THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

LEGISLATIVE AND REGULATORY GROUP
Telecommunications Outage and Intrusion Information Sharing Report

JUNE 1999

TELECOMMUNICATIONS OUTAGE AND INTRUSION INFORMATION SHARING REPORT TABLE OF CONTENTS

EXECUTIVE SUMMARY

At its November 3, 1998, meeting the President's National Security Telecommunications Advisory Committee's (NSTAC) Legislative and Regulatory Group (LRG) agreed to develop the Telecommunications Outage and Intrusion Information Sharing Report to address existing and proposed channels companies use to share outage and intrusion information with public and/or private organizations, Government departments and agencies, and other entities.

The report is intended to provide the Industry Executive Subcommittee (IES) with a clearer understanding of information sharing initiatives, including those channels proposed by Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures*. The report includes a compendium of entities with which companies share or will potentially share information. The list of entities was developed based on the entities known or identified by the LRG members and is not presented as a comprehensive list of all those with which all telecommunications companies share information. The entities examined, in alphabetical order, are as follows:

- **Agora.** Agora is a Seattle, Washington, based forum for the sharing of information related to improving computer security through countering computer intrusions and apprehending computer criminals. Agora brings together computer professionals from approximately 100 companies and law enforcement and State and Federal government officials from 45 agencies from five Pacific northwest states and Canada. Members voluntarily share information through formal and informal means.

- **Computer Emergency Response Team (CERT) Coordination Center.** CERT Coordination Center collects information on computer security vulnerabilities and incidents. Reports are voluntarily shared with CERT by incident response teams or the general public. CERT helps companies, other organizations, and individuals who report vulnerabilities solve their problems. CERT will not share vulnerability information publicly until a vendor has developed a "fix" for the problem. CERT protects the identity of the individual or entity reporting vulnerabilities or incidents.

- **Federal Bureau of Investigation (FBI).** Under a number of Federal statutes, the FBI investigates computer-related crimes that are reported through local FBI Field Offices.[1] Companies voluntarily report incidents to the FBI. In an effort to facilitate the sharing of information, the FBI developed the National InfraGard Program in Cleveland, Ohio. While in its developmental stages, this program encourages private sector members in a local area to voluntarily report actual or attempted unauthorized intrusions, disruptions, and vulnerabilities to information systems. This information is

[1] Under the Federal provisions of the Computer Fraud and Abuse Act of 1986, the FBI shares jurisdiction for computer crime with the U.S. Secret Service.

shared with other InfraGard members in sanitized formats in an effort to further strengthen the security of the Nation's critical infrastructures.

- **Federal Communications Commission (FCC).** Telecommunications carriers are required by Title 47 of the *Code of Federal Regulations* to report outage information to the FCC if more than 30,000 customers are affected. Of all the entities examined in this document this is the only one with a mandatory reporting requirement. Reports to the FCC are available to the public. Companies also have an opportunity through the FCC's Network Reliability and Interoperability Council to voluntarily share additional information with the FCC.

- **Forum of Incident Response and Security Teams (FIRST).** FIRST is composed of individual incident response teams from educational, commercial, Government, law enforcement, and military organizations from around the world. FIRST has more than 60 members who voluntarily work together to handle computer security problems. Members share alert and advisory information and security tools and techniques.

- **Information and Communications Sector Liaison Official (SLO)/Sector Coordinator (SC).** As envisioned by PDD-63, an information and communications SLO(s) and a SC(s) will be appointed to represent each critical infrastructure in developing a public-private partnership to eliminate vulnerabilities in the critical infrastructures. The Department of Commerce's National Telecommunications and Information Administration (NTIA) has been designated the SLO for the information and communications sector. The Sector Coordinator for the information and communications sector will be a consortium of three trade associations, including the Information Technology Association of America (ITAA), the Telecommunications Industry Association (TIA), and United States Telephone Association (USTA).

- **Information Sharing and Analysis Center (ISAC).** ISAC is proposed by PDD-63 to be a private sector entity designed to facilitate the sharing of vulnerability, threat, intrusion, and anomaly information for the critical infrastructures. The concept is in its developmental stages; however, it is possible that one or multiple ISACs may be created. The ISACs would collect and analyze information for dissemination to industry and Government departments and agencies as appropriate. The National Coordinating Center for Telecommunications (NCC), which today performs functions similar to those proposed by PDD-63 for an ISAC, is being considered to serve as an ISAC for telecommunications. Additional ISAC's may be considered for the information and communications sector.

- **National Coordinating Center for Telecommunications.** Both the telecommunications companies and Government departments and agencies are represented in the NCS' NCC. Representatives share information on telecommunications outages and electronic intrusions affecting telecommunications critical to national security and emergency preparedness. Companies that report information to the NCC have final approval of the content that is shared with other members.

- **National Infrastructure Protection Center (NIPC).** The NIPC's mission is to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and cyber, that threaten the critical infrastructures. It is designed to be an interagency center with representatives from many Government departments/agencies and the private sector. The NIPC is developing contacts with other Government departments and agencies to build relationships for sharing information. Companies share information through their local FBI Field Office, which forwards the information to the NIPC, or with the NIPC directly.

- **Network Security Information Exchanges (NSIE).** There are two NSIEs, an NSTAC NSIE and a Government NSIE. Each has a separate charter and membership, but they meet jointly to share information on threats, incidents, and vulnerabilities affecting the public network. Members have established trusting relationships and the signing of a nondisclosure agreement further makes the sharing of information easier.

In addition, information sharing within trade associations is examined. Descriptions of several associations are included in the report as examples.

The report also addresses potential legal barriers that might affect the sharing of information between telecommunications companies and the entities examined. The LRG used the legal impediments identified by the President's Commission on Critical Infrastructure Protection (PCCIP) in their report, *Critical Foundations: Protecting America's Infrastructures* to explain some of the legal barriers that may influence the amount or type of information that is shared by companies. The LRG did not conduct any original legal analysis of these impediments for this report.

In conclusion, the LRG observed that information sharing—

- occurs in a number of forums,
- may be affected by legal barriers,
- is mostly voluntary,
- is dependent on receiving a benefit when voluntarily shared,
- is based on trusted relationships,

- may be dependent on the company and individual participant, and
- is content-focused.

The Telecommunications Outage and Intrusion Information Sharing Report is intended for use by other NSTAC subgroups to continue addressing critical information sharing processes and issues as they unfold. In addition, further analysis and understanding of the lessons learned by the entities examined in this report could provide the foundation for determining best practices for information sharing at the National level and could be beneficial to those entities responsible for implementing PDD-63.

1.0 INTRODUCTION

The President's National Security Telecommunications Advisory Committee's (NSTAC) Legislative and Regulatory Group (LRG) agreed at its November 3, 1998, meeting to develop a report addressing the existing and proposed channels that telecommunications companies use to share outage and intrusion information. The Telecommunications Outage and Intrusion Information Sharing Report is intended for use by other NSTAC subgroups to continue addressing critical information sharing processes and issues as they unfold. In addition, further analysis and understanding of the lessons learned by the entities examined in this report could provide the foundation for determining best practices for information sharing at the National level and could be beneficial to those entities responsible for implementing Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures*.

The report includes a compendium that describes in detail the various entities, both industry and Government, with which companies share information on outage and electronic intrusions affecting both private and public networks. For this study, an intrusion is defined as unauthorized access to, and/or activity in, an information system.[1] It is recognized that in some incidents, an outage may be the intended or unintended result of an intrusion; conversely, an outage may be interpreted as being related to an intrusion, when it is not. Given this distinction, this report largely addresses the voluntary sharing of information on intrusions and outages attributed to intrusions rather than accidental outage information. Existing channels of information sharing are examined, as well as those proposed by PDD-63. Listed alphabetically to avoid any indication of prioritization, the entities examined are as follows:

- Agora,
- Computer Emergency Response Team (CERT) Coordination Center,
- Federal Bureau of Investigation (FBI),
- Federal Communications Commission (FCC),
- Forum of Incident Response and Security Teams (FIRST),
- Information and Communications Sector Liaison Official (SLO)/Sector Coordinator (SC),

[1] The President's National Security Telecommunications Advisory Committee Network Group Intrusion Detection Subgroup, *Report on the National Security and Emergency Preparedness Implications of Intrusion Detection Technology Research and Development*, December 1997, p. 6.

- Information Sharing and Analysis Centers (ISAC),
- National Coordinating Center for Telecommunications (NCC),
- National Infrastructure Protection Center (NIPC), and
- Network Security Information Exchanges (NSIE).

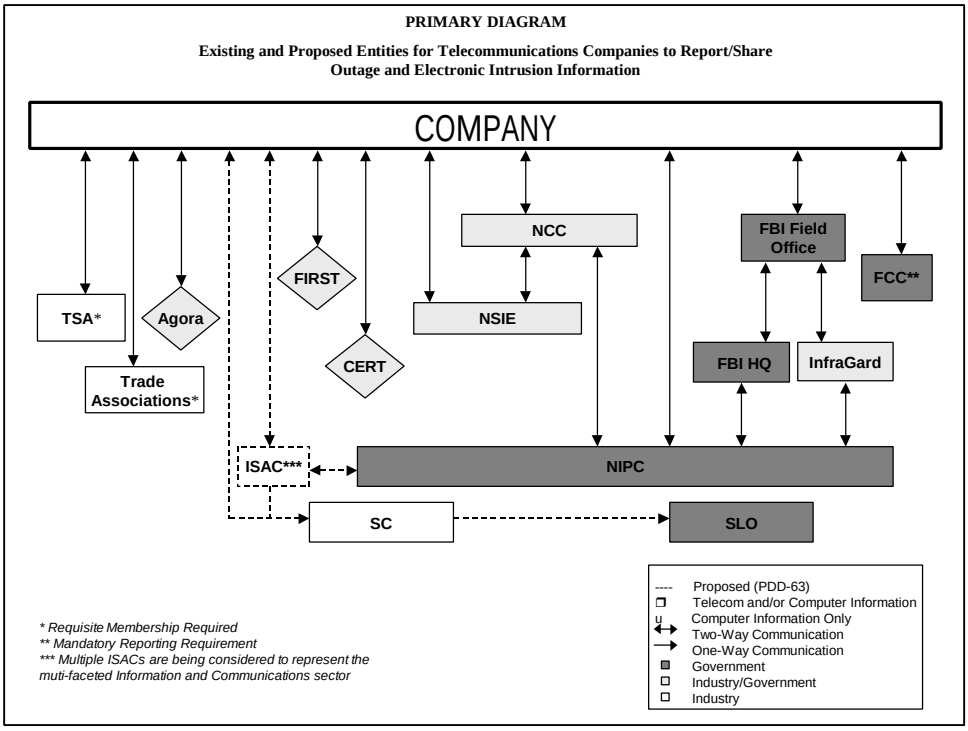
For each of the foregoing entities, individual diagrams are presented to depict where information is shared. In addition, the Telecommunications Security Association (TSA) is examined as an example of information sharing within trade associations.

The compendium describes, for each organization with which companies share information, the type of information being shared (i.e., outage versus intrusion), the sources of information, the force driving the sharing of information (i.e., voluntary versus regulated reporting), the direction in which information is flowing (i.e., one-way or multidirectional), the availability of the information, and the medium used to transmit and share information. As the primary diagram (Section 2.0) illustrates, in most cases the information sharing is intended to be reciprocal.

Although there are many reasons that companies are hesitant to share information, this report focuses on the potential legal barriers to sharing information between companies and various organizations. The legal barriers addressed are those identified by the President's Commission on Critical Infrastructure Protection (PCCIP) Report, *Critical Foundations: Protecting America's Infrastructures*, including confidential information, trade secrets and proprietary information, classified information, national security, antitrust, liability, and State government liability and disclosure. Discussion of the legal barriers includes no original legal analysis by the LRG, and it is not intended to validate or dispute the findings of the PCCIP.

In addition to making a number of general observations about information sharing, this report is intended to generate further analysis and discussion by other NSTAC subgroups, if appropriate, regarding the channels for information sharing that have been depicted in the compendium.

2.0 PRIMARY DIAGRAM



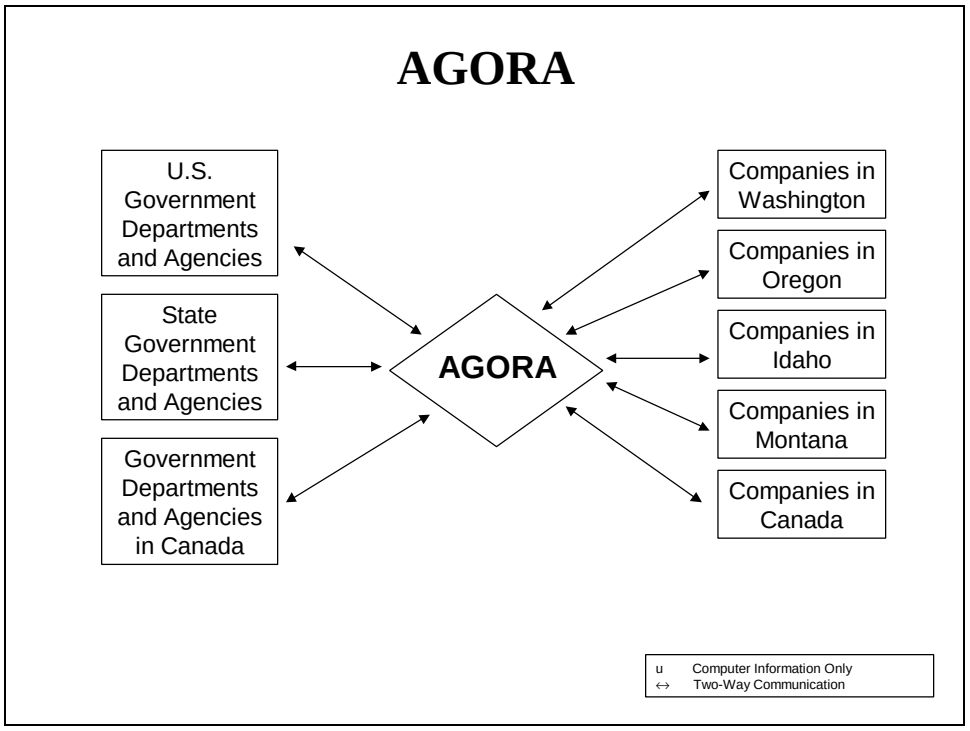
The primary diagram shows the existing and proposed channels that telecommunications companies use to share or report outage and electronic intrusion information. The diagram summarizes the path of communications between a company and the entity with which it shares information. In addition, the diagram shows how the entities described in this report share information with one another. The compendium (Section 3.0) and individual diagrams further break down the information sharing channels to include other entities with which the receiving entity shares company-provided information.

3.0 COMPENDIUM OF ORGANIZATIONS

The organizations included in this compendium were derived through discussion among LRG members.[2] The compendium may not include all the organizations with which all telecommunications companies share information.[3] The organizations are listed alphabetically to avoid any indication of prioritization.

Individual diagrams of each organization depict if telecommunications and computer information or only computer information is shared. The diagrams also depict with whom else the entity shares information. The compendium and individual diagrams, in many cases, do not address what internal action is taken by a Government agency, department or other entity once the information is shared with them.

3.1 Agora



[2] LRG members are representatives from AT&T, COMSAT, CSC, GTE, Hughes, ITT, Lockheed Martin, MCI WorldCom, Nortel, NTA, SAIC, Unisys, and USTA.

[3] Information sharing that is required under contracts with Government departments and agencies is not addressed in this study.

Agora was founded in October 1995 by the Regence Group[4] as a "virtual" forum for members to voluntarily and confidentially share sensitive information on computer security issues. Based in Seattle, Washington, Agora does not have an office or staff. Financial support for Agora is provided primarily through the Regence Group. In addition, members of Agora provide staff support.

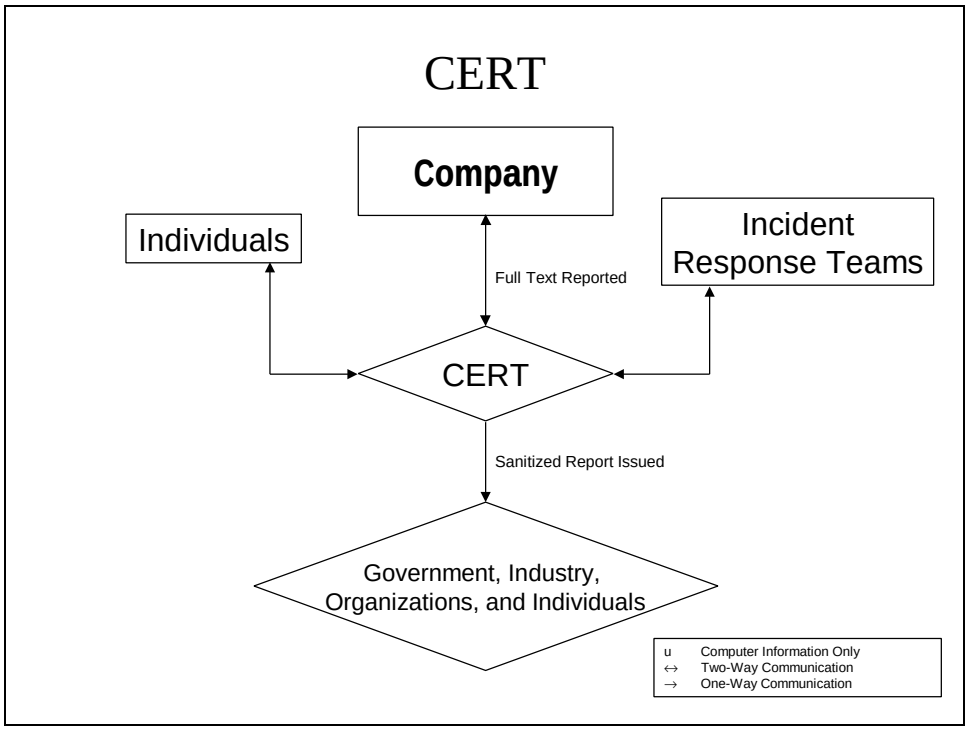
Agora is composed of more than 300 people from approximately 100 companies and 45 Government agencies, including Microsoft, Blue Shield, the FBI, U.S. Secret Service, and U.S. Customs Service agents, and the Royal Canadian Mounted Police as well as local police, county prosecutors, and computer professionals from Washington, Oregon, Idaho, Alaska, and Montana.

Members share information on common computer security problems, best practices to counter them, protecting electronic infrastructures, and educational opportunities. Strategies and new methods for countering and apprehending computer criminals are shared among members. Members also have conducted intrusion testing against one another to further share security information.

Trusted relationships among members facilitate the sharing of information, particularly among private companies who are competitors. In addition, the local scope of Agora has facilitated the building of relationships that make the sharing of information more successful. Members sign nondisclosure agreements before discussing information related to the intricacies of their respective computer security systems. Members share information through meetings and via public and private communications lines, both formally and informally.

[4] The Regence Group is a holding company based in Portland, Washington with subsidiaries that include Regence Blue Shield and the Blue Cross/Blue Shields of Washington, Oregon, Idaho, and Utah.

3.2 Computer Emergency Response Team (CERT) Coordination Center



The CERT Coordination Center is part of the Software Engineering Institute, a federally funded research and development (R&D) center at Carnegie Mellon University in Pittsburgh, Pennsylvania. CERT was established in 1988 in response to the Robert Morris Internet worm incident. CERT studies computer security vulnerabilities, provides incident response services, publishes a variety of security alerts, and researches security and survivability issues. The Coordination Center has helped establish other CERTs worldwide.

CERT receives reports on the following:

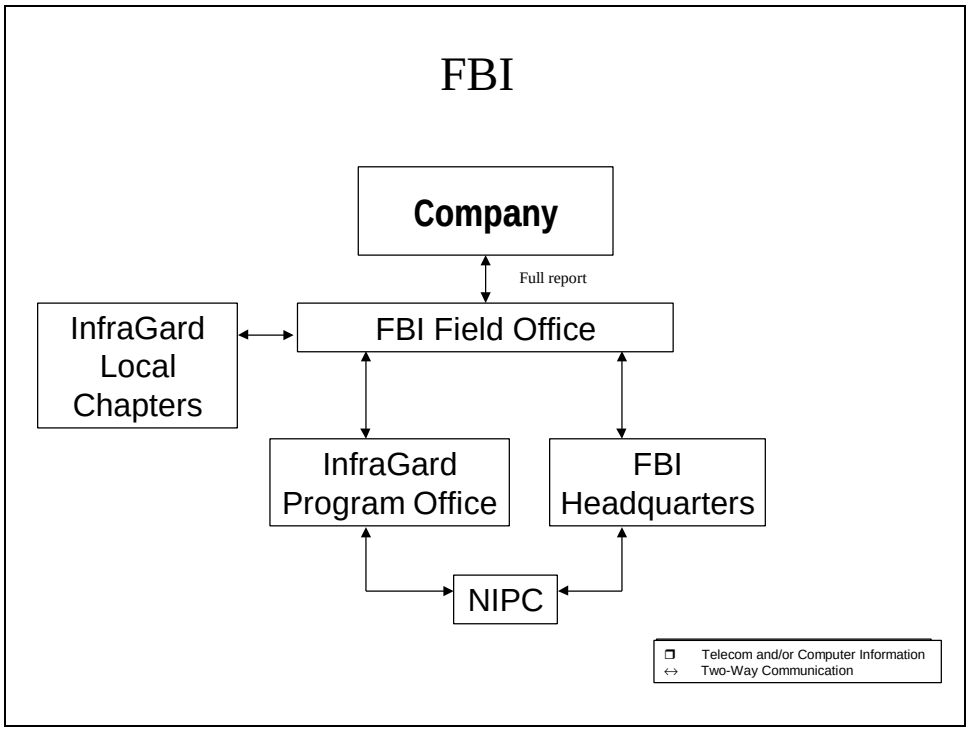
- attempts to gain unauthorized access to a system or its data,
- unwanted disruption or denial of service,
- the unauthorized use of a system for the processing or storage of data, and
- changes to system hardware, firmware, or software characteristics without the owners' knowledge, instruction, or consent.

Reports are made voluntarily by incident response teams or the general public.[5] CERT staff assist computer system administrators who report security problems to help them identify and correct the vulnerabilities that permitted the incident to occur. CERT analyzes vulnerability reports and works with technology producers to inform them of security deficiencies in their products. CERT also tracks producers' efforts to correct the problems. Incident analysis is conducted to determine whether repeated incidents point to a vulnerability. CERT has a proven ability to keep identities and sensitive information confidential and has built a level of trust that has made it a primary center for reporting vulnerability information. CERT works closely with vendors and will not disclose any vulnerability information unless a fix or workaround is available.

Reports are made to CERT via hotline, electronic mail (e-mail), encrypted mail (e.g., Pretty Good Privacy [PGP] and Data Encryption Standard [DES]), or Secure Telephone Unit [STU]-III. CERT issues advisories offering explanations of the problem, information to detect whether a site has a problem, fixes or workarounds, and vendor information. Advisories are shared with a mailing list and posted on the CERT Web site, anonymous File Transfer Protocol (FTP), and USENET newsgroup. CERT vendor-initiated bulletins containing verbatim text from vendors describing vulnerabilities and their fixes also are distributed via mailing list, Web site, anonymous FTP, and USENET newsgroup. Further, "incident notes" and "vulnerability notes" are published that describe current intrusion activities and system weaknesses. These documents are available on the Web at http://www.cert.org/.

[5] An incident response team is a group of people with the technical expertise necessary to help a defined set of users, sites, networks, or organizations with computer security incidents. In addition, it provides a forum for reporting such incidents.

3.3 Federal Bureau of Investigation (FBI)



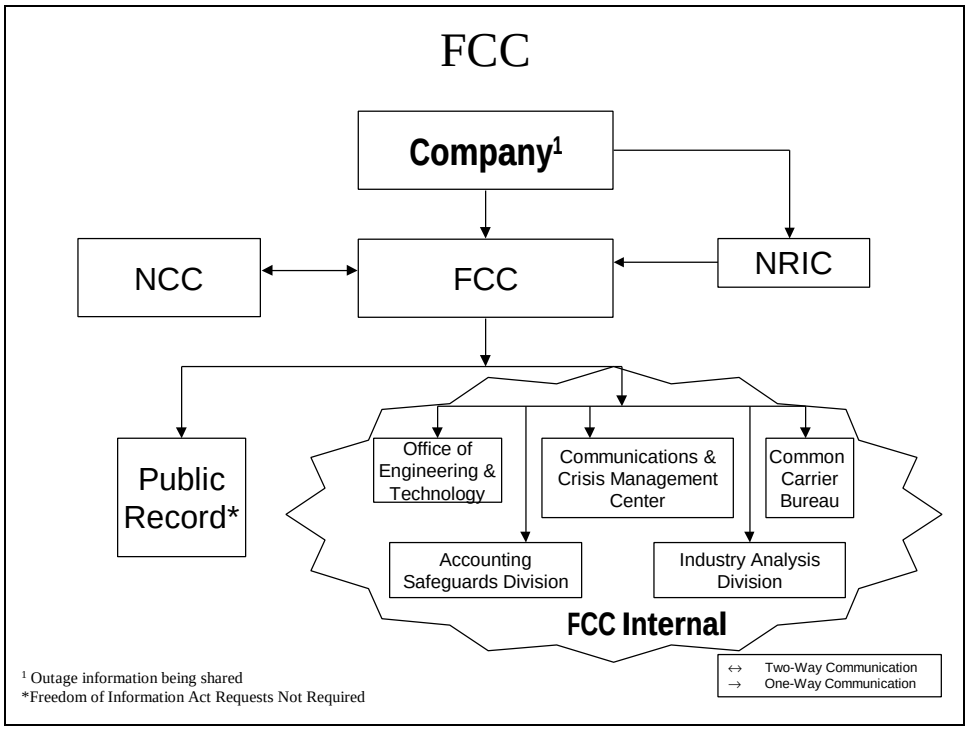
The FBI investigates numerous computer and Internet crimes through various statutes, including the Computer Fraud and Abuse Act, fraud by wire, mail fraud, interstate transportation of stolen property, money laundering, copyright, and economic espionage laws. Companies voluntarily report information through their local FBI Field Office on Public Switched Network intrusions, network intrusions, network integrity violations, privacy violations, industrial espionage, pirated computer software, and other crimes. Companies are not required to report incidents or intrusions to the FBI.

The local Field Office forwards the information to FBI Headquarters, Washington, DC. Based on the information reported, the FBI may begin an investigation into the incident, which may lead to prosecution. Information also may be shared with the NIPC by the local Field Office to facilitate NIPC analysis, watch and warning, and outreach efforts.

To facilitate the sharing of information between the public and private sectors on "cyber" and physical threats to critical infrastructures, the FBI developed the National InfraGard Program in Cleveland, Ohio. Private sector members are asked to voluntarily report actual or attempted illegal intrusions, disruptions, and vulnerabilities of information systems. InfraGard is in its developmental stages; however, it has been suggested that the program expand to eventually include all 56 FBI Field Offices.

InfraGard members provide both a "sanitized" and a detailed description of the incident to their local FBI Field Office. Sanitized descriptions provide all relevant information about the incident but do not identify the company victimized. This description is shared with other InfraGard members. The detailed description, which includes the identity of the victim company, is used by the local FBI Field Office to determine if an investigation is warranted. The NIPC also may receive a copy of the detailed description for use in its trend analysis efforts. (For additional information regarding InfraGard, see Appendix A.)

3.4 Federal Communications Commission (FCC)



Through the *Code of Federal Regulations*,[6] local exchange common carriers, interexchange common carriers, and certain competitive access providers (i.e., those operating transmission or switching facilities and providing access service or interstate or international telecommunications service) that experience an outage, which potentially affects more than 30,000 of its customers on any facilities that it owns, operates, or leases, must notify the Commission if such outage continues for 30 or more minutes.[7] Of the entities described in this report, this is the only one with mandatory outage reporting requirements. Notification of such a service outage must be

[6] Title 47 of the *Code of Federal Regulations*, Chapter 1, Subchapter B, Part 63.100 (b) (c), Notification of Service Outage.
[7] Satellite carriers and cellular carriers are exempt from this reporting requirement.

served on the Commission's duty officer, available 24 hours a day in the FCC's Communications and Crisis Management Center.

The notification must be filed as the Initial Service Disruption Report and include such information as the number of customers affected, geographic areas affected, apparent or known cause, and methods used to restore service. Notification must be by fax or other recorded means. The carrier must file with the Chief, Common Carrier Bureau, a Final Service Disruption Report no later than 30 days after the outage. The report must include all available information on the outage, details of the root cause of the outage, and a listing of the effectiveness and application of any best practices or industry standards as identified by the Network Reliability and Interoperability Council (NRIC) to eliminate or mitigate the impact of outages of the reported type. Within the FCC, reports are shared with the Office of Engineering and Technology and they are made available to the public as well. Freedom of Information Act (FOIA) requests are not required to obtain information from the FCC.

The FCC also requires reports from the NCC on mission-affecting telecommunications outages at special facilities, including nuclear power plants, major military installations, and key Government facilities.

Carriers also are required to file one or more Automated Reporting Management Information System (ARMIS) reports with the FCC. ARMIS reports are required of carriers with revenues in excess of $112 million or if the carrier is a price-cap carrier (i.e., incumbent local exchange carriers). Copies (paper and electronic) are filed annually with the FCC's Accounting Safeguards Division and the Industry Analysis Division. Reports are due on April 1 and cover the prior calendar year.

ARMIS began in 1987 to collect financial and operational data from the largest carriers. Since then, it has expanded to include 10 ARMIS reports that are available to the public. The reports collect various types of information, including—

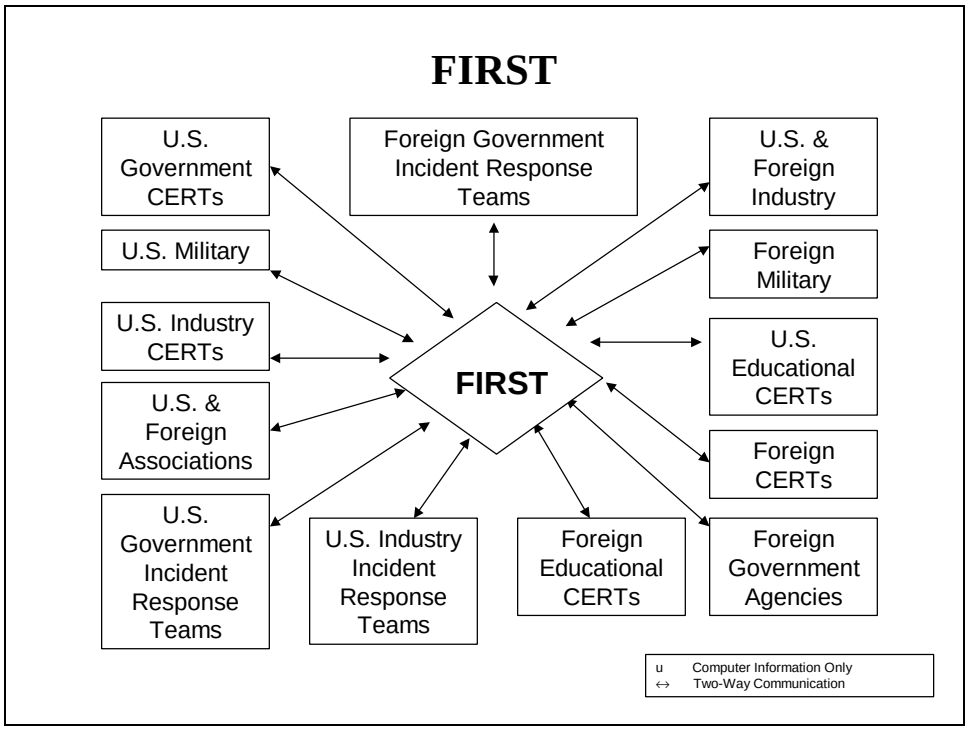
- revenue, expense, reserve, and investment data for all aspects of the carrier's operations,
- interstate access demand data,
- operating results of the local carrier's total activities (i.e., cash flows, assets purchased or sold, accumulated depreciation),
- breakdown of the local carrier's costs between regulated and nonregulated activities,
- carrier separation of revenues and costs between state and interstate jurisdictions,

- service quality data, (i.e., trunk blockages, outages of 2 or more minutes),
- customer satisfaction survey results,
- infrastructure makeup (i.e., quantities and type of switching equipment, call delivery times, amount of call access lines),
- operating data by state (i.e., access lines in service by technology and customer, telephone calls, and minutes of use),
- forecasts of expected regulated and nonregulated investment usage for the current calendar year and following two calendar years, and
- actual usage of regulated and nonregulated investment for the prior calendar year.

In addition to the legal reporting requirements discussed above, members of the telecommunications industry have an opportunity to share additional information with the FCC through the NRIC. The NRIC is made up of Chief Executive Officer (CEO)-level representatives from approximately 35 telecommunications carriers and equipment manufacturers, state regulators, and large and small consumers.

The NRIC may commission studies, prepare reports, review telecommunications industry practices, and make recommendations. The primary role of the NRIC is to develop recommendations to the FCC and the telecommunications industry that, when implemented, will assure reliability, interoperability, interconnectivity, and accessibility to public telecommunications networks. Through various informal focus groups and meetings of representatives of NRIC member organizations, the NRIC has been able to provide consensus advice from the telecommunications industry to the FCC. The NRIC provides members of the telecommunications industry with an opportunity to share information, make recommendations, and shape regulations instituted by a Government agency.

3.5 Forum of Incident Response and Security Teams (FIRST)



FIRST was formed in 1990 following an October 1989 computer security incident involving the Space Physics Analysis Network (SPAN). FIRST brings together individual incident response teams from educational, commercial, Government, law enforcement, and military organizations from around the world. FIRST is neither an official organization nor a legal entity. FIRST members work together voluntarily to handle computer security problems. For example, through FIRST, members may share alert and advisory information on potential threats and emerging incident situations as well as security tools and techniques.

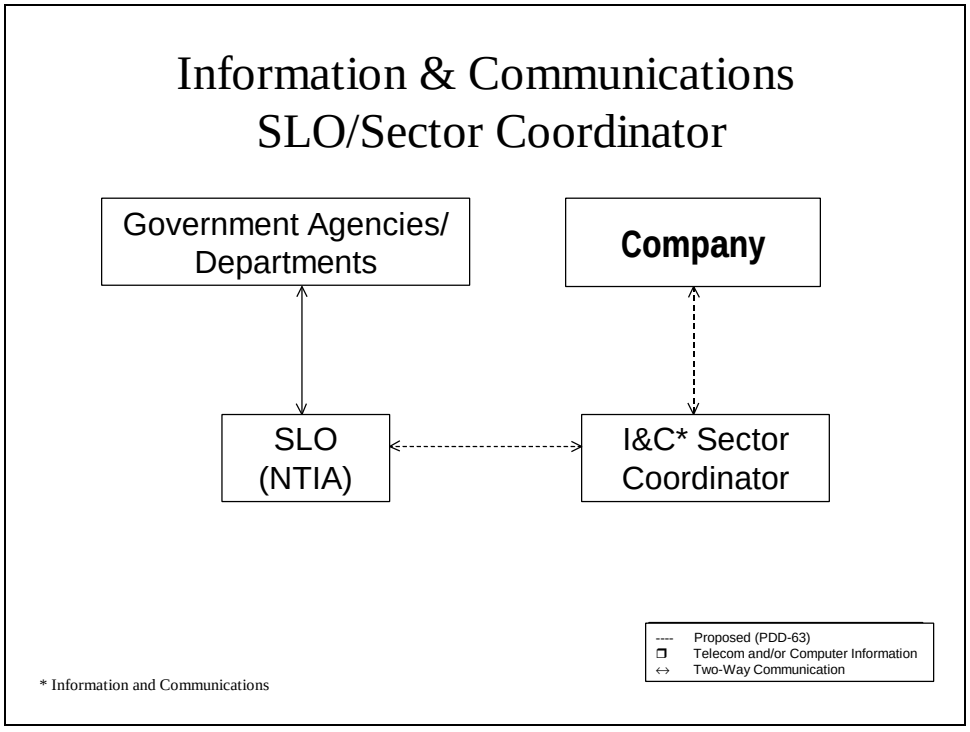
FIRST began with 11 members and has grown to include more than 60 members. The initial members of FIRST were the U.S. Air Force Computer Emergency Response Team, CERT Coordination Center, Defense Information Systems Agency (DISA), Department of Army Response Team, Department of Energy's Computer Incident Advisory Capability, Goddard Space Flight Center, National Aeronautics and Space Administration (NASA) Ames Research Center Computer Network Security Response Team, NASA SPAN, Naval Computer Incident Response Team, National Institute of Standards and Technology Computer Security Resource and Response Center, and SPAN-France.

FIRST participants serve as either members or liaisons. Members are response teams who assist an information technology community or other defined constituency in preventing and handling

computer security incidents. Liaisons are composed of an individual or a representative of an organization other than a response team that has a legitimate interest in and value to FIRST. Today, members include companies such as AT&T, Bellcore, and Cisco Systems; CERTs, including AUSCERT (Australia CERT), CERT-IT (CERT Italiano), and GTCERT (Georgia Institute of Technology CERT); and other organizations, including the Israeli Academic Network, NASA Automated Systems Incident Response Capability, and Pennsylvania State University. A full list of FIRST members may be found at http://www.first.org/team-info/.

The source of the information provided to FIRST participants controls the dissemination of that information. If the information does not contain dissemination instructions, then it cannot be disseminated further outside the FIRST membership. If a member obtains information that is subject to a nondisclosure agreement, then no other FIRST member may assume rights to that information.

3.6 Information and Communications Sector Liaison Official (SLO)/Sector Coordinator (SC)

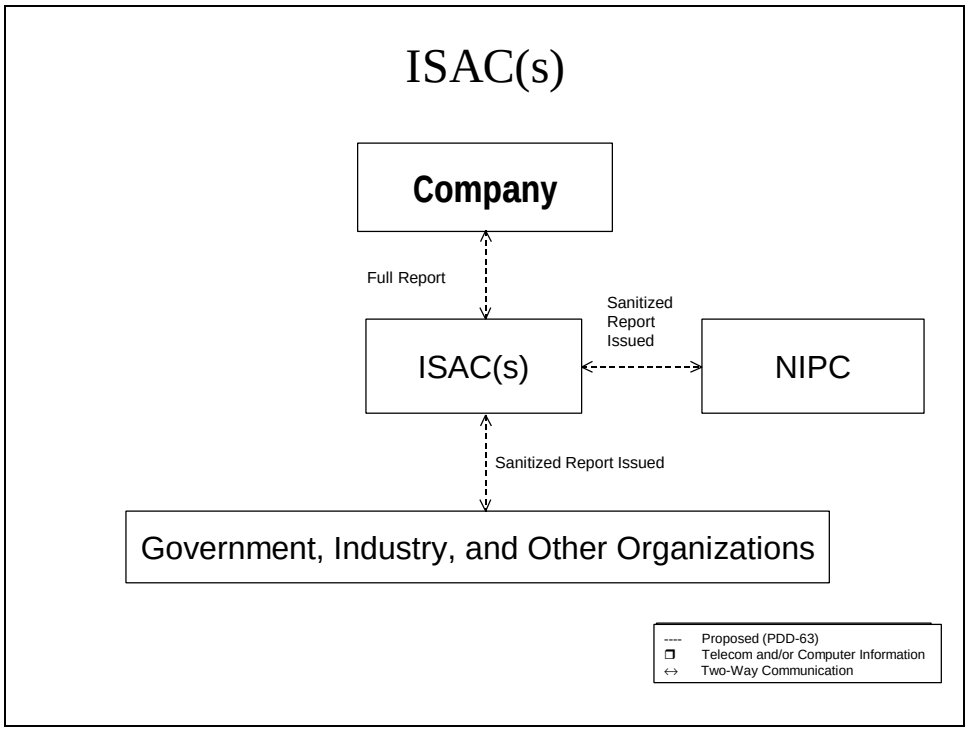


PDD-63 calls for an innovative framework to eliminate vulnerabilities in critical infrastructures through a public-private partnership. To achieve this effort, a fully coordinated effort between the public and private sectors is needed. To aid that process, for each major sector, an SLO will be appointed from the lead Government agency or department representing that sector. The SLO

will identify a private sector representative, called the Sector Coordinator, to represent the sector. The Clinton Administration's *Policy on Critical Infrastructure: PDD-63 White Paper* notes that participation by private sector owners and operators in efforts to protect the national infrastructures is voluntary.

The Department of Commerce's National Telecommunications and Information Administration (NTIA) has been designated the lead agency for the information and communications sector. The SLO, a senior officer from NTIA, will work with the Sector Coordinators to implement PDD-63 initiatives. The Sector Coordinators for the information and communications sector initially will be a consortium of three trade associations, including the Information Technology Association of America (ITAA), the Telecommunications Industry Association (TIA), and United States Telephone Association (USTA). NTIA has indicated that strategic information for use in planning and analysis efforts is of particular interest rather than individual incident information.

3.7 Information Sharing and Analysis Centers (ISAC)



PDD-63 envisions the creation of one or multiple ISACs. Per PDD-63, an ISAC(s) potentially will be a private sector entity that will share information related to vulnerabilities, threats, intrusions, and anomalies affecting the critical infrastructures. The ISAC(s) concept is in the

developmental stage with much discussion taking place. The concept is continuously evolving with time. The following highlights the characteristics of an ISAC(s) as proposed by PDD-63.

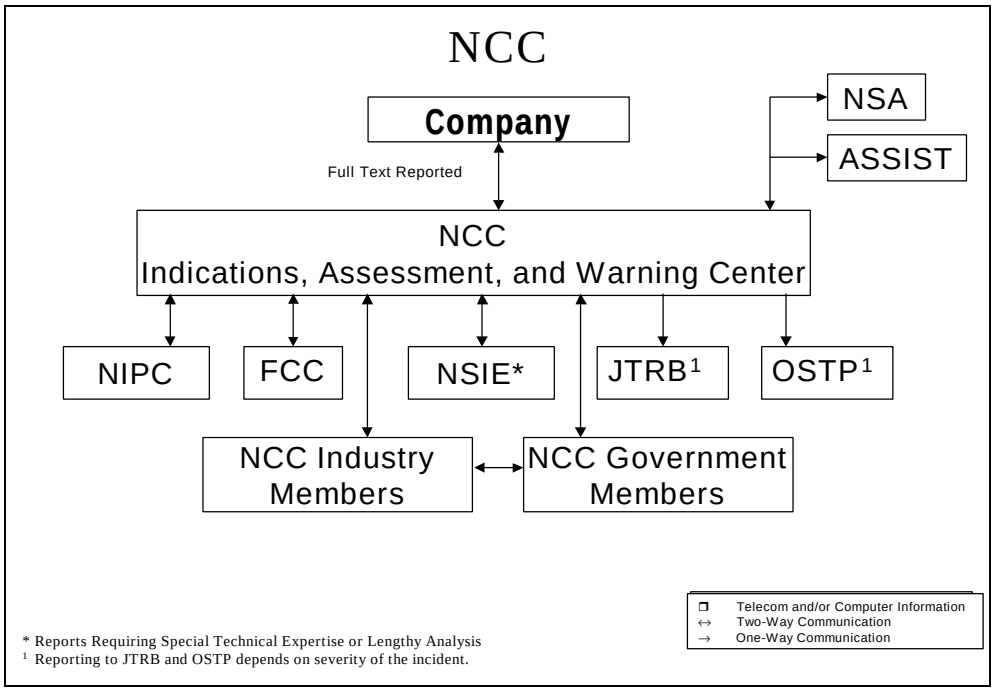
According to PDD-63, the private sector will develop the design and function of an ISAC.[9] It is envisioned that an ISAC will gather, analyze, sanitize, and disseminate private sector information to the NIPC and industry. Information collected by the NIPC also could be gathered, analyzed, and disseminated to the private sector through an ISAC. An ISAC's direct relationship to the NIPC will be determined by the private sector.

It was suggested in PDD-63 that the Centers for Disease Control and Prevention could serve as a model for designing an ISAC (see Appendix B). Employing such a model would enable an ISAC to establish baseline statistics and patterns, become a clearinghouse for information, possess a large degree of technical focus and expertise on nonregulatory and nonlaw enforcement missions, and provide a library for historical data that could be used by the private sector. The library would be made available to the Government if an ISAC deemed such access appropriate.

The NCC, which today performs functions similar to those proposed by PDD-63 for an ISAC, is being considered to serve as an ISAC for telecommunications.

[9] Currently, discussion is underway concerning the development of individual ISACs to represent each critical infrastructure sector.

3.8 National Coordinating Center for Telecommunications (NCC)



The NCC was established in 1984 to share information on telecommunications outages to expedite restoral. More recently, the NCC has expanded its operation to share information on significant electronic intrusions affecting telecommunications critical to national security and emergency preparedness (NS/EP). This includes information related to telecommunications outages, attempted or actual penetration or manipulation of databases, public network (PN) intrusion incidents and outages, and significant abnormal events or anomalies in operational activity that may indicate a coordinated attack.

The NCC is operated by the Manager, NCS, and has participants representing telecommunications companies and Government departments and agencies. The NCC has two categories of participants—resident and nonresident. Resident industry participants are AT&T, COMSAT, GTE, ITT Industries, MCI WorldCom, National Telecommunications Alliance, and Sprint. Resident Government departments and agencies are the Department of Defense (DOD), Department of State, Federal Emergency Management Agency, and General Services Administration (GSA). Non-NCC industry and Government entities also may submit reports to the NCC. Some discussion has taken place within the IES regarding the expansion of NCC participation in order to fulfill an expanded "cyber" mission, including having participants from outside the local area contribute during incidents and meetings via phone or other form of communications.

The goals of the NCC include the near real-time exchange of information on actual or potential PN operational disruptions, including electronic intrusion incident information, between the telecommunications industry and Government and among the companies participating in the NCC. The NCC's Indications, Assessment, and Warning (IAW) Center collects, analyzes, and disseminates information. The NCC will, when appropriate, share incident information with some or all NCC participants and report, where appropriate, to other Government and industry organizations. The NCC IAW Center functions are evolving. Reporting criteria established during the IAW Center Pilot Test have been revised to try to improve incident reporting. A revised concept of operations for the IAW Center is being developed.

As part of NCC membership in the NSIE, NCC staff has access to all information from the NSIEs (see paragraph 3.10), including NSIE bulletins and NSIE vulnerability database reports. The NCC is expected to forward reports to the NSIEs. These may include incident reports and requests for special technical expertise or analysis, a consolidated incident report, or any previously agreed upon report.

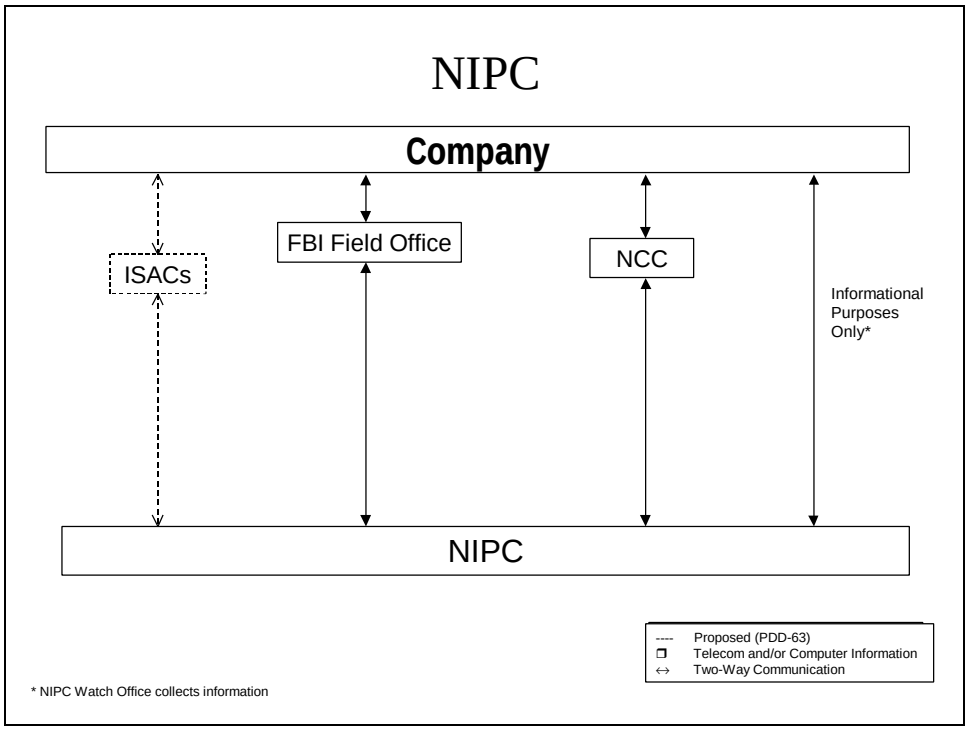
The NCC also interacts with a number of Government departments and agencies, including the National Security Agency (NSA) and DISA's Automated System Security Incident Support Team (ASSIST). In addition, it has been proposed that the NCC coordinate with the NIPC and use its existing relationship with industry to ensure that telecommunications infrastructure information is passed between the NIPC and the NCC.[10] Finally, depending on the severity of the incident, the NCC will pass along information to the Director, Office of Science and Technology Policy (OSTP). The Director, OSTP, also is the Director of the Joint Telecommunications Resources Board (JTRB). If the situation warranted it, he would convene the JTRB.

The NCC also is responsible for reporting special facility outages to the FCC (NCC Standard Operating Procedure [SOP] 010). Any mission-affecting telecommunications outage at any special facility (nuclear power plants, major military installations, and key Government facilities) reported to the NCC that is expected to last or lasts at least 30 minutes will be reported to the FCC. No reports have been made to the NCC under this SOP to date.

Reporting to the NCC is done using whatever means necessary to ensure the delivery of the information. Much of the reporting is done via public-line telephone, e-mail, or in person through resident company or agency representatives. The use of encryption is being examined by the NCC and participating companies as a means of exchanging sensitive information.

[10] A memorandum of understanding was crafted between the NCC and NIPC, but to date has not been agreed on.

3.9 National Infrastructure Protection Center (NIPC)



The DOJ and FBI created the NIPC in February 1998. The concept of the NIPC grew out of recommendations by the PCCIP to develop an integrated IAW capability to protect America's critical infrastructures. The NIPC's role was expanded under PDD-63, which directed the NIPC to serve as a national critical infrastructure threat assessment, warning, vulnerability, law enforcement investigation, and response entity. The NIPC's mission is to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and cyber, that threaten or target the Nation's critical infrastructures.

The NIPC is an interagency center operating within the FBI. The center is designed to include representatives from the FBI, DOD, the intelligence community, other Federal departments and agencies, State and local law enforcement, and private industry. As a relatively new organization, the NIPC is working to solidify contacts with not only other Government departments and agencies but also private sector organizations to fully develop a process for sharing information. This process will evolve as the NIPC becomes fully operational.

The type of information to be shared with the NIPC includes actual or attempted computer intrusions involving the critical infrastructures as well as physical attacks on the infrastructures. Although the authorities of the NIPC are derived from statute, Presidential Decision Directives, and Executive Orders, private sector reporting of information to the NIPC is voluntary.

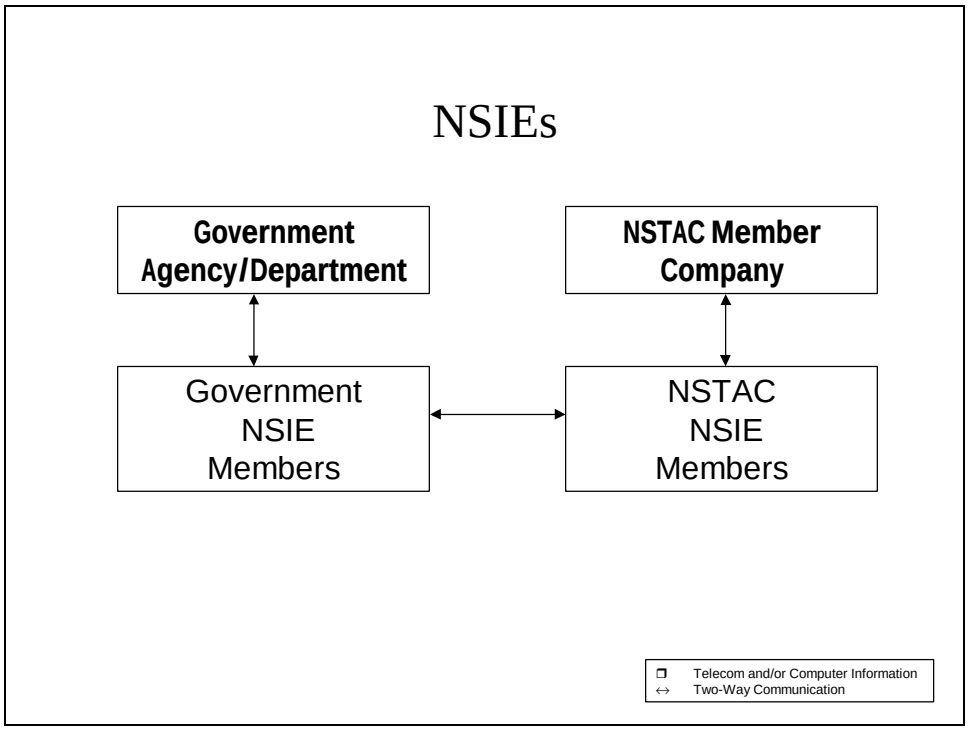
Executive branch departments and agencies will share information with the NIPC about threats and warning of attacks. In addition, the NIPC may establish its own direct relationship with the private sector and any private sector information sharing entity such as an ISAC.

Information to be shared with Federal, State, and local agencies; relevant owners and operators of critical infrastructures; and any private sector information sharing and analysis entity (i.e., an ISAC) will be sanitized before release if the information relates to law enforcement or intelligence matters. Until a case is closed, however, case-sensitive information will not be shared. Attack warnings or alerts will be issued to any private sector information sharing and analysis entity (the ISAC) and owners and operators in sanitized or unsanitized formats.

Future NIPC initiatives may include coordinating and developing trusted communications networks to exchange threat and warning data with Government and private sector entities. Furthermore, the NIPC is developing a real-time alert capability (watch and warning) for both the public and private sectors for threats to the critical infrastructures.

Currently, reports are transmitted largely via telephone, e-mail, or fax. Entities are encouraged to contact their local FBI office with information regarding a computer intrusion. The lead agent in the FBI Field Office communicates the intrusion information to the NIPC. From there, the information is analyzed and combined with other threat and vulnerability data. Information also is shared with other Government agencies as appropriate and permitted by law. The entity experiencing an intrusion also is encouraged to contact the NIPC Watch Office, which collects reports via e-mail or fax for informational use only. The Watch Office provides information to Government and private sector recipients through a variety of products, including alerts and advisories.

3.10 Network Security Information Exchanges (NSIE)



In April 1990, the Chairman of the National Security Council's (NSC) Policy Coordinating Committee-National Security Telecommunications and Information Systems requested the Manager, NCS, to identify what action should be taken on the part of Government and industry to protect critical national security telecommunications from the "hacker" threat. In early 1990, the Manager, NCS, requested that NSTAC provide industry's perspective on the network security issue. In response, NSTAC established the Network Security Task Force to identify a mechanism for security information exchange and produce an implementation plan for such a mechanism. In response to this recommendation, and to the tasking from the NSC to the Manager, NCS, Government and NSTAC established separate, but closely coordinated, NSIEs. In May 1991, the NSIE charters were finalized, and Government and industry designated their NSIE representatives, chairmen, and vice-chairmen. The first meeting of the NSIEs was held in June 1991.

The two NSIEs, the NSTAC NSIE and the Government NSIE, each have separate charters and memberships, but they meet jointly to share information. Members voluntarily share information related to threats, incidents, and vulnerabilities affecting PN software. This information includes attempted or actual penetrations or manipulations of software, databases, and systems related to critical NS/EP telecommunications. NSIE members are expected to share information on—

- new intrusion activities or updates to previously discussed intrusion 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, or 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.

NSTAC companies wishing to participate in the NSTAC NSIE are approved by the IES. Current members include the National Telecommunications Alliance, Nortel, Raytheon, GTE, U S West, Bank of America, Science Applications International Corporation, Computer Sciences Corporation, MCI WorldCom, Lockheed Martin, COMSAT, AT&T, ITT Industries, Sprint, Electronic Data Systems, Boeing, Executive Security and Engineering Technologies, Unisys, and TRW. Government NSIE members include departments and agencies that are major telecommunications service users, represent law enforcement, or have information relating to network security threats and vulnerabilities. Current Government NSIE members include DOJ, DOE, NSA, DOD, FBI, FCC, CIA, Office of the Manager, NCS (OMNCS), Defense Intelligence Agency, National Institute of Standards and Technology, and United States Secret Service. All representatives are subject matter experts engaged in prevention, detection, and/or investigation of telecommunications software penetrations or have security and investigative responsibilities as a secondary function.

Member organizations are required to sign a nondisclosure agreement, and their representatives and all guests are required to sign a personal acknowledgment before they attend their first NSIE meeting. All representatives must have secret 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 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. Most information sharing in meetings is at the N-2 level. At Level N-3, information can be shared beyond NSIE member organizations. N-3 sharing normally takes place through NSIE documents that are broadly disseminated and NSIE-sponsored workshops (e.g., the Insider Threat Workshop and white papers).

3.11 Information Sharing Within Trade Associations

An additional avenue for information sharing is provided within the forum of some trade associations. Telecommunications companies and providers, in many cases, will join organizations consisting of other corporations that operate within similar technological realms and face related market difficulties. The general mission of trade associations is to collect information and provide a forum for their members to discuss and resolve technical, regulatory, and other issues of mutual concern. The membership makeup determines the type of information that will be shared within the association. In most cases, the member companies have nonbinding formal agreements barring them from disclosing proprietary information to nonmember companies, Government agencies, or the public, unless required to do so by law.

The medium for sharing information within the association is dependent on the issues that are being presented. Many associations publish newsletters and technical reports regarding basic industry trends and new technologies. These types of publications do not require a high degree of security. If the trade association is involved with issues that include information that a company believes to be proprietary or private, avenues are established to ensure this information remains confidential. In most cases, members may submit information via public-line telephone, e-mail, or in person.

After receiving sensitive information, associations can establish forums to allow member companies to learn about incidents or actions that have occurred in other member companies. They also may discover how their own company could be at risk. In this case, the forum can provide a framework for members to strategize plausible solutions and to establish a defense to keep similar incidents from happening in the future.

TSA is a unique example of the type of information sharing discussed above as it pertains directly to the sharing of security-related information. Many other trade associations exist that facilitate the sharing of various types of information pertinent to the telecommunications industry. This report addresses only a handful of those associations. (See Appendix C for additional descriptions of several individual trade associations.)

Telecommunications Security Association

TSA is an international association made up of the Regional Bell Operating Companies, GTE, several Canadian telecommunications carriers, and a number of U.S. local exchange carriers. All TSA members are wireline companies. TSA's primary information sharing directive is to inform and protect its members from the threat of network intrusions.

TSA companies learn about network "hacking" incidents that have occurred in other companies and the possibility of these incidents occurring in their own company. TSA provides a forum for members to develop plausible solutions to numerous types of network intrusions. Finally, member companies work together to establish a defense to prevent similar incidents from happening in the future. Member companies have a long-standing partnership and do not share any information with nonmember companies, Government departments or agencies, or the public.

TSA utilizes e-mail and conference calls to inform members of network intrusions. Conference calls provide members with a real-time forum for solving problems and constructing risk management programs for the future.

4.0 POTENTIAL LEGAL BARRIERS TO INFORMATION SHARING

The PCCIP's Report, *Critical Foundations: Protecting America's Infrastructures*, identified seven legal impediments:

- confidential information,
- trade secrets and proprietary information,
- classified information,
- national security,
- antitrust,
- liability, and
- State government liability and disclosure.

In this study, these seven impediments are addressed, particularly with regard to their impact on information sharing between telecommunications companies and the various entities identified by the compendium.[11] Some channels of information sharing may be affected by several of these potential barriers, whereas others may be influenced by only one or two barriers. Sharing outage information with the FCC, for example, is required by law and records are publicly available. Solutions to address these legal barriers have been discussed in a number of forums; however, they are not examined in this report.[12]

4.1 Confidential Information

The term "confidential information" mentioned in this section is used as it was by the PCCIP and is addressed in that context by examining limitations that FOIA may place on information sharing. It is not referring to confidential information under the terms of Executive Order 12958 "Classified National Security Information" which classifies as confidential information that which the unauthorized disclosure of could cause damage to national security. Classification issues are addressed in Section 4.3 with regard to different levels of classification and national security.

Confidential information that is shared with the Government may be subject to FOIA requests. FOIA mandates that records in the possession of departments or agencies in the executive branch of the Government be available to the public on request. There are, however, nine exemptions under FOIA that protect against the disclosure of information that would harm national defense or

[11] No original legal analysis of these impediments was conducted by the LRG for this report. The legal analysis is based on the work of the PCCIP and is in no way intended to validate or dispute the PCCIP's findings. The LRG recognizes that other potential barriers to information sharing such as privacy do exist; however, the LRG decided to limit the scope of the study to only those legal impediments identified by the PCCIP.

[12] The LRG determined that addressing solutions to overcoming legal barriers exceeded the scope of this particular report. The topic could be addressed as a next step once PDD-63 initiatives are further along.

foreign policy, the privacy of individuals, the proprietary interests of business, and the functioning of the Government.

Two exemptions permitted under FOIA are particularly relevant to sharing confidential information. The first exemption is the withholding of confidential business information and trade secrets. A trade secret refers to a commercially valuable plan, formula, process, or device. Confidential or privileged business information includes commercial or financial information obtained from a person. Documents qualify for withholding in this category if the disclosure of such information would harm the competitive position of the person or entity who submitted the information. Agencies are required to notify the submitter of the business information that disclosure of the information is being requested. The submitter then has an opportunity to persuade the agency that the information should be withheld. If the submitter disagrees with the agency's determination, the submitter also may file suit to block disclosure.

The second exemption of relevance to this study permits agencies to withhold law enforcement records that could interfere with enforcement proceedings, deprive a person of a right to a fair trial or an impartial adjudication, constitute an unwarranted invasion of personal privacy, reveal the identity of confidential sources, reveal the techniques and procedures used in investigations or prosecutions, or endanger the life or physical safety of any individual.

In addition to the two outlined above, the following exemptions are permitted under FOIA:

- the withholding of material that is properly classified pursuant to an Executive Order in the interest of national defense or foreign policy;
- the withholding of internal Government documents;
- the withholding of documents related solely to an agency's internal personnel rules and practices;
- the withholding of documents whose distribution is restricted by other laws;
- the withholding of personnel, medical, and similar files that if disclosed would permit the invasion of personal privacy;
- the withholding of reports or information prepared by or for a bank supervisory agency; and,
- the withholding of documents relating to geological and geophysical information, data, and maps concerning wells.

Although some information obtained by the FBI during investigations is covered by the FOIA exemption regarding law enforcement records, it is unclear whether information shared with the NIPC will fall inside that category. Companies may be reluctant to share information with the FBI and the NIPC out of concern that the records will not be protected by FOIA exemptions.

Should public awareness of NCC operations increase, FOIA requests for records may become a concern for participating companies. Participants may be reluctant to share information with the NCC if the NCC is unable to ensure that such records qualify for exemption and can be withheld upon request.[13]

4.2 Trade Secrets and Proprietary Information

Although trade secrets and proprietary information are addressed by exemptions within FOIA, concerns related to these areas may prevent companies from sharing information with other companies. One issue is that the costs associated with the release of proprietary information, trade secrets, or other sensitive information may exceed the benefits associated with sharing information on an incident with other companies, organizations, or Government departments and agencies. The release of such information may provide a competitor with the means to gain an advantage over or take market share or power away from the reporting company. In addition, a company's public image may be tarnished significantly, even destroyed, by the release of proprietary information, trade secrets, or other similar information.

Trade secrets are defined as formulas, patterns, devices, or a compilation of information that enables a business to attain a competitive advantage over other companies. Trade secrets are generally protected by State law, not federal law. Material usually qualifies as a trade secret if measures have been taken to ensure the secrecy of the information. Widely distributed information is not considered a trade secret unless adequate security measures have been taken to ensure that access to the material being distributed maintains the secrecy of the information. A trade secret holder is protected from unauthorized disclosure and use of the trade secret by others and from another person's obtaining the trade secret through improper means.[14] In this context, companies may be reluctant to share information unless measures are adequate to ensure the secrecy of the information.

InfraGard member companies share proprietary information with the FBI and sensitive information with other companies. Although some progress has been made, significant obstacles will remain when/if InfraGard is expanded. To date, members have been willing to share some information; however, when/if the number of InfraGard chapters grows, the sharing of proprietary information may become a larger concern.

[13] To date, the NCC has not been the subject of any FOIA requests, but the concern exists that FOIA could eventually become a barrier to sharing information.
[14] *Intellectual Property and the National Information Infrastructure*, pp. 173-175.

CERT has developed a trusted relationship with companies and organizations that ensures that identities and sensitive information remain confidential. By not sharing any information on a vulnerability until a fix is available, CERT has a proven history of protecting information. With increased competition, some companies may continue to be concerned that such publicity would hurt them competitively.

NCC Standard Operating Procedure (SOP) 016 stipulates that concerns regarding proprietary information be resolved with the reporting entity before the incident report is released to other industry or Government representatives or organizations. The NCC seeks to ensure the anonymity of the entity reporting an incident. Information reported to the NCC belongs to the organization reporting the incident. An incident report is released to only those organizations with which the reporting organization wishes to share the information. Moreover, the reporting organization has final approval of the content contained in the report.

NCC participants have built a relationship based on trust that encourages information flow; however, concerns may arise among participants if the current makeup is changed. There has been discussion within the NCC regarding the inclusion of new participants in order to fulfill the NCC's enhanced "cyber" mission. These participants would share information, report incidents, and serve as points of contact for other NCC participants during an event. The participants, however, would not be resident at the NCC.[15] There is some concern that increased participation in the NCC would weaken the trusting relationships that have been fostered among current NCC participants.

NSIE representatives have developed relationships built on trust that make information easier to share. Nondisclosure agreements signed by member organizations, their representatives, and their guests before attending their first meeting largely alleviate proprietary information concerns that companies might have.

4.3 Classified Information and National Security

Information usually is classified at some level by various Government departments and agencies, to safeguard national security and to protect intelligence "sources and methods." Executive Order 12958 "Classified National Security Information" permits the classification of information at the top secret, secret, and confidential levels. Information may be classified if the information is about military plans, weapons systems, or operations; foreign government information, intelligence activities, sources, methods, or cryptology; foreign relations or activities of the United States, including confidential sources; scientific, technological, or economic matters relating to national security; U.S. Government programs for safeguarding nuclear materials and facilities; and

[15] Virtual membership in the NCC is an evolving concept. It is in its preliminary stages, characterized by much discussion focused on fleshing out concerns and issues surrounding such membership.

vulnerabilities or capabilities of systems, installations, projects or plans relating to national security.

Although there is an FOIA exemption that permits the withholding of material that is properly classified pursuant to Executive Order 12958, classification can make the dissemination of information to those who might need it, difficult, or in some cases, impossible. Further, Government departments and agencies are constrained in sharing information by specific guidelines that control their interaction with foreign corporations or corporate entities with significant foreign ownership.

These factors may prevent Government departments and agencies such as the NIPC from sharing certain information with companies that have foreign interests. InfraGard members share only unclassified and sensitive-but-unclassified information. For the NSIEs, classification is not a barrier to information sharing because the OMNCS, as secretariat to the NSTAC, can sponsor and facilitate one-time clearances to NSIE representatives who do not have "permanent" clearances through their companies.

4.4 Antitrust

Three major Federal antitrust laws protect competition and ensure that consumers enjoy lower prices and improved products: the Sherman Antitrust Act, the Clayton Act, and the Federal Trade Commission Act. The Sherman Antitrust Act outlaws all contracts, combinations, and conspiracies that unreasonably restrain interstate trade, including agreements to fix prices, rig bids, and allocate customers. The act also makes monopolization of interstate commerce a crime. The Clayton Act prohibits mergers or acquisitions that would lessen competition; but as a civil statute, it carries no criminal penalties. The Federal Trade Commission Act prohibits unfair methods of competition in interstate commerce. Like the Clayton Act, it carries no criminal penalties.

Overall, the law recognizes that firms do make certain arrangements to cooperate jointly on R&D projects that may benefit consumers and allow companies to compete more effectively as a result of the arrangement. The Government does not prosecute all agreements between companies, primarily those that would fix prices or prevent consumers from accessing new and improved products.

Although it appears that arrangements for sharing information among the companies and other entities described throughout this study may be interpreted to not violate the three major Federal antitrust laws, companies may be reluctant to share information because of impediments that they perceive might arise from antitrust and unfair business practices.

4.5 Liability

Liability for failure to disclose information that could have prevented harm to a critical infrastructure is a concern for telecommunications companies. This concern has been particularly evident in light of the Year 2000 (Y2K) technology problem. In this regard, the Y2K experience may prove to be instructive. As a result of Y2K, companies may experience outages, incidents, or other events attributable to Y2K that they may choose to report to not only Government departments and agencies but also other companies and private sector organizations. Congress passed the Y2K Information and Readiness Disclosure Act to encourage the disclosure of information about computer problems, solutions, test practices, and test results. Although the Y2K legislation contains several exclusions and exemptions that protect companies from liability and antitrust issues, some companies may continue to be reluctant to share information related to Y2K events.

4.6 State Government Liability and Disclosure

Common law and statutes vary in each of the 50 states. For example, individual states have public access laws regarding the disclosure of State and local records. The diverse nature of State law may further complicate information sharing. Given that there is no uniform code relating to the sharing of information by companies in the telecommunications arena, companies find themselves monitoring the laws on a state-by-state basis.

5.0 CONCLUSION

For some time, the NS/EP telecommunications community has recognized information sharing between industry and Government as a critical factor in responding to and preparing for outages and intrusions into networks. The NCC and the NSIEs have been successfully sharing information for several years—the NCC for 15 years and the NSIEs for 8 years. While a great deal has been learned from the experience and longevity of the NCC and NSIEs, the identification and discussion of other existing and proposed outage and intrusion information sharing channels provides additional insights to assist the NSTAC in assessing critical information sharing issues, particularly implementation of PDD-63.

For this report, industry and Government forums that share information were identified and discussed. From this compendium of telecommunications outage and intrusion information sharing entities, some general observations were made.

- *Information sharing occurs in a number of forums.* This compendium demonstrates that companies within the information and communications industry are sharing information on outages and intrusions with the Government and other entities through several forums. It also demonstrates that the telecommunications portion of the information and communications sector is further along in the process of establishing mechanisms (e.g., an ISAC) to share information on network outages and intrusions.

- *Information sharing may be affected by legal barriers*. When considering the decision whether to share information, companies may be concerned about the legal impediments identified by the PCCIP. Once these concerns (e.g., disclosure and liability), which may contribute to a reluctance on the part of entities and individuals to share information within a particular forum, have been addressed, participants are in a position to share information more freely.[16]

- *Information sharing is mostly voluntary*. Of the existing and proposed information sharing channels addressed in this report, all but one are voluntary. Current information sharing practices between and among industry and Government take place almost entirely without regulation. Only the FCC has established a mandatory two-stage reporting scheme in its Notification of Service Outage requirement.

[16] The original intent of this LRG initiative was to review and comment on the potential legal and regulatory barriers to information sharing the PCCIP identified in its final report, *Critical Foundations: Protecting America's Infrastructures*. However, based on LRG discussions, as well as discussions in other IES groups, it became apparent that implementation of PDD-63, based primarily on the PCCIP's recommendations, was still at an early, evolutionary stage. Simply stated, the LRG was not in a position to critically assess how the potential legal and regulatory barriers identified could affect information sharing in the PDD-63 context.

- *Voluntary information sharing is dependent on receiving a benefit.* Participants share information when they receive information or other benefit in return. Reciprocal information can include assistance in solving a problem, awareness about a vulnerability, or a bulletin on potential threats. If it is perceived that a participant/company will not receive useful information in return, the participant/company will assume the "default position"—if there is nothing in it for me, why should I expend the resources to participate in the sharing process? The existing channels of information sharing addressed in this report suggest that this attitude can be overcome if there is value from information sharing.

- *Information sharing is based on trusted relationships.* Information sharing is the result of mutual trust between participants. Relationships have been built over time between individuals and entities. The type of information and amount shared are a reflection of the trust inherent in these relationships.

- *Information sharing may be dependent on the company and individual participant.* Although organizations may be official members of an information sharing entity, their participation can be influenced by their management's internal policies. Further, the effectiveness of the information sharing process depends largely on the individual. Even when management genuinely supports the process, the individual representative may not be inclined to participate fully. In contrast, there are some cases in which an organization's participation is based solely on the value to the representative, who finds a way to participate in a meaningful way.

- *Information sharing is content-focused.* This report describes a number of entities with which companies share or potentially will share information on outages and electronic intrusions affecting telecommunications. Companies are not necessarily sharing the same type of information with all of the entities. The entities examined, in most cases, focus on specific types of information they need to receive. For example, entities are interested in such specifics as computer security best practices, vulnerabilities, incident response activities, or intrusions affecting NS/EP telecommunications. In addition, some entities function with a near-real-time capability to detect and respond to incidents; others are involved in more long-term planning and analysis efforts. The function of the entity receiving information and how it uses information influence the type and timeliness of the information shared.

As reliance on the evolving telecommunications infrastructure continues to grow, outage and intrusion information sharing is increasingly important, especially where it contributes to the Nation's NS/EP. It is the intent of the LRG that this report be used by other NSTAC subgroups to continue addressing critical information sharing processes and issues as they unfold. Further analysis and understanding of the lessons learned by the entities examined in this report, for

example, could provide the foundation for determining best practices for information sharing at the National level and could be beneficial to those entities responsible for implementing PDD-63.

SELECTED REFERENCES

Antitrust Enforcement and the Consumer, U.S. Department of Justice.

Beauprez, Jennifer, "Hack Attack: FBI, Area Companies Team up to Alert Each Other to Security Breaches," *Crain's Cleveland Business*, July 13, 1998.

CERT Coordination Center Web Site, http://www.cert.gov

Critical Infrastructure Assurance Office Web Site, http://www.ciao.gov

Executive Order 12958 "Classified National Security Information," April 17, 1995.

Federal Bureau of Investigation Web Site, http://www.fbi.gov

Federal Communications Commission Web Site, http://www.fcc.gov

Forum of Incident Response Teams Web Site, http://www.first.org

Freedom of Information Act, 5 U.S.C. §552.

"High-Tech Crime Inspires Alliance in Cyberspace," *HeraldNet*, January 21, 1998.

Intellectual Property and the National Information Infrastructure, Report of the Working Group on Intellectual Property Rights, Washington, DC, September 1995.

Kelley, Tina, "In Northwest, Computer Security is a Private-Public Effort," *The New York Times*, March 12, 1998.

McCarthy, Shawn P., "If You Want to Catch a Hacker, Hire One – Or Be A Sophisticated Fed," *Government Computer News*, June 1, 1998.

National Coordinating Center for Telecommunications Standard Operating Procedure (SOP) 016 – Public Network Electronic Intrusion Indications, Assessment and Warning Activities, May 13, 1998.

National Communications System Web Site, http://www.ncs.gov

National InfraGard Program Fact Sheet, 1998.

National Infrastructure Protection Center Fact Sheet, March 11, 1998.

National Infrastructure Protection Center Web Site, http://www.fbi.gov/nipc

Network Reliability and Interoperability Council Web Site, http://www.nric.org

The President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection*, Washington, DC, October 1997.

The President's National Security Telecommunications Advisory Committee Network Group Intrusion Detection Subgroup, *Report on the National Security and Emergency Preparedness Implications of Intrusion Detection Technology Research and Development*, December 1997.

The President's National Security Telecommunications Advisory Committee's Network Security Information Exchange Charter, Amendment 1.

Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*, May 22, 1998.

The Privacy Act of 1974.

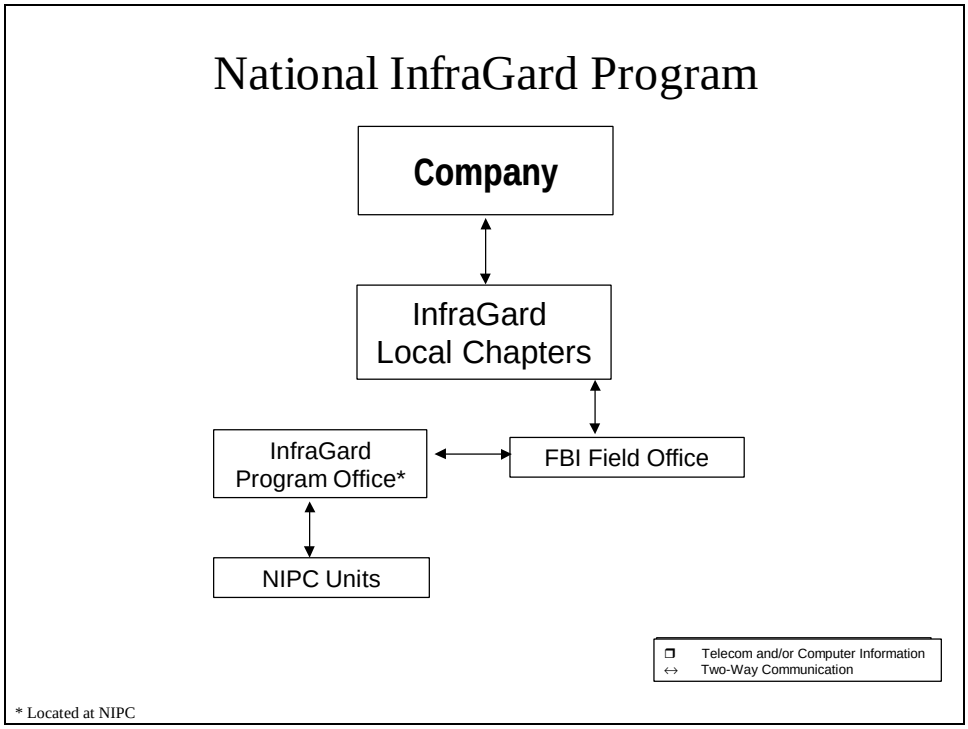
White Paper on the Clinton Administration's Policy on Critical Infrastructure Protection: PDD-63, May 1998.

Year 2000 Information and Readiness Disclosure Act, October 19, 1998.

APPENDIX A

NATIONAL INFRAGARD PROGRAM

APPENDIX A: NATIONAL INFRAGARD PROGRAM



The National InfraGard Program grew out of Executive Order 13010, "Critical Infrastructure Protection," which, among other things, directed the Federal Bureau of Investigation (FBI) to identify and coordinate existing infrastructure expertise inside and outside the Government. The National InfraGard Program began as a pilot project in summer 1996 in Cleveland, Ohio. The National InfraGard Program is currently composed of local InfraGard chapters in Cleveland and Columbus, Ohio, and Indianapolis, Indiana. (The Columbus and Indianapolis chapters are recent additions to the national program.)

The InfraGard Program is in its developmental stages; however, it has been proposed that all 56 FBI Field Offices have an InfraGard Coordinator. That Coordinator will eventually be responsible for developing the local InfraGard chapter and will be the FBI point of contact for all InfraGard issues at the local level.

InfraGard is intended to bring together both the public and private sectors to address "cyber" and physical threats to the critical infrastructures. Private sector members voluntarily report actual or attempted illegal intrusions, disruptions, and vulnerabilities of information systems. Information is

to be shared through both informal and formal means. Members share information at local chapter meetings and via the Alert Network and the InfraGard Secure Web site. Members of the business community, academic institutions, and other Government agencies worked together with the FBI to form the existing local InfraGard chapters. Each chapter tailored its program to meet the needs of the local membership. The FBI Field Office worked with members to identify local infrastructure protection concerns and needs.

InfraGard members determine when it is necessary to report an incident to the FBI. Though not the only means of reporting, the Alert Network facilitates the reporting of physical or cyber attacks. InfraGard member companies share proprietary information with the FBI and sensitive information with other companies. Information that is shared is unclassified and sensitive-but-unclassified. Using encryption technology provided by the National Infrastructure Protection Center (NIPC), members send both a "sanitized" and detailed description of the incident to the InfraGard Program Office (IPO) located at the NIPC.

The sanitized version of the incident sent to the IPO provides all relevant information; however, it protects proprietary information and does not identify the victim company. The IPO forwards this version to other InfraGard members. It is envisioned that this will be conducted at a national level. The detailed version of the incident relates information about the victim's identity and provides adequate background information to analyze the threat in depth. This information is provided to the relevant units within the NIPC and the local FBI Field Office.

Members also share information through the InfraGard Secure Web site. The site can be accessed for information on recent intrusions, real-time infrastructure protection information, recent news articles and press releases on critical infrastructures, and links to computer security technical papers and hacker case summaries. Eventually, the Web site will provide the capability for a secure, integrated electronic discussion group.

InfraGard members sign an agreement allowing them to participate in local chapter meetings and discussions. In addition, InfraGard members must sign a secure access agreement to use the Alert Network and gain access to the InfraGard Secure Web site.

APPENDIX B

CENTERS FOR DISEASE CONTROL AND PREVENTION

APPENDIX B: CENTERS FOR DISEASE CONTROL AND PREVENTION

Background and Mission

The Centers for Disease Control and Prevention (CDC) is the lead federal agency for promoting health and quality of life. The CDC accomplishes its mission of preventing and controlling disease, injury and disability by working with its state, local, and international partners to monitor and detect health problems, conduct research on prevention methods, develop and implement health policies, promote healthy behaviors, and provide public health leadership. The CDC is housed within the Department of Heath and Human Services (DHHS) and is considered part of the Public Health Service (PHS).

The CDC defines its mission as promoting health and quality of life by preventing and controlling disease, injury, and disability. To accomplish this mission, the agency has developed four goals:

- commit to a strong science base in epidemiological, laboratory, behavior, and social science research in developing public health policies,
- utilize CDC's surveillance and health information systems to collect comprehensive information on health problems and risks in order to detect and assess threats to public health,
- provide leadership to State, local, and international partners on prevention policy and practice, and
- develop the ability of public health departments and community-based organizations to carry out essential public health services.

The CDC as a Model for Information Sharing Under PDD-63

The President's Commission on Critical Infrastructure Protection (PCCIP) identified the CDC as a highly successful model for "expeditious information sharing to support action planning."[1] As a result, PDD-63 points to the CDC as a successful model for information sharing that could be applied to protecting the Nation's critical infrastructures. The CDC has shown an ability to work with its partners in determining risks and issuing warnings on various health threats. Its successes regarding various health conditions show that the CDC has been relatively successful in accomplishing its mission. This success is attributed in large part to the CDC's ability to generate cooperation based on an acknowledgment among its partners that the agency's activities are in the

[1] The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October 1997, p. 29.

best interests of public safety. As a result, the CDC is acknowledged by its partners as a leader in chronic disease and injury prevention and control. This respect has developed into strong working partnerships with state and local health departments and other critical partners, which is a basis for its success in gathering and disseminating information. The CDC has in place the following mechanisms that support information sharing and dissemination:

- **CDC Prevention Centers and Programs in Infections Diseases, Environmental Health, Occupational Safety and Health, and Epidemic Services.** This is the primary vehicle through which the CDC monitors health concerns and develops policies and procedures to address those concerns. These national centers are designed to focus on key health problems and health conditions.

- **National Center for Health Statistics.** OMB has designated the CDC as the Federal Government's general-purpose health statistics organization. The CDC supports an information base for identifying health risks as well as designing and tracking prevention programs. Information is then disseminated to its partners in the health community.

- **Sentinel Surveillance Health Information Network.** The Sentinel Health Network is the primary way in which the CDC can receive or disseminate information to its partners in public heath. Information flows into the CDC through this network via its relationships within the state and local health community

- **Mortality and Morbidity Weekly.** Weekly newsletter issued by the CDC to its partners in the health community, which disseminates information to its partners on troubling health conditions.

Note that there are limitations on information reporting that raise questions in the applicability of the CDC model for information sharing for infrastructure protection. The primary question involves reporting policies. The CDC does not have authority to require reporting from health departments and depends on the 50 different State health departments, regulations, and general concern over the public safety to garner data. The formal decision to make a disease reportable is not made by the CDC but rather by the Conference of State and Territorial Epidemiologists. This conference does not have statutory power, but no disease can become reportable without its recommendations. The process by which a state makes a disease reportable varies among executive orders and legislation. Further, the CDC has no authority to impose penalties if information sharing requests are not met. In addition, data collection is hampered by the fact that the CDC does not provide resources to the State and local health departments to support the national notifiable disease system.

APPENDIX C

TRADE ASSOCIATIONS

APPENDIX C: TRADE ASSOCIATIONS

Cellular Telecommunications Industry Association (CTIA)

CTIA is a national trade association composed of more than 700 direct and associate member companies that represent personal communications systems (PCS) and cellular providers, specialized mobile radio (SMR) providers, wireless manufacturers, and numerous wireless support companies. CTIA promotes wireless products and issues currently facing the wireless industry. The association promotes member companies and shares information with members through a number of media, including an interactive Web site. Through this site, which includes newsletters, press releases, reports, and association information, members and the public can register to receive daily and weekly e-mails regarding pertinent wireless topics and news. CTIA also sponsors a number of conferences and trade shows that deal directly with products and matters within the wireless industry.

CTIA has not incorporated any privacy conventions in its information sharing practices. Currently, non-disclosure agreements are not used to protect proprietary information. There have been instances where an outside entity has requested information and CTIA members were asked to submit data that could be viewed as proprietary. Under these circumstances, member companies submitted the necessary information to a third party to be sanitized before it was delivered to the requester.

Communications Fraud Control Association (CFCA)

CFCA is a not-for-profit international educational association composed of interexchange carriers, local exchange carriers, competitive local exchange carriers (CLEC) and independent local exchange carriers (ILEC), private network companies, law enforcement officers and agents, customer premises equipment-private branch exchange (CPE-PBX) users, e-mail providers, security product vendors, and corporations that use telecommunication services. CFCA was founded in 1985 to combat telecommunications fraud. With more than 300 members, CFCA works to develop close relationships among telecommunications security professionals and to serve as a clearinghouse for information related to telecommunications fraud.

Member representatives must have primary or secondary responsibility for the detection, prevention, and/or investigation, apprehension, and prosecution of fraud offenders, or must be directly involved with primary or secondary responsibility for the areas concerned with telecommunications systems fraud within a company. Members in CFCA have access to information on local exchange and interexchange carriers, carrier identification codes, educational conferences and workshops, vendor products, legal and legislative updates, and law enforcement contacts. Members also have access through CFCA to public awareness materials for use in educating members' customers and employees as well as the public. In addition, members receive

a weekly newsletter abstracting breaking cases, telecommunications news briefs, and terminating numbers connected with high abuse. Through membership in the CFCA, members are able to turn to one another to solve certain security issues.

Information Technology Association of America (ITAA)

ITAA is a national trade association that encompasses more than 11,000 direct and affiliate members from U.S. information technology companies. ITAA members are involved in the sale, support, and service of computers and software, telecommunications products and services, Internet and online services, and systems integration. A number of professional service groups also are members of ITAA.

ITAA was established to provide its members with a forum in which to discuss industry topics. Many ITAA members share information regarding related industry topics, including possible legislative and regulatory concerns that could affect member companies. ITAA uses a number of media for sharing information, including newsletters, reports, and an interactive Web site. Divisions or groups within the association also publish newsletters and reports on subjects related to their topic; these newsletters and reports are then shared with members and the public. ITAA also shares information with non-member companies and the public by sponsoring conventions and trade shows where member companies display company products.

ITAA utilizes a strong private forum that provides member companies an opportunity to share sensitive company information. ITAA has strict privacy guidelines and recommends the use of signed contracts embodying confidentiality agreements (non-disclosure) between firms when attributional data is involved. Members share information via non-secure e-mail. To be able to receive sensitive information, ITAA is structuring its Web site to receive encrypted information.

National Association of Broadcasters (NAB)

NAB is an international trade association that is composed of U.S. and non-U.S. based radio and television broadcasters. NAB also has extended membership to individuals and companies worldwide who provide products and services to electronic media industries.

The NAB's primary mission is to update and inform members of current and future legislative and regulatory actions that could affect the broadcast industry. The predominant form of information sharing within the NAB is exhibited in its grassroots lobbying activities. This form of lobbying allows for a high frequency of information sharing and allows members to learn successful lobbying techniques. Further, it strengthens NAB's lobbying success by giving it a greater voice before Congress.
NAB utilizes a journal, reports and newsletters, as well as conferences and seminars to update the membership of the NAB supported policy platforms. The membership is highly involved in

constructing the legislative and regulatory policy platform that the association will work to accomplish. Notably, NAB has no formal procedure for establishing nondisclosure agreements between members, due in part to the nature of the information that is shared.

Personal Communications Industry Association (PCIA)

PCIA is a national trade association representing providers of wireless and data communications. PCIA member companies include PCS licensees, paging providers, SMR, enhanced SMR (ESMR), mobile data, cable, computer, manufacturing, and local and inter-exchange sectors of the industry, as well as technicians, wireless systems integrators, communications site owners, distributors and service professionals, and private corporate system users.

PCIA's mission is to advance regulatory policies, legislation, and technical standards to aid in the launch of personal communications services. PCIA's membership makes decisions regarding the association's legislative and regulatory policy platform. The association utilizes information sharing within the realm of its lobbying activities, as well as in the production of its newsletters and Internet publications. PCIA also sponsors a number of conferences and trade shows where members can discuss new technologies and form partnerships for future system collaborations.

PCIA has an Internet site that provides members with a medium for information sharing. The site includes wireless news, as well as information about member companies and certain issues PCIA is closely following or supporting. The site also includes an on-line library, known as the Wireless Resource Center (WRC), which provides valuable information about the wireless industry and current trends facing member companies.

Telecommunications Industry Association (TIA)

TIA is a national trade organization with a membership of 1,000 companies that provides communications and information technology products, materials, systems, distribution services, and professional services in the United States and around the world. TIA represents their membership on issues regarding domestic and international issues before Congress, Federal Communications Commission (FCC), National Telecommunications and Information Administration (NTIA), and other Federal and international agencies.

TIA employs the greatest amount of information sharing within its structured committees and trade show forums. These committees and conventions allow members to interact with regard to public policy, standards, and market-development issues. The association also provides its members with a forum for the examination of global industry issues and information. TIA distributes to its members a journal, newsletters, and numerous reports regarding issues that affect the future of its industry. Because of the nature of the information shared, typically there is no formal procedure for establishing nondisclosure agreements among members.

United States Telephone Association (USTA)

USTA is an association composed of 1,200 member companies consisting of local exchange carriers and telecommunications technology companies. USTA's mission is to collect information and provide a forum for its members to discuss and resolve technical, regulatory, and other issues of mutual concern. USTA members share information that is of a regulatory or technical nature.

USTA is structured in a committee system, based on subject matter, in order to place member companies in forums where their expertise can assist other members. Members work within their committees and at USTA-sponsored seminars and conferences to share information about technical advances within the industry. Members also use the committee structure to manage or respond to new Government regulations.

USTA uses numerous reports and newsletters as well as conferences and seminars to inform members of basic technological advances and general information.