GUIDE TO UNDERSTANDING THE NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS AND THE NETWORK SECURITY INFORMATION EXCHANGES

PREPARED BY
THE OFFICE OF THE MANAGER,
NATIONAL COMMUNICATIONS SYSTEM

MARCH 2001

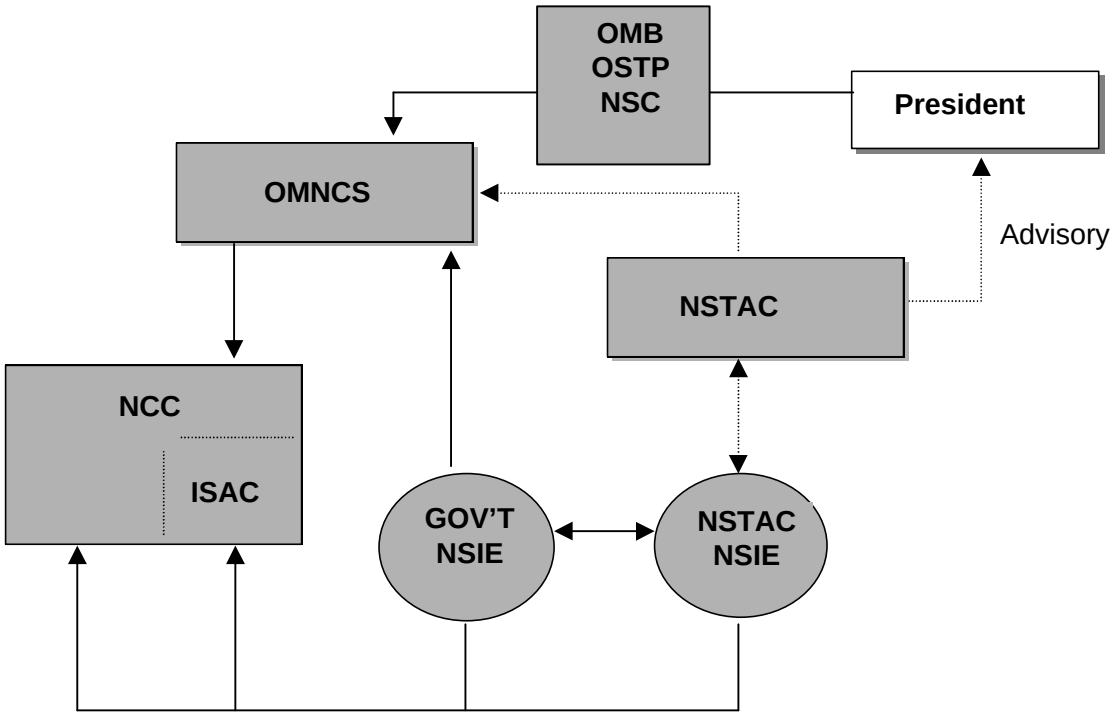
TABLE OF CONTENTS

1. DOCUMENT BACKGROUND

In November 2000, members of the National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee (IES) expressed concerns regarding the National Coordinating Center for Telecommunications (NCC) operations, its role as an Information Sharing and Analysis Center (ISAC), and its relationship with the Government and NSTAC Network Security Information Exchanges (NSIEs). The NCC-ISAC/NSIE Roles and Responsibilities Ad Hoc Group was established to address IES concerns. The Ad Hoc Group decided at its initial meeting to focus primarily on examining the interactions between the NCC-ISAC and the NSIEs to identify opportunities to enhance the Government/industry partnership in the national security and emergency preparedness (NS/EP) operational environment. Through briefings on the NCC, its ISAC function, and the NSIEs, the Ad Hoc Group gained an understanding of the respective entities and their relationships. The Ad Hoc Group also reviewed the status of NSTAC conclusions and recommendations related to the NCC. Appendix A captures those conclusions and recommendations and provides an update on their status. After considering all this input, the Ad Hoc Group concluded that a guide to understanding the NCC and the NSIEs should be prepared by the Office of the Manager, National Communications System (OMNCS).

2. DOCUMENT PURPOSE

The purpose of this document is to serve as a single, accessible document that provides background information about the NCC, its ISAC function, and the NSIEs, and describes their relationships. To fully understand the NCC and the NSIEs, it is necessary to understand the relationships each entity has with the NSTAC and the OMNCS.



The NSTAC advises the President on NS/EP telecommunications issues. The OMNCS serves as Secretariat to the NSTAC. In addition, the OMNCS coordinates joint Government/industry NS/EP telecommunications planning and therefore is often responsible for implementing actions that result from the President's acceptance of NSTAC recommendations. Government and industry participate in both the NCC and the NSIE processes. In addition, the NCC and the NSIEs each have a relationship with the OMNCS. The OMNCS operates and staffs the NCC. NCC operations and day-to-day activities are supervised by the Manager and Deputy Manager, NCC, who report to the Operations Division Chief, the Deputy Manager, and Manager, NCS. The OMNCS also chairs the Government NSIE and provides secretariat support to both the Government and NSTAC NSIEs.

For several years, beginning in 1997, the NSTAC's Operations Support Group (OSG) and its NCC Vision and NCC Vision-Operations Subgroups have examined NCC operations and provided conclusions and recommendations to enhance the NCC's operational capabilities. Appendix A is an overview of

NSTAC OSG conclusions and recommendations related to the NCC. In some instances, NSTAC conclusions and recommendations supported or contributed to Government action to address related issues. NSTAC also provides operational oversight to the NSTAC NSIE.

3. NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS

At a series of meetings in 1982, Government and industry identified a need for an authoritative entity to coordinate initiation and restoration of NS/EP telecommunications services. This requirement led to the development of the concept of a National Coordinating Mechanism (NCM). In February 1983, the IES convened a meeting of the NSTAC's Emergency Response Procedures Working Group (ERPWG) to address the NCM. The ERPWG, in turn, established an NCM Task Force to evaluate alternative NCM concepts. The task force made a recommendation to the NSTAC and subsequently to the President that a Government and industry-staffed NCC be created as the operational arm of the NCM.[1]

Under the framework of Executive Order (E.O.) 12472, *Assignment of NS/EP Telecommunications Functions,* the NCC, a joint Government/industry staffed body, was established on January 3, 1984.

The NCC mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities.

The NCC's primary focus is the NS/EP telecommunications[2] service requirements of the Federal Government. However, the NCC also has access to the status of all essential telecommunications facilities, including public networks (PN).[3]

Traditionally, the NCC has supported and coordinated responses across a broad spectrum of events. Since its inception in 1984, the NCC has shared information on telecommunications outages to expedite restoral in an "all hazards" environment. Initially, "all hazards" generally referred to international crises, acts of war, and natural disasters. As technology has migrated toward, and become increasingly dependent on, automated information systems, the concept of "all hazards" has expanded to include the electronic intrusion threat to operations, administration, maintenance, and provisioning (OAM&P) systems supporting NS/EP telecommunications.

In response to this changing environment, the NCC has expanded its operations to address cyber hazards. Following the approach for addressing critical infrastructure protection set forth in Presidential Decision Directive (PDD) 63:

[1] See *NCM Implementation Plan*, January 1984, for additional details on the NCM concept.
[2] Telecommunications, in this context, refers to any transmission, emission, or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. [T1 American National Standard for Telecommunications, *Telecommunications Glossary 2000*, http://www.itsbldrdoc.gov/projects/telecomglossary2000/]
[3] NCC Operating Charter, Section 1, Scope of Operations.

Protecting America's Critical Infrastructures,[4] the NCC implemented an ISAC function to share information on significant physical and cyber events affecting the telecommunications infrastructure, which includes organizations, personnel, procedures, facilities, and networks employed to transmit and receive information by electrical or electronic means.[5] Information related to telecommunications outages, attempted or actual penetration or manipulation of databases, PN intrusion incidents and outages, and significant abnormal events or anomalies in operational activity that may indicate a coordinated attack are shared through the ISAC function.

To assist the Government in meeting NS/EP telecommunications service requirements, the NCC performs or contributes to the performance of the following functions—

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

[4] PDD-63 called for the Government to consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector ISAC that could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the National Infrastructure Protection Center (NIPC). The center could also gather, analyze, and disseminate information from the NIPC for further distribution to the private sector. This mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the Government. (White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: PDD-63, May 22, 1998). Since PDD-63 was issued several ISACs have been established across the spectrum of critical infrastructures.

[5] Op. cit., *Telecommunications Glossary*.

- Coordinate, direct, and expedite the initiation of NS/EP telecommunications services

- Contribute to the development of technical standards and national network planning, and ensure application of those standards and dissemination of those plans to facilities serving NS/EP needs

- Coordinate and direct network reconfiguration plans in support of NS/EP needs. In performing these functions, the NCC monitors the status of all essential telecommunications facilities, including the public switched networks.[6]

3.1 Membership

The NCC is composed of U.S. Government and telecommunications industry members. Both Government and industry have resident and nonresident representatives. As defined in the NCC Operating Charter[7]:

- Resident representatives are physically present in the NCC on a regular basis and routinely participate in NCC activities and operations.

- Nonresident representatives function as a liaison to the NCC and are physically present in the NCC on a periodic basis. They are the routine NCC point of contact (POC) within their parent entity and may be called on to perform duties in the NCC in support of emergency situations.

Government presence in the NCC is provided by representatives of NCS member departments, agencies, and entities that have significant NS/EP responsibilities or whose operations are heavily dependent on communications provided by the U.S. commercial telecommunications industry. Government participants are selected using criteria such as: the department or agency's level of NS/EP telecommunications involvement (indicators include number and level of restoration priority circuits, and level of responsibility for, and participation in, E.O. 12472 activities), whether the department or agency is a Category A agency,[8] and whether the department or agency has communications assets. Government entities provide individuals to staff and support NCC operations.

[6] NCC Operating Charter, Section 3, Functions of the NCC.
[7] NCC Operating Charter, Section 2, Participation in the NCC.
[8] As defined by the Federal Emergency Management Agency (FEMA) Preparedness Circular No. 60.

Table 1: NCC Government Members[9]

Resident	Nonresident
Department of Defense (DOD)	Defense Information Systems Agency (DISA)
Department of Justice (DOJ)	Department of Commerce (DOC)
Department of State (DOS)	Federal Communications Commission (FCC)
General Services Administration (GSA)	Federal Emergency Management Agency (FEMA)

Memorandums of agreement state the arrangements whereby entities will provide personnel to the NCC. Government departments, agencies, and entities enter into agreements with the Secretary of Defense, as Executive Agent for the NCS, or his designee. In addition to resident and nonresident NCC representatives, Government entities may also detail individuals to the OMNCS in support of the NCC and other programs.

U.S. telecommunications industry presence in the NCC is provided by commercial entities. Entities are selected by the OMNCS in accordance with participation criteria such as the entity's ability and willingness to provide or support the provision of NS/EP telecommunications service requirements; whether the entity provides a portion of a circuit bearing an NCS/FCC approved restoration priority of 1-4;[10] or whether the entity is important to an effective industry response to NS/EP telecommunications service requirements.

Table 2: NCC Industry Members[11]

Resident	Nonresident
AT&T	Cisco Systems
BellSouth[12]	Computer Sciences Corporation (CSC)
ITT Industries	Electronic Data Systems (EDS)
Qwest	Lockheed Martin
SBC Communications[13]	Nortel Networks
Verizon	Science Applications International Corporation (SAIC)
WorldCom	Sprint
	USTA

Government and industry share the costs associated with operating the NCC. Government pays for some costs directly related to operating the NCC. Industry also voluntarily bears some of the costs of participating in the NCC. As a result, the number of NCC members must be commensurate with Government

[9] As of March 1, 2001.
[10] For a description of these priority levels, see the TSP Service User Manual (NCSM 3-1-1), http://tsp.ncs.gov/tsp/documents/html.
[11] As of March 1, 2001.
[12] The National Telecommunications Alliance (NTA) was an NCC member; however, following NTA's dissolution in December 2000, some companies that had been represented by NTA are now participating directly in the NCC.
[13] Ibid.

resources available to manage and operate the NCC. This has the potential to limit the number of resident representatives in the NCC; however, through nonresident representatives or the ISAC function the NCC can expand its membership and access to other NS/EP telecommunications providers.

NCC Government and industry representatives draw on the resources of their individual companies and departments and agencies when the NCC responds to an emergency or crisis situation. For the most part, NCC Government and industry representatives act as coordinators; all representatives know where to go within their respective corporations and departments and agencies to get the information and expertise necessary to resolve problems and to direct commitment of resources.

3.2 Responsibilities of NCC Representatives

The responsibilities of NCC Government and industry representatives fall into three categories:

- Joint Responsibilities: Responsibilities that both Government and industry representatives perform.

- Parallel Responsibilities: Responsibilities that are similar for both Government and industry representatives.

- Complementary Responsibilities: Responsibilities that are different for Government and industry representatives; however, their respective responsibilities complement each other.

The following table summarizes Government and industry responsibilities in each of the three general categories.

Table 3: Responsibilities of NCC Representatives[14]

Joint Responsibilities	
• Assist in developing scenarios for exercises to ascertain the adequacy of telecommunications plans and resources to support NS/EP requirements • Participate in evaluating the response to communications emergencies, results of exercises, or response to other emergencies or disasters.	
Parallel Responsibilities	
Government	**Industry**
• Maintain interfaces with Government operations centers • Maintain access to databases containing information concerning facility and network status for Federal Government telecommunications systems	• Maintain interfaces with respective operations centers • Assure access to appropriate databases to monitor the service status of their corporate networks and facilities
Complementary Responsibilities	
Government	**Industry**
• Assist in control and management of national communications assets • Coordinate with industry representatives on NS/EP telecommunications requirements • Work with industry on a day-to-day basis to develop operational plans, procedures, and guidelines	• Serve as POC for expediting restoration or initiation of NS/EP telecommunications services • Consult with and provide advice to Government in developing alternative approaches for response to NS/EP telecommunication requirements • Have ready access to the authority to make decisions and direct the use of corporate resources to fulfill NS/EP requirements

3.3 ISAC Function

In 1998, the NCC's operations were expanded in response to an NSTAC recommendation to include the development of an indications, assessment, and warning (IAW) capability. The NCC conducted a 120-day trial of the IAW Center pilot that focused on reporting cyber events, a category of hazard that had not previously fallen within the normal thresholds of operational activity monitored and addressed by NCC representatives. Following the IAW Center pilot, the NCC decided to fully incorporate the IAW function into its operations.[15]

In June 1999, the NSTAC concluded that the NCC performs the primary functions of an ISAC for the telecommunications infrastructure as outlined in PDD-63.[16] The NCC's development of an IAW capability was a key factor

[14] NCC Operating Charter, Section 2.
[15] See NSTAC OSG Report to NSTAC XXII, June 1999 for additional information on the IAW Center pilot.
[16] NSTAC, OSG Report to NSTAC XXII, June 1999.

leading to this conclusion. The NSTAC and NCC also concluded that the NCC Operating Charter was broad enough to encompass the ISAC function.[17] On January 18, 2000, the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism signed a memorandum agreeing with the conclusion and supporting the decision by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to designate the NCC as an ISAC for telecommunications.

The ISAC and the NCC are not separate entities; rather, the ISAC is one of the NCC's functions. The ISAC function supports not only the mission assigned to the NCC as mandated by E.O. 12472 (1984), but it also supports the national critical infrastructure protection goals of Government and industry as identified in PDD-63 (1998) and the National Plan for Information Systems Protection[18] (2000).

The NCC-ISAC —

- Facilitates voluntary collaboration and information sharing among its participants
- Gathers information on vulnerabilities, threats, intrusions, and anomalies from the Government, the telecommunications industry, and other sources
- Analyzes the data with the goal of averting or mitigating impact on the telecommunications infrastructure
- Establishes baseline statistics and patterns
- Maintains a library of historical data, and
- Sanitizes and disseminates results in accordance with sharing agreements established among the NCC-ISAC participants.[19]

3.3.1 Focus of ISAC Operations

Just as the NCC responds to "all hazards" with the potential to affect NS/EP telecommunications services or facilities, the ISAC focuses on collecting, analyzing, and sharing information about all such hazards (physical and cyber). Hazards may appear as outages, anomalies, or other events or incidents, including a coordinated attack, in any of the systems that constitute or support the national telecommunications infrastructure. The primary goal of the NCC-ISAC is to analyze reported events and symptoms as rapidly as possible to avert

[17] Ibid.
[18] National Plan for Information Systems Protection: An Invitation to a Dialogue, Version 1.0, January 7, 2000. http://www.ciao.gov/National_Plan/national_plan%20_final.pdf
[19] NCC-ISAC Concept of Operations, Version 1.0, May 1, 2000.

or minimize impending damage to telecommunications operations. The secondary goal is to establish causes after the fact in order to prevent future recurrences.[20]

It is anticipated that ISAC operations will include real-time analytic capabilities. Requirements necessary to achieve this and data points to be considered for analysis will be defined over time. NCC operations are evolving to fully implement the ISAC function. Plans, policies, procedures, and tools are being developed to support ISAC operations. For example, the NCC is developing the Information Sharing and Analysis System (ISAS), which includes a database to facilitate the collection and dissemination of information. In addition, as part of the ISAS development, analytical tools are being developed to support processing and correlation of data. (See Section 3.4 for additional information regarding the ISAS.)

3.3.2 ISAC Participants

Initial participants in the NCC-ISAC include all NCC Government and industry members, both resident and nonresident. There are four levels of ISAC participation:

- NCC Member,
- NCC-ISAC Participant,
- NCC-ISAC Subscriber, and
- Public Domain.[21]

Each level of participation requires the entity to meet certain criteria and fulfill certain obligations. Access to ISAC information varies based on the entity's participation level.

[20] Ibid.
[21] NCC-ISAC, Criteria for Participation in the NCC-ISAC, June 28, 2000.

Table 4: Overview of ISAC Participation Levels, Criteria, Requirements, Information, and Obligations

Level	Criteria	Requirements	Information	Obligations
NCC Member	NCC Government or industry membership	NCC membership and Information Sharing Agreement (ISA)	Unclassified, classified,[22] threat/intelligence, ISAS database, e-mail warnings, and public release information	Contribute to the NCC-ISAC function and interact with the ISAS database on a regular basis.[23]
NCC-ISAC Participant	Companies that provide network services, equipment, or software to the information and communications (I&C) sector or are Government NS/EP users	ISA	Unclassified, classified,[24] threat/intelligence, ISAS database, e-mail warnings, and public release information	Contribute to the NCC-ISAC function and interact with the ISAS database on a regular basis.[25]
NCC-ISAC Subscriber	Entities that participate or have a presence in the I&C sector (e.g., telecommunications professionals, telecommunications organizations, and State and local governments)	Subscription form and letter of recommendation from an existing NCC Member or NCC-ISAC Participant	E-mail warnings and public release information	None
Public Domain	Individuals and/or organizations with public access to the Internet[26]	None	Public release information	None

Any NCC member, NCC-ISAC Participant, or NCC-ISAC Subscriber can nominate a new candidate for participation. In addition, any entity can apply for participation in the NCC-ISAC by submitting a request to the Manager, NCC, for consideration by the Manager, NCS. Candidates for participation in all levels will be considered based on the value they bring to the overall operation of the NCC-ISAC.[27] The expansion of NCC operations to include the ISAC function allows the NCC to more widely reflect the composition of the telecommunications industry. The ISAC function encourages participation by companies within the information and communications sector that are not presently represented in the NCC.

[22] If appropriately cleared.
[23] Op. cit., Criteria for Participation in the NCC-ISAC.
[24] If appropriately cleared.
[25] Op. cit., Criteria for Participation in the NCC-ISAC.
[26] The Public Domain level of participation is designed to meet Government's requirement to provide information to the public.
[27] Op. cit., Criteria for Participation in the NCC-ISAC.

3.4 Information Handling

Traditionally, Government and industry information has been shared with the NCC using whatever means necessary to ensure the delivery of the information. These means include transmittal via public-line telephone, e-mail, or in person through resident Government and industry representatives. From time to time the NCC deals with classified information, which is handled in accordance with Government classification procedures.

The ISAS allows for formal reporting of information under the ISAC function. A prototype has been developed using a secure, Web-based system that serves as a repository for collecting and disseminating information from participants in near-real-time. Participants can share information through various mechanisms, including a structured ticket containing specific fields and information, a threaded message forum that allows free-form discussion and exchange of information, and NCC-issued advisories that alert participants of significant events or information.[28]

Information handling procedures are based on information sharing agreements, which reflect the desires of each participating organization regarding how its information may be shared with others (e.g., what information can be shared and with whom it can be shared). The NCC-ISAC Concept of Operations establishes an operational process flow based on these information sharing agreements; the ISAS is designed to enforce these agreements. The NCC-ISAC will provide no information to any entity not authorized by a sharing agreement to receive the information. These information handling procedures apply to protection of the original submitted data and all derivative products resulting from analysis or correlation, whether contained in the ISAS or not.

3.5 Value

The NCC was established as a result of the NSTAC's first recommendation to the President. With the divestiture of AT&T in 1982, the Federal Government no longer had a single POC to provision and restore critical telecommunications needed to prepare for, or respond to, natural and manmade disasters or a national security emergency or crisis. The NSTAC recommended the creation of an NCM, which resulted in the establishment of the NCC. The industry's sustained contribution to the NCC since 1984 reflects its commitment to good corporate citizenship. Although this is a significant benefit to Government, this joint Government and industry partnership has also been helpful to industry, particularly with regard to ensuring the availability of telecommunications services critical to both Government and industry.

[28] Additional information on the ISAS can be found in the NCC-ISAC Implementation Plan, and the ISAS Functional System Description and ISAS Data Set Description documents available through the NCS.

Just as technologies have evolved, the threat has changed. The NCC has adapted to meet changing technologies and threats by creating the ISAC function, which focuses on gathering a broader range of information than was required previously to respond to crises and threats. Fulfillment of the ISAC function allows the NCC to gather and analyze the information needed to enhance the NCC's other key function—response and restoration. Value is derived by individual participation in the information sharing process.

The NCC, with its ISAC function, is uniquely positioned to address all hazards affecting NS/EP telecommunications. The NCC has almost 20 years of experience in coordinating response, recovery and restoration of telecommunications services. Over that time, it has developed a number of operational capabilities and tools for response, recovery, and restoration, and has conducted exercises and training to continually refine those capabilities and tools. In addition, its history of sharing classified Government and sensitive industry information has provided the basic foundation, processes, procedures, tools, and infrastructures for serving as the ISAC for the telecommunications infrastructure.

4.0 NETWORK SECURITY INFORMATION EXCHANGES

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, identify what action should be taken by 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 the NSC tasking, the Manager, NCS and the NSTAC established separate, but closely coordinated, NSIEs. In May 1991, the NSIE charters were finalized, and Government departments and agencies and NSTAC companies designated their NSIE representatives, chairmen, and vice-chairmen. The first joint meeting of the Government and NSTAC NSIEs was held in June 1991.

The Government and NSTAC NSIEs meet jointly approximately every two months. The NSIEs provide a working forum to identify issues involving penetration or manipulation of software and databases affecting NS/EP telecommunications. The NSIEs share information with the objectives of:

- Learning more about intrusions into and vulnerabilities affecting the PN
- Developing recommendations for reducing network security vulnerabilities
- Assessing network risks affecting network assurance
- Acquiring threat and threat mitigation information
- Providing expertise to the NSTAC on which to base network security recommendations to the President.

To support this effort the OMNCS developed and maintains a database of known network security vulnerabilities. This database tracks vulnerabilities derived from multiple sources, including reports from NSIE representatives, Government-sponsored operations centers (e.g., Computer Emergency Response Team Coordination Center [CERT/CC], Department of Energy's Computer Incident Advisory Capability [CIAC], Department of Defense CERT), and open sources (e.g., Bugtraq). Information contained in the database on known vulnerabilities is scrubbed to ensure that the reporting entity cannot be identified and is made available to NSIE representatives through a bulletin. The database includes vulnerabilities dating from January 1, 1989.

The operational time frame of the NSIEs is not generally real-time. The original NSIE Charters had envisioned a real-time operational response function; however, the NSTAC NSIE recommended that the response function be dropped because it implied that the NSIEs had some authority over network response and recovery. Although individual representatives may have operational responsibilities within their own companies or Government departments and agencies, the NSIEs as organizations do not.

The priority for representatives is to first protect and maintain their own networks, and then communicate with other NSIE representatives. Although most often NSIE representatives share their information at the bimonthly meetings, events occur that warrant a more rapid response and representatives communicate with each other on an ad hoc basis between meetings. Through personal contacts, telephone, and e-mail, NSIE representatives have developed an informal, accelerated information sharing capability. Such event driven communication allows Government and industry representatives to collaborate to rapidly contain, respond to, and recover from an incident, mitigating the impact of the incident. In addition, relationships with NSIE representatives provide Government with industry POCs to confirm events in real-time. For example, during Solar Sunrise and the Melissa and I Love You viruses, Government turned to the NSTAC NSIE to confirm events and discuss mitigation techniques.

4.1 Membership

The two NSIEs—the Government NSIE and the NSTAC NSIE—each have separate charters and memberships. Government NSIE members include departments and agencies that are NS/EP telecommunications service users, represent law enforcement, or have information relating to network security threats and vulnerabilities. Government NSIE membership was originally established by a Government Network Security Subgroup under the Manager, NCS. NSTAC NSIE representatives include subject matter experts who are engaged in prevention, detection, and/or investigation of telecommunications software penetrations or have security and investigative responsibilities. NSTAC companies wishing to participate in the NSTAC NSIE are approved by the IES. The current membership in the Government and NSTAC NSIEs is shown in the following table.

Table 5: Government and NSTAC NSIE Membership[29]

GOVERNMENT NSIE	NSTAC NSIE
Central Intelligence Agency	AT&T
Defense Intelligence Agency	Bank of America
DISA	BellSouth[30]
DOD	Boeing
DOJ	CSC
Federal Bureau of Investigation	EDS
FCC	Executive Security & Engineering Technologies
NIPC	ITT Industries
National Institute of Standards & Technology	Lockheed Martin
National Security Agency	Lucent
OMNCS	Nortel Networks
United States Secret Service	Qwest
	Raytheon
	SAIC
	SBC Communications[31]
	Sprint
	Telcordia
	Verizon
	WorldCom

NSTAC NSIE membership consisted of ten companies when the NSIEs were established in 1991. Membership was intentionally limited by the IES because the IES understood the importance of developing trust among member organizations. In 1995, two additional companies were added—Boeing and Bank of America—to determine the effect membership expansion would have on NSIE operations. Expansion did not have a negative effect on operations, and as a result, in 1997, NSIE membership was opened to any NSTAC company that wanted to join. Eleven additional companies chose to join; however, some never designated a representative, and others have participated only sporadically. In addition, NSIE representatives periodically invite guests to attend meetings and observe the NSIEs in action in return for briefings on the guest's security-related activities. In two cases, Carnegie Mellon's CERT/CC and Mitre, guests have been given permanent invitations to attend and participate based on their value and contributions to the NSIE process. Although increased membership did not erode the trust or destroy the ability of the NSIEs to share information, NSIE representatives continue to be concerned that the NSIE model may not work with a much larger membership.

[29] As of March 2001.
[30] NTA was an NSTAC NSIE member; however, following NTA's dissolution in December 2000, some companies that had been represented by the NTA are now participating directly in the NSTAC NSIE.
[31] Ibid.

Government NSIE membership was initially limited to ten departments and agencies; however, because GSA and the FCC declined, at the time, to sign the nondisclosure agreement they did not initially participate in meetings. The FCC subsequently signed the nondisclosure agreement. GSA is currently reconsidering its decision not to sign the nondisclosure agreement so that it may participate. In 1997, DOJ and DOE asked to join the Government NSIE and both were added to the membership. DOJ has participated sporadically since joining. DOE never signed the nondisclosure agreement and did not designate a representative.

Original NSIE member organizations had two seats in the NSIEs; however, due to concern about making NSIE meetings too large, members added in 1997 were allowed only one seat. Each organization decides whether to designate technologists or generalists as representatives. Representatives bring not only their first hand knowledge to NSIE meetings, but they have access to a variety of additional information sources in their organizations on which they draw to share information.

4.2 Responsibilities of NSIE Representatives

Representatives voluntarily share information related to threats, incidents, and vulnerabilities affecting OAM&P systems supporting the telecommunications infrastructure. This information includes attempted or actual penetrations or manipulations of software, databases, and systems related to critical NS/EP telecommunications. In addition, representatives share information on physical intrusions pursuant to attacking these assets. NSIE representatives are expected to voluntarily share the following information:

- 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 (e.g., viruses, worms, and Trojan horses)
- Hacker skills, tools, or new methods of attack
- Threats to the PN
- Security policies, processes, and procedures found to be useful in mitigating significant security risks

- Problems with the potential to affect the availability, confidentiality, or integrity of infrastructure systems

- New or ongoing law enforcement cases regarding intrusions into communications and information system networks

- New or significant changes to existing laws, regulations, and standards relating to or affecting network and information security

- Information on security products or tools.

4.3 Information Handling

NSIE 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 U.S. SECRET security clearances. The sharing of NSIE information is categorized in three levels: N-1, N-2, and N-3.

Table 6: NSIE Information Sharing Levels

• **Level N-1:** Information can be shared with only other NSIE representatives.
• **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.
• **Level N-3:** Information can be shared beyond NSIE member organizations.

Most information sharing in meetings is conducted at the N-2 level. N-3 sharing normally takes place through NSIE documents that are broadly disseminated and NSIE-sponsored white papers and workshops (e.g., the Insider Threat Workshop). In addition, the NSIEs periodically produce a risk assessment of the PN highlighting technological developments that may have the potential to affect network security. NSIE representatives also use a secure Web site to post meeting announcements, meeting summaries, action items, and information of interest to other representatives.

Nondisclosure agreements and different levels of information sharing provide members some protection from unauthorized disclosure when sharing information. However, the critical factor that fosters information sharing within the NSIEs is the trust among the NSIE representatives themselves.

4.4 Value

The NSIEs help to bridge Government and industry. When the NSIEs were first established in 1991, Government advocated avoiding risk at whatever the cost to Government or industry. As Government and industry representatives began to interact more closely through forums such as the NSIEs, Government developed an understanding of industry's concerns. Industry is interested in striking a balance between risk and cost so as to ensure a return on their investment. As a result, NSIE industry members are interested in risk management rather than risk avoidance. Industry's primary interest in improving the bottom line is greatly aided by better managing the risk to their networks. Prevention and detection enable NSIE representatives to improve the security of their individual networks and reduce the level of risk. However, industry must balance the cost of implementing prevention and detection capabilities with the potential risk if no action is taken. NSIE participation affords member companies a more comprehensive view of the environment in which they operate. Likewise, access to the experiences of other companies provides new and different perspectives for handling an incident or vulnerability or making other security decisions.

Often the vulnerabilities facing industry are the same as those facing Government. Participation in the NSIEs gives Government departments, agencies, and entities information on known vulnerabilities and insights into how industry detects and responds to intrusions and incidents affecting the PN. Government departments, agencies, and entities can use this information to ensure that Government systems and networks are more secure. In addition, participation in the NSIEs provides Government with a POC in industry that can confirm events, vulnerabilities, and mitigation strategies.

Membership in the NSIEs is an organizational decision. Participation is an individual decision. If the individual assigned to represent an organization does not see value in the NSIEs, he/she will be unwilling to make the personal commitment to attend and participate. When individuals stop participating in the NSIEs, some organizations designate new participants and others simply stop participating.

5.0 SUMMARY

Although having the same general objective (i.e., ensuring adequate NS/EP telecommunications services) the NCC and the NSIE have different, but complementary, characteristics in terms of focus, time frame, skill sets, products, and value. The following table summarizes the key features of the NCC, its ISAC function, and the NSIEs.

Table 7: Key Features of the NCC and the NSIEs

Characteristic	NCC (NCC-ISAC)	NSIE
Focus	Response & Restoration All hazards (e.g., natural and manmade disasters, and cyber and physical attacks)	Protection & Deterrence Threats to and vulnerabilities of networks and the OAM&P systems supporting the telecommunications infrastructure
Time frame	Near real-time/real-time	Post-event/Ad hoc real-time
Skill sets	Policy and coordination	Technologists, security experts
Products	Alerts, bulletins, after-action reports	Assessments of the risks to networks and OAM&P systems supporting the telecommunications infrastructure; workshops; white papers
Value	Warning, response assistance	Lessons learned, prevention

As described earlier, the NCC focuses on near real-time operational response to all hazards. The NSIEs focus on post-event analysis of threats to and vulnerabilities of networks and the OAM&P systems supporting the telecommunications infrastructure and on general sharing related to establishing an effective security program. From time to time, Government and NSTAC NSIE representatives communicate in real-time on an ad hoc basis depending on the event or incident.

Although the same companies and departments and agencies may participate in both the NCC and the Government and NSTAC NSIEs, the representatives are usually not the same individuals. Furthermore, NCC and NSIE representatives may represent different perspectives within their organizations. For example, NCC representatives, for the most part, act as POCs and help allocate, coordinate, and expedite resources to support response activities. NSIE representatives are in most cases technical subject matter experts involved in

preventing, detecting, and responding to events within their respective organizations.

The NSIEs and the NCC routinely share information. The NSTAC NSIE Charter operating principles state that:

> *to the maximum extent possible within the constraints of the nondisclosure agreement, information shared by the NSIE will be provided to the NCC in its role as an IAW center (now known as the NCC-ISAC) for the telecommunications industry.*

There are several ways the NCC, its ISAC function, and the NSIEs share information with each other:

- An NCC representative participates in NSIE meetings and has access to all NSIE information, including NSIE bulletins and vulnerability database reports.

- The NCC forwards incident reports and requests for special technical expertise or analysis, consolidated incident reports, or any previously agreed on reports to the NSIEs.

- The NCC gives the NSIEs information from other sources, including the NIPC, CIAC, and the Federal Computer Incident Response Center.

Participation in the NCC, its ISAC function, and the NSIEs enables participants to interact with one another and exchange valuable information, and also gives them access to a variety of external information sources. Access to these information sources is made possible both through organizations and individual representatives. The relationship between the NCC and the NSIE has evolved and will continue to do so as the political and technological environment change.

APPENDIX A

OVERVIEW OF NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE OPERATIONS SUPPORT GROUP CONCLUSIONS AND RECOMMENDATIONS RELEVANT TO THE NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS[32]

A.1 Operations Support Group (OSG) Report to National Security Telecommunications Advisory Committee (NSTAC) XX, December 1997

National Coordinating Center for Telecommunications (NCC) Vision Subgroup Conclusions[33]

The subgroup concluded that the NCC can implement an initial intrusion incident processing capability, but more study is needed to fully integrate an initial intrusion incident information processing function into the NCC. The NCC is envisioned to serve as a focal point for receiving, screening, and processing electronic intrusion incident information for Government and industry telecommunications service providers and network operators.

NCC Vision Subgroup Recommendations[34]

Recommendation for the President: The President establish a mechanism within the Federal Government with which the NCC can coordinate intrusion incident information issues and with which NSTAC groups can coordinate the development of standardized reporting criteria.

STATUS: NSTAC approved the OSG's NSTAC XX report and submitted the recommendation to the President.

Recommendation for the NSTAC: The NSTAC endorse NCC implementation of an initial intrusion incident information processing pilot based on voluntary reporting by Government and industry.

STATUS: NSTAC endorsed this recommendation. The pilot was initiated on June 15, 1998, and completed in October 1998.

---

[32] The NSTAC's Industry Executive Subcommittee (IES) tasked the NCC-ISAC/NSIE Roles and Responsibilities Ad Hoc Group to determine as part of its effort the status of NSTAC conclusions and recommendations related to the NCC.

[33] NSTAC, OSG Report to NSTAC XX, December 1997, Section 3.1.2, p. 4.

[34] NSTAC, OSG Report to NSTAC XX, December 1997, Section 4.1, pp. 6-7.

Recommendations for the Industry Executive Subcommittee (IES):

- The IES extend the Vision Subgroup tasking into the next NSTAC cycle
- The IES approve the revised Section 2.0 and Section 3.0 of the *NCC Operational Guidelines.*

STATUS: The NCC modified its standard operating procedures to accommodate an electronic intrusion incident information processing capability.

Related Event: **In May 1998, Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures*, was released.**

A.2 OSG Report to NSTAC XXI, September 1998

National Coordinating Mechanism (NCM) Concept Conclusions[35]

Because the Government is continuing to establish an information reporting structure, the NCM concept cannot be finalized at this time. However, experience within NSTAC indicates that more than one individual may be required to adequately represent each critical infrastructure sector.

The NCC provides a model, which is currently being examined to provide cyber indications, assessment, and warning (IAW), through which several telecommunications companies have found it worthwhile to provide, at their own expense, personnel to work with the Government in facilities provided by the Government. It can provide a model for cooperation and the gathering, analyzing, sanitizing, and disseminating of information that can be scaled appropriately to fit the other critical infrastructures.

Related Event: **Three industry organizations were selected to represent the Information and Communications sector: Information Technology Association of America, United States Telecom Association, and Telecommunications Industry Association.**

[35] NSTAC, OSG Report to NSTAC XXI, September 1998, Section 3.1.2, p. 3.

NCM Concept Recommendations[36]

Recommendations to the President: The President should direct the lead departments and agencies as designated in PDD-63 to—

- Establish a Government-industry coordinating activity to advise in the selection of a sector coordinator and provide continuing advice in order to effectively represent each critical infrastructure

- Consider adapting the NCC model as appropriate for the various critical infrastructures to provide warning and information centers for reporting and exchange of information with the National Infrastructure Protection Center through the NCM process.

Recommendation to the NSTAC: The NSTAC should task the IES to continue to refine the NCM concept in coordination with the designated Government departments and agencies developing critical infrastructure protection plans, processes, and procedures.

STATUS: NSTAC XXI approved the OSG report and forwarded the recommendations to the President.

NCC Vision-Operations Subgroup Conclusions[37]

The ongoing work of the electronic intrusion incident information pilot program, the NCC Year 2000 coordination study, and other ongoing efforts may reveal a requirement for expanded NCC capabilities.

NCC Vision-Operations Subgroup Intrusion Incident Reporting Criteria Recommendations[38]

Recommendation to the IES: The IES should task the OSG to review and make recommendations on the makeup of the NCC to accomplish its expanded mission, focusing on facilities, staffing, funding, support tools, and resources.

STATUS: Following NSTAC XXI, the OSG's NCC Vision-Operations Subgroup worked closely with the Office of the Manager, National Communications System, and the Manager, NCC, as the NCC continued its electronic intrusion incident processing function. The subgroup also continued to assist the NCC in evaluating any needed revisions to the IAW reporting criteria and format guidelines.

[36] NSTAC, OSG Report to NSTAC XXI, September 1998, Section 3.1.3, p. 3.
[37] NSTAC, OSG Report to NSTAC XXI, September 1998, Section 3.2.2, p. 4.
[38] NSTAC, OSG Report to NSTAC XXI, September 1998, Section 3.2.3, pp. 4-5.

The OSG's NCC Vision-Operations Subgroup assessed whether the NCC requires additional Government and industry participation within the NCC to widen the scope of expertise and operational personnel available to fulfill the IAW mission.

A.3 OSG Report to NSTAC XXII, June 1999

OSG Conclusions[39]

- The NCC IAW Center *(now known as the "NCC-Information Sharing and Analysis Center [ISAC]")* revised reporting criteria and process flow and their use as guidelines were found to be appropriate.

- To fulfill the NCC's enhanced mission, the Manager, NCS, should consider expanding participation in the NCC and invite additional participation deemed necessary. (Annex D to this report provides a list, developed through subgroup consensus, of companies and Government agencies and departments recommended for consideration by the Manager, NCS, as potential new NCC participants.)[40]

- The NCC today performs the primary functions of an ISAC for the telecommunications sector and the Manager, NCS, should complete the memorandum of understanding establishing it as such.

OSG Recommendations[41]

NCC Vision Subgroup—NSTAC Direction to the IES: The NSTAC directs the IES to continue to monitor the NCC's implementation of its IAW function and to help refine, in an evolutionary fashion, reporting criteria and guidelines that facilitate the performance of the IAW function in the NCC.

STATUS: The ISAC Concept of Operations, Version 1.0, was published on May 1, 2000. Subsequent documents, including functional requirements and data set descriptions for the Information Sharing and Analysis System (ISAS), a tool to facilitate the ISAC function, have been developed. An ISAS prototype is nearing completion.

Related Event: **In January 2000, the National Security Council agreed with the NSTAC's 1999 *conclusion* that the NCC was performing the primary functions of an ISAC and in March 2000, the NCC formally achieved initial operating capability as an ISAC for the telecommunications sector.**

[39] NSTAC, OSG Report to NSTAC XXII, June 1999, Section 3.2.1, p. 6.
[40] Annex D of the OSG Report to NSTAC XXII.
[41] NSTAC, OSG Report to NSTAC XXII, June 1999, Section 3.2.2, p. 6.

APPENDIX B

GLOSSARY

Attack—An intentional act of attempting to bypass one or more of the following security controls of an information system: nonrepudiation, authentication, integrity, availability, or confidentiality.[42]

Detection—Comparing normal patterns of behavior and identifying abnormalities that could be unauthorized activity; the process of identifying that an unauthorized activity has been attempted, is occurring, or has occurred.[43]

Event—An occurrence, not yet assessed, that may affect the integrity and performance of the telecommunications infrastructure.[44]

Incident—An assessed occurrence having actual or potentially adverse effects on the telecommunications infrastructure.[45]

Indication—Information that suggests that a threat to a system exists or may exist.[46]

Information Sharing and Analysis System (ISAS)—The systems and tools that will support the information sharing and analysis functions of the NCC-ISAC.[47]

Infrastructure—A framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.[48]

---

[42] *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, Revision 1, January 1999 (http://www.nstissc.gov/html/library/html).
[43] *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document*, 3rd Edition, Office of the Manager, National Communications System, March 1999.
[44] *National Coordinating Center for Telecommunications-Information Sharing and Analysis Center (NCC-ISAC) Concept of Operations (CONOPS)*, Version 1.0, May 1, 2000.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.

National Security and Emergency Preparedness (NS/EP)—Capabilities required to maintain a state of readiness or to respond to and manage any event or crisis that causes or could cause injury or harm to the population, damages or causes loss of property, or degrades or threatens the NS/EP posture of the United States.[49]

Near Real-Time—The brief period between the collection of data about an event and the receipt of the data at another location, during which time it is relayed and processed.[50]

Public Network (PN)—The PN supports virtually all NS/EP telecommunications and information system requirements. The PN includes any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched network, public data networks, private line services, wireless services, and signaling networks).[51]

Telecommunication—1. Any transmission, emission, or reception of signs, signals, writing, images and sounds, or intelligence of any nature, by wire, radio, optical or other electromagnetic systems. 2. Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems.[52]

Telecommunications Infrastructure—The organizations, personnel, procedures, facilities, and networks employed to transmit and receive information by electrical or electronic means. Note 1: Telecommunications facilities include, but are not necessarily limited to, terrestrial radio, metallic and optical fiber cables, artificial Earth satellite communications, radio and television stations (traditional broadcast as well as cable and satellite broadcast), public switched telephone network (s), etc. Note 2: Examples of advanced telecommunications infrastructure facilities are direct broadcast satellite, digital audio broadcasting, Advanced Digital Television, and the Global Positioning System, which is used extensively for precise navigation and timing.[53]

Threat—Capabilities, intentions, and attack methods of adversaries to exploit vulnerabilities of an information system, with a potential to cause harm in the form of destruction, disruption, and/or denial of service.[54]

---

[49] Op. cit., *The Electronic Intrusion Threat to NS/EP Telecommunications*.
[50] Op. cit., *NCC-ISAC CONOPS*.
[51] Op. cit., *The Electronic Intrusion Threat to NS/EP Telecommunications*.
[52] T1 American National Standard for Telecommunications, *Telecommunications Glossary 2000*, (http://www.its.bldrdoc.gov/projects/telecomglossary2000).
[53] Ibid.
[54] Op. cit., *The Electronic Intrusion Threat to NS/EP Telecommunications*.

Vulnerability—A weakness in system security procedures, system design, implementation, hardware design, or internal controls that could be exploited to violate system security policy.[55]

[55] Ibid.

APPENDIX C

RELATED DOCUMENTS AND REFERENCES[56]

1. *The Clinton Administration's Policy on Critical Infrastructure Protection: PDD 63 White Paper*, May 22, 1998 (http://www.ciao.gov/CIAO_Document_Library/paper598.html).

2. *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document*, 3rd Edition, Office of the Manager, National Communications System, March 1999.

3. Executive Order 12472: *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984 (http://www.ncs.gov/ncs/html/EO12472.htm).

4. *National Coordinating Center for Telecommunications (NCC) Operating Charter*, October 9, 1985 (http://www.ncs.gov/ncc/OP_Chart/OpChart2.HTM).

5. *NCC-Information Sharing and Analysis Center (ISAC) Concept of Operations*, Version 1.0, May 1, 2000.

6. NCC-ISAC, Criteria for Participation in the NCC-ISAC, June 28, 2000.

7. NCC-ISAC Implementation Plan, Version 1.0, April 24, 2000.

8. *National Plan for Information Systems Protection: An Invitation to a Dialogue, Version 1.0*, January 7, 2000 (http://www.ciao.gov/National_Plan/national_plan%20_final.pdf).

9. National Security Telecommunications Advisory Committee (NSTAC) Emergency Response Procedures Working Group *National Coordinating Mechanism Implementation Plan*, January 1984.

10. *NSTAC Issue Review*, May 2000 (http://www.ncs.gov/nstac/IssueReview2000/nstac.pdf).

11. NSTAC Legislative and Regulatory Group, *Telecommunications Outage and Intrusion Information Sharing Report*, June 1999 (http://www.ncs.gov/nstac/NSTACXXII/Reports/InfoShare.pdf).

12. NSTAC Network Security Information Exchange Charter, as Amended March 1999 (http://www.ncs.gov/nstac/NSTACXXII/Reports/NSTAC22-NG.pdf).

[56] The documents listed provide additional information related to the NCC, its ISAC function, and the NSIE.

13. NSTAC Operations Support Group (OSG) Report to NSTAC XX, December 1997 (http://www.ncs.gov/nstac/FOSGREP.pdf).

14. NSTAC OSG Report to NSTAC XXI, September 1998 (http://www.ncs.gov/nstac/NSTACXXI/Reports/0925osg.pdf).

15. NSTAC OSG Report to NSTAC XXII, June 1999 (http://www.ncs.gov/nstac/NSTACXXII/Reports/NSTAC22-OSG.pdf).

16. *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, Revision 1, January 1999 (http://www.nstissc.gov/html/library/html).

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

18. President's Commission on Critical Infrastructure Protection (PCCIP) Report, *Critical Foundations: Protecting America's Infrastructures*, October 1997 (http://www.ciao.gov/CIAO_Document_Library/PCCIP_Report.pdf).

19. T1 American National Standard for Telecommunications, *Telecommunications Glossary 2000*, (http://www.its.bldrdoc.gov/projects/telecomglossary2000).

20. *TSP Service User Manual* (NCSM 3-1-1), (http://tsp.ncs.gov/tsp/documents.html).

21. U.S. Government, *Federal Response Plan* (Emergency Support Function #2 - Communications Annex), April 1999.

APPENDIX D

ACRONYMS

CERT/CC	Computer Emergency Response Team Coordination Center
CIAC	Computer Incident Advisory Capability
CONOPS	Concept of Operations
CSC	Computer Sciences Corporation
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EDS	Electronic Data Systems
E.O.	Executive Order
ERPWG	Emergency Response Procedures Working Group
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GSA	General Services Administration
I&C	Information and Communications
IAW	Indications, Assessment, and Warning
IES	Industry Executive Subcommittee
ISA	Information Sharing Agreement
ISAC	Information Sharing and Analysis Center
ISAS	Information Sharing and Analysis System
NCC	National Coordinating Center for Telecommunications

NCM	National Coordinating Mechanism
NCS	National Communications System
NIPC	National Infrastructure Protection Center
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMNCS	Office of the Manager, NCS
OSG	Operations Support Group
PDD	Presidential Decision Directive
PN	Public Network
POC	Point of Contact
SAIC	Science Applications International Corporation