the Y2K Information and Readiness Disclosure Act can be found at http://www.itpolicy.gsa.gov/mks/yr2000/hill/s2392es.htm

ATTACHMENT 5
SUMMARY OF FOIA[15]

Enacted in 1966, FOIA established for the first time an effective statutory right of access to Government information.[16] FOIA applies to "records" maintained by "agencies" within the executive branch of the Federal Government, including the Executive Office of the President and independent regulatory agencies. Agency records are considered to be documents that are either created or obtained by an agency and that are under agency control at the time of the FOIA request. Records maintained by State governments, municipal corporations, the courts, Congress, or private citizens are not included in the scope of FOIA.

Each Federal agency is required to publish in the *Federal Register* its procedural regulations governing access to its records under FOIA. These regulations inform the public of where and how to address requests; schedule of fees for search, review, and duplication; fee waiver criteria; and administrative appeal procedures.

An FOIA request can be made by "any person," a term that encompasses individuals (including foreign citizens), partnerships, corporations, associations, and foreign or domestic governments. FOIA requests can be made for any reason whatsoever, with no showing of relevancy required. In addition, FOIA specifies only two requirements for access requests: that they "reasonably describe" the records sought and that they be made in accordance with each agency's published procedural regulations.

Once an agency is in receipt of a proper FOIA request, it must inform the requester of its decision to grant or deny access to the requested records within 20 working days. The time period for processing requests may be extended. In addition, when an agency locates records responsive to an FOIA request, it should determine whether any of those records, or information contained in those records, originated with another agency or component. Any agency receiving such a request should consult with the component or agency whose information appears in responsive records. When entire records originating with another agency or component are located, those records ordinarily should be referred to their originating agency for its direct response to the requester, and the requester should be advised of such a referral.

Using the following nine exemptions, disclosure under FOIA can be prevented, as long as the information is—

1. (A) specifically authorized under criteria established by an E.O. to be kept secret in the interest of national defense or foreign policy and (B) is in fact properly classified pursuant to such E.O.;

[15] Material extracted from http://www.usdoj.gov/oip/introduc.htm and http://www.usdoj.gov/oip/procereq.htm
[16] Congress enacted both the Freedom of Information Reform Act of 1986 and the Electronic Freedom of Information Act Amendments of 1996, which amended FOIA.

2. related solely to the internal personnel rules and practice of an agency;
3. specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
4. trade secrets and commercial or financial information obtained from a person and privileged or confidential;
5. inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
6. personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
7. records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information
(A) could reasonably be expected to interfere with enforcement proceeding,
(B) would deprive a person of a right to a fair trial or an impartial adjudication,
(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
(D) could reasonably be expected to disclose the identity of a confidential source including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,
(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, if such disclosure could reasonably be expected to risk circumvention of the law, or
(F) could reasonably be expected to endanger the life or physical safety of any individual;
8. contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation of supervision of financial institutions; or
9. geological and geophysical information and data, including maps, concerning wells. Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.

Once these nine exemptions have been applied, FOIA requires that "any reasonably segregable portion of a record" must be released. A decision to deny an initial request must inform the requester of the reasons for denial, of the right to appeal, and of the name and title of each person responsible for the denial. Agencies also must include administrative appeal notifications in all of their "no record" responses to FOIA requesters. An administrative appeal decision upholding

a denial must inform the requester of the reasons for denial, of the requester's right to judicial review in the federal courts, and of the name and title of each person responsible for the appeal denial.

It is useful to note a number of miscellaneous FOIA characteristics. Agencies are not required to create records to respond to FOIA requests. Nor are agencies required to answer questions posed as FOIA requests. Providing exempt information to a requester and limiting his ability to further disclose it through a protective order is not authorized under FOIA. There is also no damage remedy available to FOIA requesters for nondisclosure.

ATTACHMENT 6
LEGISLATIVE AND REGULATORY WORKING GROUP MEMBERS

COMSAT	Dr. Jack Oslund, Chair
ITT	Mr. Joe Gancie, Vice-Chair
AT&T	Mr. Gordy Bendick
Cisco Systems	Mr. Jim Massa
CSC	Mr. Guy Copeland
GTE	Mr. Lowell Thomas
Hughes	Ms. Jennifer Smolker
Lockheed Martin	Mr. Mike Collins
NTA	Mr. Bob Burns
Rockwell	Mr. Ken Kato
SAIC	Mr. Hank Kluepfel
Unisys	Mr. Dan Wiener
USTA	Mr. Paul Johnson
U S WEST	Mr. Jon Lofstedt

OTHER CONTRIBUTORS

AT&T	Mr. Harry Underhill
COMSAT	Mr. Ernie Wallace
GTE	Ms. Ernie Gormsen

APPENDIX D

NSTAC RECOMMENDED INPUT TO THE NATIONAL PLAN

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE RECOMMENDED INPUT TO THE NATIONAL PLAN

The following text is recommended for inclusion in subsequent versions of the National Plan. The text addresses the designation and implementation of the National Coordinating Center for Telecommunications as an Information Sharing and Analysis Center for telecommunications.

National Coordinating Center for Telecommunications

In response to a National Security Telecommunications Advisory Committee (NSTAC) recommendation, the National Coordinating Center for Telecommunications (NCC) was established and began operations on January 1, 1984, as a joint industry/Government National Coordinating Center capable of assisting in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness (NS/EP) telecommunications services and facilities under all conditions of crisis or emergency. Subsequent to beginning operations, the NCC was formalized on April 3, 1984, when President Reagan signed Executive Order 12472, *Assignment of NS/EP Telecommunications Functions.*

This joint industry/Government center facilitates information sharing between industry and Government through the following functions as identified in the industry/Government approved Charter:

- promptly provide technical analysis and damage assessment of service disruptions and identify necessary restoration actions,
- coordinate/direct prompt restoration of telecommunications services in support of NS/EP needs,
- develop and exercise comprehensive service restoration plans,
- develop watch center type functions to work through cooperating industry operation centers to effectively monitor the status of essential telecommunications facilities,
- maintain access to an accurate inventory of the minimum essential equipment, personnel, and other resources that are available for restoration operations, including the location and capabilities of all industry's network operations centers,
- identify liaison points in each company,

- maintain ability to rapidly transfer operations from normal to emergency operations,
- coordinate/direct and expedite the initiation of NS/EP telecommunications services,
- contribute to the development of technical standards and national network planning and ensure application of those standards and dissemination of those plans to facilities serving NS/EP needs, and
- coordinate/direct network reconfiguration plans in support of NS/EP needs.

The NCC's role in fulfilling its charter functions began to evolve in the changing environment following the end of the Cold War and as the Administration determined that national security includes economic security. In 1996, the NCC began to develop an indications, assessment, and warning (IAW) capability. The NSTAC concluded that the IAW capability was within the scope of the NCC Charter, and in 1998 directed the NCC conduct an IAW pilot project. Lessons learned from the pilot project were incorporated into the NCC's ongoing operations.

Following the issuance of Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures*, in May 1998, the NSTAC concluded that the NCC performs the primary functions of an Information Sharing and Analysis Center (ISAC) in the context of PDD-63. The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism agreed in a memorandum dated January 18, 2000.

The NCC is unique as an ISAC. It is a joint industry/Government organization located in the Office of the Manager, National Communications System and staffed by both industry and Government. Information sharing between industry and Government has been taking place in a trusted environment over the past 16 years in the NCC. A phased implementation plan, developed by both industry and Government, will address expanded participation, NCC activities, and external coordination to achieve full operating capability.

APPENDIX E

ACRONYM LIST

ACRONYM LIST

CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Protection
CERT	Computer Emergency Response Team
DOD	Department of Defense
DOJ	Department of Justice
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FIRST	Forum of Incident Response and Security Teams
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
GSA	General Services Administration
I&C	Information and Communications
IAW	Indications, Assessment, and Warning
IES	Industry Executive Subcommittee
IIG	
ISAC	Information Sharing and Analysis Center
IS/CIP	Information Sharing and Critical Infrastructure Protection
LRG	Legislative and Regulatory Group
LRWG	Legislative and Regulatory Working Group
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NIAC	National Infrastructure Assurance Council
NIDC	National Infrastructure Development Corporation
NIIC	National Infrastructure Insurance Corporation
NIPC	National Infrastructure Protection Center
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration

OMB	Office of Management and Budget
OSG	Operations Support Group
PDD	Presidential Decision Directive
PSTF	Protecting Systems Task Force
R&D	Research and Development
SC	Sector Coordinator
SLO	Sector Liaison Official
UTSA	Uniform Trade Secrets Act
Y2K	Year 2000