



Chicago, Illinois - USA
29 May – 2 June 2006

SOURCE : NSTAC (submitted by TIA)

TITLE : President’s National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the National Coordinating Center

AGENDA ITEM : JOINT item 4.2

DOCUMENT FOR :

Decision	
Discussion	
Information	x

1 DECISION/ACTION REQUESTED

N/A

2 REFERENCES

Published May 10, 2006.

When adopted by the NSTAC and presented to the President of the USA, these reports become publicly available at http://www.ncs.gov/nstac/nstac_publications.html

3 RATIONALE

Document related to NGN and NS/EP, including restoration of infrastructure and services.

4 CONSEQUENCES AND IMPLICATIONS

(The implications for (including human resources) should be set out in this section).

5 ISSUES FOR DISCUSSION

On pages 30 and 31, the Task Force and the NSTAC noted the work of the GSC and our Resolution on Emergency Communications.

**THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE**



***NSTAC Report to the President
on the National Coordinating Center***

May 10, 2006

TABLE OF CONTENTS

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION AND CHARGE 1

 1.1 Background on the NCC 1

 1.1.1 History of NSTAC Studies on the NCC 3

 1.1.2 NCC Membership 3

 1.1.3 NCC Value Statement 4

 1.2 Charge of the NCCTF 5

 1.3 Scope of Study 5

 1.4 Approach 6

2.0 NCC FINDINGS 7

 2.1 Authorities Guiding Mission 7

 2.2 NCC Mission Statement 8

 2.3 NCC Functions 9

 2.4 NCC Membership and Operating Structure 10

 2.4.1 Sector Coordinating Council Framework 11

 2.4.2 NCC Membership Expectations 12

3.0 NCC ROADMAP FOR THE FUTURE 13

 3.1 One-Year and Ongoing Roadmap Actions 14

 3.1.1 Organizational Structure 14

 3.1.2 Information Sharing and Analysis 15

 3.1.3 Who’s in Charge? 17

 3.1.4 Incident Management/Emergency Response 20

 3.1.5 Policy 25

 3.2 Three-Year Roadmap Actions 25

 3.2.1 The New Value Proposition 25

 3.2.2 IT and Communications 27

 3.2.3 Industry Analysis 29

 3.3 Five-Year Roadmap Actions 29

 3.3.1 Incident Management/Emergency Response 29

 3.3.2 International 30

 3.4 Potential Roadblocks 31

 3.5 Conclusion 33

4.0 RECOMMENDATIONS TO THE PRESIDENT 33

APPENDIX A TASK FORCE MEMBERS, OTHER PARTICIPANTS, AND GOVERNMENT PERSONNEL A-1

APPENDIX B NCCTF INTERIM REPORT B-1

APPENDIX C NCC ROADMAP FOR THE FUTURE RECOMMENDED ACTIONS LIST C-1

APPENDIX D MEMBER EXPECTATIONS OF THE NATIONAL COMMUNICATIONS SYSTEM (NCS) AND THE NATIONAL COORDINATING CENTER (NCC).....D-1

APPENDIX E NCS DIRECTIVE 3-4: NATIONAL TELECOMMUNICATIONS MANAGEMENT STRUCTURE..... E-1

APPENDIX F IT ISAC CONOPS F-1

EXECUTIVE SUMMARY

The President's National Security Telecommunications Advisory Committee (NSTAC) Principals requested that a task force be formed to examine the future mission and role of the National Coordinating Center (NCC) during their October 21, 2004, NSTAC Principals Conference Call. The NSTAC established the National Coordinating Center Task Force (NCCTF) to study the direction of the NCC over the next year, three years, and five years, including—

1. How industry members of the NCC should continue to partner with Government;
2. How the NCC should be structured; and
3. How the new Department of Homeland Security (DHS) Sector Coordinating Council (SCC) approach could impact the NCC.

The NCCTF deliberated on numerous issues, focusing its discussions on the NCC's organizational structure, information sharing and analysis, leadership, incident management and response, and international mutual aid. To gain additional insight into incident management, and information sharing practices in particular, the task force co-hosted an all-day incident management subject matter experts meeting with the Next Generation Networks Task Force (NGNTF) on August 30, 2005.

Hurricane Katrina struck the Gulf Coast during the course of the task force's work, and the group incorporated lessons learned from its hurricane experiences into the final months of task force deliberation. The NCCTF also took into consideration the recent White House report on Hurricane Katrina in making recommendations on improved coordination between industry and Government.

The NCCTF first developed a vision statement that articulated the direction it believed the NCC should work toward over the next five years: "The NCC will be a flexible, inclusive, and trusted partnership for all industry and Government organizations focused on preserving the operations of the Nation's communications infrastructure." In addition, the task force drafted a vision statement that summarized its primary functions—national security and emergency preparedness (NS/EP) and information sharing and analysis. Two major findings of the task force are as follows: the NCC's organizational structure should have a single membership that performs both functions, and the NCC should work to incorporate the information technology (IT) sector over the next three years.

One central area of the task force's focus and findings was the need to clarify who is in charge of the NCC and Emergency Support Function (ESF) #2—Communications. The NCC's and National Communications System's (NCS) role in planning and incident response for NS/EP communications seems to have become less defined since transitioning to DHS. The lack of clear command and control of ESF#2 became a broader issue during the response to Hurricane Katrina, in which NCS' and the NCC's resources were overwhelmed and other ESF#2 support agencies (e.g., Federal Communications Commission and Department of Defense Northern Command) assumed new operational roles. Clarifying the delineation of roles and

responsibilities, especially regarding data reporting and the prioritization and escalation of requests, will improve incident response because there will be clear points of contact to address issues, less duplication of effort, and improved focus on fulfilling missions rather than on roles and responsibilities during an event.

Based on the NCCTF's analysis of issues facing the NCC, the NSTAC makes the following recommendations, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, and other existing authorities, that the President—

- **Direct the Secretary of Homeland Security, the Director of the Office of Science and Technology, the Secretary of Defense, and other ESF#2 Federal support agencies to develop and implement policies and procedures with respect to: (1) managing and escalating requests from the NCC, and (2) the delineation of authorities and responsibilities when ESF#2 is invoked.**
- **Direct the Office of Science and Technology Policy and the Homeland Security Council to join with the Communications SCC and the IT-SCC to support an industry-led task force with the primary goal of planning a regional communications and information technology coordinating capability in the Gulf Coast and Southeastern regions prior to the 2006 hurricane season. Subsequently, the task force will determine the best approach for a long-term regional communications and information technology coordinating capability that can serve all regions of the Nation. The task force should primarily be made up of industry representatives, as well as Federal, State, and local Government representatives.**
- **Direct the Secretary of Homeland Security to expand the NCC to include both communications and IT companies and organizations. This would be a cross-sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies.**
- **Direct the Secretary of Homeland Security to engage the private sector in critical infrastructure protection activities by increasing the flow of threat information to the private sector, facilitating private sector participation in impact analyses, and clarifying policies for the protection of private sector information.**
- **Direct the Secretary of Homeland Security to improve the ESF#2 Emergency Response Training and Exercise program, with a focus on enhancing coordination among industry members and Federal, State, and local responders during incidents of national significance. This program should focus on sector interdependencies for both physical and cyber threats, and would aim to produce actionable results. Industry must be involved from the earliest planning stages.**
- **Encourage the Secretary of Homeland Security to improve the Federal Government's cyber response strategy to delineate roles and responsibilities of Government and the**

private sector in the *National Response Plan*, aligning communications and cyber operations centers, and enhancing relationships with international computer emergency readiness teams.

- **Direct the Secretary of Homeland Security and other Government stakeholders to examine the value received from the NCC relationship and, if sufficiently supported, commit the resources necessary to strengthen and support the organization and its mission.**

To further these recommendations, the NCCTF developed a roadmap of action items for the NCC to assist it in evolving to address new issues and challenges over the next five years.

1.0 INTRODUCTION AND CHARGE

The National Coordinating Center (NCC)¹ has been the hub for coordinating the initiation and restoration of national security and emergency preparedness (NS/EP) communications services for more than 20 years—supporting four administrations and evolving as threats and national priorities have shifted. Following the September 11, 2001, terrorist attacks, the NCC proved its value to the Nation as it supported the restoration of communications in the New York and Washington, D.C., areas. The NCC has also repeatedly shown its strength during hurricane recovery efforts, including Hurricane Katrina.

The President's National Security Telecommunications Advisory Committee (NSTAC) recommended the establishment of the NCC in a 1983 report and has evaluated the NCC regularly in the time since. The NSTAC has periodically revisited the functions and missions of the NCC as the threat and policy environments have shifted. Most significantly, the NSTAC recommended designating the NCC as the Information Sharing and Analysis Center (ISAC) for telecommunications in 1999.

With the establishment of the Department of the Homeland Security (DHS) and the transfer of the National Communications System (NCS) to the new department in 2003, the NCC also has made the transition to DHS. With more than three years having gone by since the transition, this is an opportune time to evaluate the NCC, its value, and its functions to help create a roadmap for the next three to five years. Following the October 21, 2004, NSTAC Principal's Conference Call, the NCC Task Force (NCCTF) was formed to examine how best to balance traditional network and cyber concerns within the NCC moving forward.

1.1 Background on the NCC

The NCC was established to fulfill a critical need for a national coordinating mechanism to organize and manage the initiation and restoration of NS/EP communications services. This need was identified at the dawn of the divestiture of AT&T and the height of the Cold War. As Government increasingly relied on commercial communications services and no longer had a single point of contact (POC) for the industry, Government needed a joint industry and Government-staffed organization to coordinate emergency requests. The NCC became operational on January 3, 1984.

The primary mission of the NCC throughout its history has been to coordinate the restoration and provisioning of communications services for NS/EP users during natural disasters, armed conflicts, and terrorist attacks. Significant events such as the Hinsdale, Illinois, central office fire, the Oklahoma terrorist bombing, the events of September 11, 2001, and Hurricane Katrina have proved the value of this partnership. During a crisis, Government personnel communicate NS/EP requirement priorities to industry, and industry representatives assist the Government in developing situational awareness by providing restoration status information. Having the

¹ Also known as the National Coordinating Center for Telecommunications and National Coordinating Center for Telecommunications ISAC.

President's National Security Telecommunications Advisory Committee

representatives in one location ensures a smoother restoration effort. The NCC's all-hazards response depends on the flexible application of NCS resources, such as its priority service programs (e.g., Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority [TSP] Program).

During day-to-day operations, NCC members work on plans and share information on vulnerabilities and threats to the telecom infrastructure. Planning activities include developing lessons learned following events, creating comprehensive service restoration plans, planning for continuity of operations (COOP)/continuity of Government (COG) activities, and participating in exercise planning. In addition, the NCC works with international emergency response partners, including the North Atlantic Treaty Organization (NATO), International Telecommunication Union (ITU), and Canada, on crisis communications and mutual assistance.

In 2000, the NCC was designated the ISAC for telecommunications per the guidance in the 1998 Presidential Decision Directive 63 (PDD-63), *Protecting America's Critical Infrastructures*, which encouraged the private sector to establish ISACs to "serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information."² As part of the ISAC mission, the NCC collects and shares information about threats, vulnerabilities, intrusions, and anomalies from the communications industry, Government, and other sources. Analysis on information is performed with the goal of averting or mitigating impact on the communications infrastructure.

The NCC has historically been an operational element and as such does not fall under provisions of the Federal Advisory Committee Act (FACA). A June 1, 1983, letter to the NCS from Assistant Attorney General William F. Baxter discussed issues of incident management and information sharing for the proposed National Coordinating Mechanism (NCM) (which became the NCC) and noted that such an organization posed no significant antitrust problems. NCCTF members recognize that the NCC's mission has not changed, and the organization's information continues to be protected from FACA.³

Since the transition to DHS, the NCC has been involved in additional critical infrastructure protection (CIP) activities. As part of the implementation of Homeland Security Presidential Directive (HSPD) 7, DHS is tasked with identifying, prioritizing, and protecting the Nation's critical infrastructure. Through the NCC, the NCS often coordinates data calls on the identification of assets, coordinates planning for national special security events (NSSE), and provides impact analyses. In the future, NCC industry members may be asked to further assist in the risk assessment process as detailed in the sector's Sector-Specific Plan.

² The White House. "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." White Paper. May 22, 1998.
http://permanent.access.gpo.gov/lps9890/lps9890/www.ojp.usdoj.gov/osldps/lib_pdd598.htm.

³ Some NCC data is exempt from release under a number of exemptions to the Freedom of Information Act (FOIA, 5 U.S. Code [U.S.C.] Section 552.) In addition, some data may qualify as Protected Critical Infrastructure Information (PCII) if DHS determines the data meets the statutory and regulatory criteria. Data designated PCII is exempt from release under FOIA per 6 U.S. Code Section 133 {which is a 5 U.S.C. Section 552 (b)(3) statutory exemption.}

1.1.1 History of NSTAC Studies on the NCC

The history of NSTAC studies on the NCC extends back to the NSTAC's early days. One of NSTAC's original task forces—the NCM Task Force—recommended establishment of the NCC in its May 1983 report. Following that report, the NSTAC developed a recommended implementation plan. Since then, the NSTAC has periodically revisited the NCC by evaluating its mission, information sharing procedures, and effectiveness as changes occurred in the threat, policy, and technological environments. In 1996, the Industry Executive Subcommittee established a task force to consider these environmental changes and whether the NCC mission, organization, and capabilities remained valid. In addition to updating the *NCC Operating Guidelines* and chartered functions, the NSTAC recommended the integration of an electronic intrusion incident information process for the NCC. The NSTAC also concluded that the NCM concept should be applied to other critical infrastructures using the NCC as a model. Subsequent to the issuance of PDD-63, the NSTAC determined that the NCC already served the primary functions of an ISAC. The National Security Council agreed with this conclusion and officially recognized the NCC as the ISAC for the telecommunications sector in January 2000.⁴

1.1.2 NCC Membership

As of January 2006, the NCC had 23 Federal agencies represented and 33 communications infrastructure companies (see Tables 1.1 and 1.2) that work together to restore communications services to key user groups during NS/EP incidents. The NCS members—Federal departments, agencies, and entities that have significant NS/EP responsibilities and whose operations are heavily dependent on communications provided by industry—act as the NCC's Government membership. Industry membership is broadly representative of the communications infrastructure with a couple of exceptions. Based on a 2005 *NSTAC Member Market Study*, current NCC industry membership covers:

85%	U.S. wireline market
79%	U.S. wireless market
70%	Worldwide router market
59%	Aerospace and defense market
19%	North America fixed satellite services
18%	Web-hosting market
16%	Mobile-phone equipment market
12%	Consumer Internet service provider (ISP) market
6%	Information technology (IT) services market

Because industry owns more than 90 percent of the Nation's critical communications infrastructure, corporations recognize their responsibility to ensure stability and dependability of the communications network. The partnership continues to reflect the original commitments of 1984, as well as additional initiatives related to the risks of terrorism.

⁴ Richard A. Clarke. "Memorandum: Designation of the National Coordinating Center as an Information Sharing and Analysis Center." January 18, 2000.

Table 1.1. NCC Government Membership
(as of January 2006)

Central Intelligence Agency	Federal Communications Commission
Department of Commerce	Federal Emergency Management Agency
Department of Defense	Federal Reserve Board
Department of Energy	General Services Administration
Department of Health and Human Services	Joint Chiefs of Staff
Department of Homeland Security	National Aeronautics and Space Administration
Department of Interior	National Security Agency
Department of Justice	National Telecommunications and Information Administration
Department of State	Nuclear Regulatory Commission
Department of Transportation	United States Department of Agriculture
Department of Treasury	United States Postal Service
Department of Veterans Affairs	

Table 1.2. NCC Industry Membership
(as of January 2006)

Americom	Lockheed Martin
AT&T	Lucent Technologies
Avici	McLeodUSA
BellSouth	Motorola
Boeing	New Skies
Cincinnati Bell	Nortel Networks
Cingular Wireless	Northrop Grumman
Cisco Systems	Qwest Communications
Computer Sciences Corporation	Raytheon
CTIA—The Wireless Association	Savvis
EDS	SAIC, Inc.
GlobalstarUSA	Sprint Nextel Corporation
Intelsat General Corporation	Telecommunications Industry Association
Internap	United States Telecom Association
Intrado	VeriSign
Juniper Networks	Verizon
Level 3 Communications	

1.1.3 NCC Value Statement

A public-private partnership must exhibit value to all parties involved if it is to be successful and remain viable. Value in partnership with the Federal Government should transcend patriotic duty for companies. The NCC partnership has been resilient and has grown during its 22-year history because it creates value for industry and Government participants. However, there is always room for improvement, particularly in strengthening the value proposition for the private sector.

To the NCC, private sector member companies and their representatives bring knowledge of the communications architecture, assets, vulnerabilities, and service functionality. In addition, as

owners of the infrastructure, they provide visibility into situations, response capability, and the customer viewpoint. Acting as Federal agency liaisons, Government personnel can share information compiled on threats, vulnerabilities, and restoration plans, including sensitive and classified data. During events, Government personnel are able to cut through Federal “red tape” to obtain assistance when needed (e.g., transportation issues, priority energy/refueling for critical facilities, security).⁵ Government personnel can offer NCC facilities a 24x7 watch center, tools, and staff support.

During crisis situations, the value for both sides comes from having trusted, personal relationships with each other. The center offers a single point of collaboration for Federal, State, and local information sharing and requests for information.

1.2 Charge of the NCCTF

The NSTAC Principals requested that a task force be formed to examine the future mission and role of the NCC. Specifically, the NCCTF was tasked to study the direction of the NCC over the next year, three years, and five years, including:

1. How industry members of the NCC should continue to partner with Government;
2. How the NCC should be structured; and
3. How the new DHS Sector Coordinating Council (SCC) approach could impact the NCC.

1.3 Scope of Study

The NCCTF was provided with a broad task to develop a roadmap for the NCC for the next five years. As a result, the task force discussed a broad array of issues related to the NCC, including its organizational structure, relationships, information sharing, and operations. At the outset of the study, the task force identified the following issues for investigation:

Organizational Structure

- Are any organizational structure changes required? (Sections 2.4, 3.1.1, and 3.2.2)
- How can companies better use scarce resources for participation in industry-Government groups? (Section 3.4)
- How can the NCC best perform outreach to other sector segments that are not represented or are underrepresented in the NCC, such as ISPs, Internet infrastructure companies, cable firms, and satellite providers? (Section 3.1.1 and 3.2.2)

Information Sharing and Analysis

- How should industry share information? (Section 3.1.2 and 3.2.3)
- What information needs to be shared? (Section 3.1.2)

⁵ During the aftermath of Katrina in fall 2005, telecommunications infrastructure providers (TIP) had a difficult time cutting through red tape to provide disaster response assistance as a result of inconsistent interpretations of key legal and policy documents, including the *Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)*. The NSTAC Legislative and Regulatory Task Force (LRTF) issued a report in January 2006 that seeks designation of TIPs as “Emergency Responders (Private Sector)” to avoid delays in restoring basic communications infrastructure.

- Who analyzes the information? (Section 3.1.2 and 3.2.3)
- How should the NCC participate in *National Infrastructure Protection Plan* (NIPP) infrastructure protection activities? (Sections 2.4.1 and 3.1.2)

Leadership

- From whom should the NCC take direction during incident response activities? (Section 3.1.3 and 3.1.4)
- How does the NCC integrate with the DHS National Incident Management System (NIMS) framework? (Section 3.1.3)

Incident Management/Emergency Response

- How does the NCC support the new *National Response Plan* (NRP) cyber requirements? (Sections 3.1.4 and 3.2.2)
- Can the NCC implement a more effective planning and training strategy? (Section 3.1.4)
- How can the NCC meet increasing demands for outage reporting by the Federal Communications Commission (FCC) and DHS? (Sections 3.1.4 and 3.4)

Policy

- Are there any policy changes the NCC should be prepared to address? (Section 3.1.5)

International

- What role should the NCC play in international response? (Section 3.3.2)

1.4 Approach

Representatives of NSTAC member companies and Government participants contributed to the NCCTF effort. It was imperative to the success of the effort that many of the members be those actively participating in NCC operations. This effort enabled the NCCTF to fully understand the NCC and to have the capability to reach back to non-NSTAC members to receive feedback on proposed recommendations. Appendix A provides a list of task force members, other participants, and Government personnel.

The task force examined the NCC and investigated issues in three phases: issue definition, issue discussion, and reporting. The activities related to each phase were as follows:

- **Phase 1:** Researched and developed the NCC mission statement, functions, and value statement and mapped its authorities to missions. The result of Phase 1 was an interim report provided to the NSTAC Principals at the NSTAC XXVIII Meeting in May 2005 (see Appendix B).
- **Phase 2:** Discussed long-term issues impacting the NCC, focusing on organizational structure, information sharing and analysis, incident management/emergency response, leadership, policy, and international mutual aid. For added perspective on incident management issues, the NCCTF received a briefing on incident management practices during the response to the September 11 terrorist attacks on the World Trade Center in New York City. In addition, the NCCTF co-hosted an incident management subject matter experts (SME) meeting with the NGNTF. During the study, the NCC became

actively engaged in the Hurricane Katrina response efforts, and relevant lessons learned were discussed in the NCCTF meetings.

- **Phase 3:** Drafted task force report, Presidential recommendations, and roadmap for the NCC's future.

2.0 NCC FINDINGS

The first step in developing a roadmap for the NCC was to document the NCC's authorities, missions, and functions. This action enabled the task force to gain a clear understanding of its current operating picture so it could address how it might need to be adapted in the future.

2.1 Authorities Guiding Mission

The NCC's primary driver is Executive Order (E.O.) 12472, which establishes a joint industry-Government NCC that "is capable of assisting in the initiation, coordination, restoration, and reconstitution of national security or emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency."

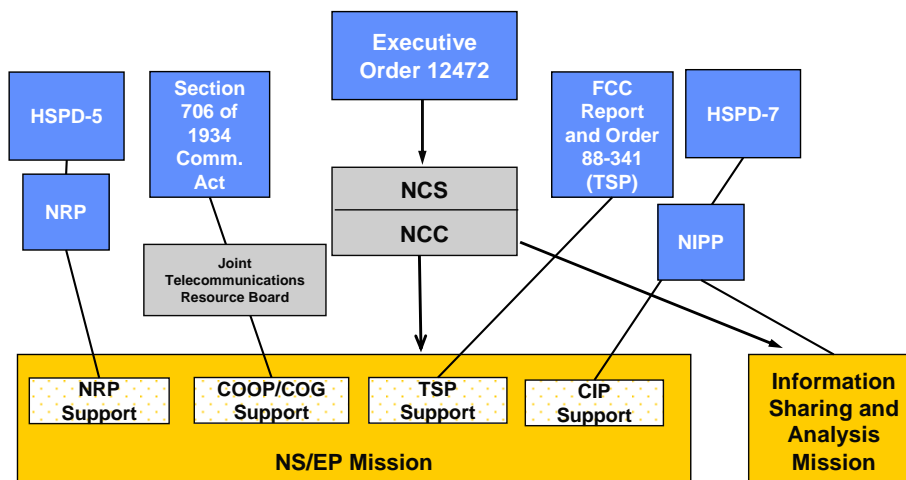
The NCC is also governed by several additional authorities. It provides support to the NRP as directed by HSPD-5, and Section 706 of the *Communications Act of 1934*⁶ governs its engagement in COOP/COG activities. It also supports the TSP Program through the authority of the FCC.⁷ HSPD-7 encourages information sharing and analysis mechanisms, in addition to focusing on other CIP activities, such as the identification, assessment, and protection of critical assets. HSPD-8, a companion directive to HSPD-5 and HSPD-7, describes the way Federal departments and agencies will prepare for such responses, including a mandate for developing a National Preparedness Goal,⁸ providing Federal assistance for first responder preparedness, and establishing a comprehensive training program to meet the goal. Figure 2.1 illustrates the relationship of the various authorities to the NCC and its NS/EP, CIP, and ISAC missions.

⁶ Codified at 47 U.S.C. Section 606, *War Powers of President*.

⁷ See 47 C.F.R. Part 64, Section 64.401 and Part 64 Appendix A.

⁸ HSPD-8 mandates development of the National Preparedness Goal, which establishes three overarching priorities: (1) implementation of the NIMS and the NRP, (2) expansion of regional collaboration, and (3) implementation of the NIPP, and several capability specific priorities, which include strengthening information sharing and collaborative capabilities and interoperable communications capabilities.

Figure 2.1 NCC Authorities and Missions



As a result of distinct authorities and leadership, NS/EP communications services and CIP missions have been viewed as distinct missions. However, the NCCTF affirms the following definition of NS/EP communications:

“[T]hose telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States.” (47 Code of Federal Regulations [CFR] 201.2[g])

This definition should be interpreted to include telecommunications and cyber events. In addition, the NSTAC believes that protecting against the degradation of NS/EP posture inherently includes CIP matters. This statement assists the NCC in the evolution of its membership and structure and affirms the continued viability and mission of the NCC.

2.2 NCC Mission Statement

The task force worked to clarify the NCC’s vision, mission, and functions that are derived from the various authorities noted above. As such, the NCCTF proposed a new NCC mission statement.

NCC Mission Statement: The joint industry-Government NCC provides an operations center to plan for and respond to events in support of NS/EP, including NS/EP communications services and CIP, and information sharing and analysis.

- **NS/EP Communications Services:** Assists in the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency. In addition, the NCC enhances physical and cyber security of the Nation’s critical communications infrastructures by facilitating cooperation, information

sharing, and system-to-system interaction among the critical infrastructures and between the Government and the private sector.

- **Information Sharing and Analysis:** Averts or mitigates impact on the communications infrastructure on behalf of the private sector by collecting, analyzing, and sharing information on threats, vulnerabilities, intrusions, and anomalies from the communications industry, Government, and other sources.

2.3 NCC Functions

The NCC performs numerous functions within and beyond the broad categories listed above and described in the background section. The task force developed the following comprehensive list of the NCC's duties and functions, in order of importance.

1. **Industry:** Coordinate/direct prompt restoration of communications and information services in support of NS/EP needs.
2. **Industry:** Coordinate/direct and expedite the initiation of NS/EP communications services.
3. **Industry:** Promptly provide technical analysis/damage assessment of service disruptions and identify necessary restoration actions.
4. **Government:** Collect, distribute, analyze, and share information relevant to threats, vulnerabilities, and alerts.
5. **Government:** Deliver alerts, warnings, and advisories to the sector and share information with DHS and Sector-Specific Agencies regarding threats and incidents.
6. **Industry:** Plan, develop, and exercise comprehensive service restoration plans.
7. **All:** Develop watch center type functions to work through cooperating industry operation centers to effectively monitor the status of essential communications facilities.
8. **Industry:** 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 industry's network operations centers.
9. **Industry:** Identify liaison points in each company for rapid response to emergencies.
10. **Industry:** Maintain ability to rapidly transfer operations from normal to emergency operations.
11. **All:** 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.
12. **Government:** Work on policy-level CIP and NS/EP planning and issues.
13. **Industry:** Coordinate/direct network reconfiguration plans in support of NS/EP needs. In performing these functions, the NCC monitors the status of all essential communications facilities, including public switched networks.

14. **Government:** Work with international emergency response partners, including NATO, ITU, and Canada, on crisis coordination, mutual assistance, and CIP issues.
15. **Government:** Facilitate the processing and analysis of information collected from private sector companies and the Government in key critical infrastructure sectors—IT, communications—with Government services and others.
16. **All:** Facilitate cooperation, information sharing, and system-to-system interaction between the Government and the private sector for CIP and homeland security.
17. **All:** Conduct outreach to companies and other organizations within the sector to educate them on the NCC and value of membership.
18. **All:** Monitor research and development related to NS/EP and CIP within Government and private sector.

2.4 NCC Membership and Operating Structure

The industry presence in the NCC is composed of resident and nonresident entities that the Federal Government has selected from communications industry. The Manager of the NCS reviews industry participation on a continuing basis. Nonresident industry entities are afforded the maximum practicable opportunity to participate in NCC activities through virtual or direct actions. Industry representatives maintain interfaces with their representative operations centers and access to appropriate databases to monitor the service status of their network and facilities. These representatives serve as POCs for expediting restoration or initiation of NS/EP communications services.

For the communications sector, the NCC has long served as the forum for information-sharing activities. Since September 11, 2001, the NCC has experienced roughly 125 percent growth, expanding from 16 to 36 member companies. Most new members are nontraditional service providers or equipment manufacturers. This influx of new members, however, has hindered information sharing.

It takes time for trust levels to build, especially when the participation level in information sharing varies greatly from one member to another. Some companies now hesitate to share sensitive information, and do not want to potentially put their customers at risk by revealing vulnerability data.⁹ Some might be more likely to share with those with whom they have active contracts or with whom they have signed nondisclosure agreements and/or service-level agreements.

⁹ Section 222 of *The Communications Act of 1934*, as amended, requires that telecommunications carriers protect the privacy of customer proprietary network information (CPNI). The FCC has initiated several inquiries into the procedures used by telecommunications carriers to ensure confidentiality of CPNI based on concerns regarding the apparent sale of telephone call records over the Internet. On January 30, 2006, the FCC issued a Public Notice directing all telecommunications carriers, including wireline and wireless carriers, to submit certifications demonstrating CPNI compliance as required by Section 64.2009(e) of the FCC rules.

An ongoing organizational structure issue is the relationship between NS/EP and information sharing and analysis and how the division of these missions should affect the organizational structure. Currently, the NCC has a single membership for both missions; however, most members do not participate in both mission areas. Furthermore, questions were asked about Government participation in the ISAC because ISACs are designed to be industry-only organizations. The NCCTF discussed four future organizational options:

1. The NCC and the ISAC will have a single membership. Participation in the information sharing and analysis function will require membership in the NCC.
2. The NCC will continue to have a limited membership as determined by the Government. The ISAC, while remaining an NCC function for resource purposes, will be identified separately as the ISAC and will have a separate and distinct membership.
3. The NCC will continue to be an NS/EP-focused organization, but will have a limited membership as determined by Government. The ISAC will break off as a separate and distinct group with its own resources and membership.
4. The NCC will continue to be considered the primary operational and planning entity for the communications sector, and Government may need to determine who participates in the NS/EP function.

The task force concluded that the NCC should have an organizational structure with a single membership that performs the NS/EP functions and information sharing and analysis (i.e., the role of the ISAC).

The NCC operating structure has evolved as the organization has adopted additional functions, such as the ISAC. The Manager of the NCC, a Government employee, leads the NCC, with industry electing a Chair and Vice Chair from within NCC industry membership. There also is an industry representative for international issues who works closely with the Department of State representative in the NCC. Within the NCC, a watch desk operates 24x7. The NCC Watch monitors events, tracks action items, and disseminates alerts and warnings. Regular operations include a weekly meeting with all industry and Government members to share information on threats or incidents and discuss issues. During emergency operations, daily meetings are held with Government and industry members who have a role in the current response effort.

2.4.1 Sector Coordinating Council Framework

One major issue in the task force charge was to determine how the new SCC approach could affect the NCC. The NIPP requests that each critical infrastructure sector establish an SCC to coordinate with DHS on a range of infrastructure protection activities and policy issues. The task force discussed the option of making SCC a function of the NCC, as well as the option of having the Communications SCC (C-SCC) set up as an entirely separate organization. One reason given for including the SCC as a function of the NCC was to maintain a single POC for the Federal Government to interact with the sector. However, there were other reasons to maintain it as a separate entity. One of the task force's concerns was the effect of integrating

policy functions of the C-SCC with operationally focused NCC functions. Because the NCC has always been focused on operational activities and not sector-wide policy, FACA guidelines have never applied to the organization; however, if expanded NCC policy and advisory functions were intertwined, the organization's FACA status might be altered.

The NCC industry members established a working group to evaluate the establishment of an SCC. The working group had several concerns regarding the combination of the NCC and SCC organizations, including (1) potential exists for industry members to be discouraged from participating in a group integrated with the Government, (2) skill sets of NCC and SCC members might be different, and (3) expanding NCC membership to incorporate those wanting to participate only in the SCC function might dilute the organization's NS/EP focus. After further deliberation, **the C-SCC was established as a separate entity in mid-2005** and has established operating procedures. If industry reconsiders combining the NCC and SCC in the future, these considerations should be taken into account.

2.4.2 NCC Membership Expectations

Industry members note that their involvement in the NCC is on a pro bono basis and that the commitment brings with it varying corporate expectations. A recent survey of industry and Government NCC members showed an overwhelming expectation for increased flows of information from public sector agencies to industry. The survey also underscored industry's desire to become a true partner with Government in the information-sharing process.

The following represents an overview of expectations related to information sharing illuminated in the member survey (see Appendix D):

- An increased flow of terrorist threat information from the intelligence community to industry would provide justification for industry's continued participation in the NCC.
- Supporting an industry decision to identify vulnerabilities based on Government-provided threat information would result in more-accurate risk analyses.
- Industry members request improved communications from Government on "U.S. space-based objects" and related activities located in proximity to commercial satellites.

To receive this type of information, industry must have the proper clearances. The NSTAC has previously suggested that the creation of a standard industry-wide credentialing process, combined with standard processes for access permissions, will further solidify the Nation's communications infrastructure because it will aid in identifying trusted individuals (i.e., those who have passed the national screening).¹⁰

The NSTAC Satellite Task Force recommended sharing information between the Government and the commercial satellite service providers with the NCC Watch as the focal point for this information sharing. The NCC Watch should communicate regularly with the U.S. Strategic Command Satellite Operations Center, and the Government should provide situational awareness information to the NCC Watch on all potential threats to any element of the commercial satellite

¹⁰ NSTAC Trusted Access Task Force: *Screening, Credentialing, and Perimeter Access Controls Report*, January 19, 2005.

constellations, including radio frequency interference and/or potential physical interference or potential collisions by other space objects. This information would be made available to the appropriate satellite service provider(s), and any resulting actions would be coordinated through the NCC Watch.¹¹

3.0 NCC ROADMAP FOR THE FUTURE

One of the overall objectives of the NCCTF was the development of a roadmap of potential actions for a five-year period to evolve its organization and focus. As part of this process, the NCCTF composed a vision statement for the NCC, which defines the desired end state for the organization.

NCC Vision Statement for 2010

The NCC will be a flexible, inclusive, and trusted partnership for all industry and Government organizations focused on preserving the operations of the Nation's communications infrastructure.

In developing the NCC Roadmap, the task force made the following assumptions.

- The NCC is a single entity with multiple functions.
- Presidential E.O. 12472, with its focus on NS/EP, will continue to be the main driver of the NCC.
- The NCC will continue its all-hazards approach to incident management.
- Membership will expand to cover a wider range of the communications infrastructure sector.
- The communications infrastructure and IT sectors will work together more closely during the next several years.
- The NCC is prepared to work under any changes brought about by the current NS/EP review of HSPD-7.

Noting these assumptions, the NCCTF identified six primary issue areas related to the future of the NCC during its deliberations: (1) organizational structure; (2) information sharing and analysis; (3) leadership; (4) incident management/emergency response; (5) policy; and (6) international issues. The task force focused on ways in which the NCC's mission and membership structure should change to address the new homeland security and technology environments. As the NCC develops a plan for the next five years, these findings and

¹¹ NSTAC Satellite Task Force, March 2004.

recommendations related to its core functions should be addressed to improve NCC's overall operations.

The following paragraphs include actions that the NCC and DHS should plan to take over the next one year, three years, and five years. Appendix C lists all roadmap actions.

3.1 One-Year and Ongoing Roadmap Actions

Within the next year, the NCC should focus on the most pressing issues. Incident management and the NCC's relationship with the IT industry will be at the forefront.

3.1.1 Organizational Structure

The NCCTF notes that PDD-63 covered communications and IT companies under a single "Information and Communications" (I&C) Sector. Subsequently, HSPD-7¹² unilaterally separated the two portions of the I&C sector into telecommunications and IT. In reality, numerous companies' products and services span and reside in both sectors, and we as industry disagree with this separation. The separation of communications and IT presents policy, operational, and administrative challenges, particularly in the areas of information sharing and incident management during cyber events.¹³

To effectively prepare for a converged communications environment, the NCS and NCC should plan to do the following over the next year.

- **The NCS should work with NCC industry members to clarify the process for membership as it pertains to the NS/EP function.**
- **The NCC must accept the new mission statement proposed by the NCCTF in order to more clearly define its vision, mission, and functions.**
- **The NCC must establish a working group to facilitate the transition to an NCC that includes broad representation from within the existing IT sector. This group will address structural, funding, and operational issues.**
- **The NCC must facilitate the ability of nontraditional communications providers to respond to NS/EP incidents.**
- **The NCS should convene a conference for communications and IT providers to plan for an improved focus on cyber issues, including preparing a vision on how to combine the NCC and IT ISAC.**

¹² HSPD-7 ("Critical Infrastructure Identification, Prioritization, and Protection"), issued in December 2003, superseded PDD/NSC-63 of May 22, 1998 ("Protecting America's Critical Infrastructures").

¹³ For clarity, the NCCTF refers to the sector as "communications" instead of "telecommunications" in this report.

- **The NCC should conduct outreach to enhance membership in underrepresented communications subsectors, including cable network operators, ISPs, satellite operators, broadcast infrastructure operators, and unlicensed wireless operators.**

3.1.2 Information Sharing and Analysis

The communications sector owns the vast majority of the communications infrastructure necessary for NS/EP communications; as such, this sector requires assurance that information shared in the NCC and related forums is protected from public disclosure.

The Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission Report) states, “the President should take the responsibility for determining what information can be shared by which agencies and under what conditions.”¹⁴ This mandate should protect not only the privacy rights of individuals but also the confidentiality needs of companies. The NCCTF notes that certain types of information need more protection than others. Industry NCC members have suggested that it would be helpful to understand the operational purpose behind information requests from the Government. For instance, some information is intended to be used specifically for public release, such as outage information during a hurricane, whereas more detailed information might be requested as part of an infrastructure modeling database. The provider of the information should be given a full explanation of the use of its information and those persons or organizations that will have access to it.

The NCCTF recommends that DHS clarify its policy with respect to the use of private sector information and those persons or organizations that will have access to such information. The NCCTF has been advised that proprietary information meeting the criteria specified in the Freedom of Information Act (FOIA)¹⁵ voluntarily provided to the Government in confidence, and clearly marked “industry proprietary,” can be protected from disclosure under FOIA.¹⁶ DHS is also finalizing rules for the Protected Critical Infrastructure Information (PCII) program. Some companies would more willingly provide data if they had assurance regarding who within Government will have access to information once it is provided voluntarily.

Two of Homeland Security Secretary Chertoff’s themes in the release of the Second Stage Review were (1) improving the Department’s information sharing, and (2) strengthening its partnerships with the private sector. For the communications sector to improve its information sharing and partnership with Government, a shift needs to occur toward proportional information sharing to include more Government-to-industry and industry-to-industry information sharing, in addition to industry-to-Government sharing. The NCC has worked with DHS on the development of information sharing templates through the ISAC Council. These templates outline the different types of information shared, how it is shared, with whom it is shared, and the time sensitivity of the information. The NCCTF also suggests that the NCC reexamine the

¹⁴ p. 394.

¹⁵ E.g., 5 U.S. Code Section 552(b)(4) exempts from release “trade secrets and commercial or financial information obtained from a person and privileged or confidential.”

¹⁶ NSTAC. *NCCTF Meeting Summary*, November 14, 2005.

use of nondisclosure agreements (NDA) for industry and Government members based on models such as the Network Security Information Exchanges (NSIE). In the past, efforts to institute an NDA process have met with resistance, but its importance cannot be overstated.

A recent *Lessons Learned Information Sharing* Intelligence and Information Sharing Initiative determined that DHS intelligence analysts did not effectively communicate with their communities of interests.¹⁷ Threat information received from DHS was nonspecific and did not meet the recipient's requirements. Individuals who transmitted threat information to DHS or other Federal agencies rarely received any feedback. The NSTAC agrees with the report's recommendation to DHS to "foster a transmit and receive environment for information sharing that involves a greater two-way flow of intelligence/information—based on State, local, tribal, and private sector requirements."

For the NCC to improve its information-sharing function, the following steps must be taken on an ongoing basis.

- **DHS should increase the flow of threat information or issues of concern through the NCC, to include information regarding Government-owned assets or activities that may potentially jeopardize industry or Government assets.**
- **NCC members should improve information sharing among industry members and between industry and Government. Some of the issues for consideration should include but should not be limited to: (1) protection mechanisms for member companies; (2) partitioning industry and Government information-sharing systems; and (3) improving modeling capabilities.**

A related issue is the NCC's role in implementing the NIPP, which is being finalized as of the writing of the report. The NIPP requests industry participation in protecting the Nation's critical infrastructure through sharing information on critical assets, participating in the risk assessment process, and implementing protective measures. The C-SCC will be the primary POC for Government in developing the Telecommunications Sector-Specific Plan; however, the NCC will have a role in providing asset data and assisting in impact analyses—two roles that NCC industry members have historically fulfilled.

The NCCTF has determined that the role of industry in data analysis needs to be enhanced. The communications infrastructure is highly complex, composed of tens of thousands of assets and company-specific network architectures. To effectively monitor the security of its networks, member companies require input into analyses related to their network and threats to the sector. Although the NCS, with the information available to it, can make rough assessments of the entire sector, the NCS' assessment process would significantly benefit from the involvement of the owners and operators of the communications networks, who can fully assess impact to their networks. Currently, communications service providers are invited to review Government-provided analyses only after these analyses have been finalized. Such after-the-fact review provides little benefit to the end product.

¹⁷ DHS. "LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process." December 2005.

Although industry members are frequently asked for asset data to contribute to analyses, the involvement of communications service providers can make a great impact in the interpretation of asset information. Government should bring industry experts into the analysis process to produce more accurate assessments. The NSTAC believes this collaborative action will greatly improve the quality of Government's analyses, and members are eager to participate in the process. Enhancing the analysis of information will improve the sector's security posture and the NCC's value.

The NSTAC recommends that DHS begin planning for a multi-industry coordinating center that would incorporate and be modeled on the NCC. As also recommended in the *NSTAC Report on Next Generation Networks*, the center would initially focus on the Communications and IT Sectors but ultimately would include all key sectors. In addition, the NSTAC recommends that the Manager of the NCS involve companies at an earlier stage in the impact analysis process, rather than inviting participation for verification purposes or after the fact. Depending on the scope of these analyses, some companies might require contractual relationships and reimbursement as a result of the expense involved.

To continue to foster an environment that cultivates information sharing and analysis, DHS and the NCS should plan to do the following over the next year.

- **DHS should clarify its policy with respect to the use of private sector information and those persons or organizations that will have access to such information.**
- **The NCS should enter into agreements to broaden its collaboration with communications service providers prior to and throughout the impact-analysis process. Such collaboration would significantly enhance the value and validity of the analysis.**
- **The NCS should involve industry experts at an earlier stage in the threat, vulnerability, and impact analysis processes in order to produce more accurate assessments.**
- **DHS should begin planning for a multi-industry coordinating center that would incorporate and be modeled on the NCC. It would initially focus on Communications and IT Sectors.**

3.1.3 Who's in Charge?

The final report of the 9/11 Commission determined that the lack of clear delineations of responsibility and authority was a failure of the Government. This deficiency also has been an issue for the NCC. Since the NCS transitioned to DHS in 2003, the NCC has lacked clarity regarding which missions and requests should take priority. The NCC's and NCS' roles in planning and incident response for NS/EP communications seem to have become less defined. During recent incidents and exercises, it became clear to the NCC that one of its main challenges was the prioritization of requests coming from the NCC's various leadership organizations. The

NCC typically takes direction from DHS and the Office of Science and Technology Policy (OSTP). During the Hurricane Katrina response, a new player was the Department of Defense's (DOD) Northern Command (NORTHCOM). In addition, the FCC assumed new operational roles to help the NCS deal with excessive Emergency Support Function (ESF) #2 requirements derived from Hurricane Katrina. The addition of new players' roles and responsibilities introduced confusion into the existing processes. This is an area on which the new Assistant Secretary for Cyber Security and Telecommunications can focus.

According to authorities, including E.O. 12472 and the NRP's ESF#2, the NCS has a lead role for incident response and planning for NS/EP communications. E.O. 12472 states that the NCS should assist the President and other Executive Office of the President (EOP) agencies in coordinating the planning for and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.¹⁸ E.O. 12472 specifically states that the NCS shall—

*Serve as a focal point for joint industry-Government national security and emergency preparedness telecommunications planning.*¹⁹

The NRP ESF#2 Annex identifies the NCS as the primary agency responsible for ESF#2, noting that the Director of OSTP officially delegated its functional responsibility to the Office of the Manager, NCS, in a June 11, 1993, memorandum: "Subject: National Security and Emergency Preparedness Telecommunications." DOD's responsibilities, as defined in the ESF#2 Annex, are limited to assisting the Manager of the NCS in the deployment and use of DOD owned/leased communications assets to support the response effort. Under the NRP, the FCC's primary responsibilities are to review policies, plans, and procedures related to licensed/regulating entities by FCC to ensure that policies are consistent with the public interest, to perform all functions required by law with respect to all entities licensed or regulated by the FCC, and to provide support to the Federal Emergency Communications Coordinator (FECC) to resolve radio frequency interference and issue frequency assignment requests. The FCC also continues to perform functions with respect to all entities under its purview, such as the extension, discontinuance, or reduction of common carrier facilities/services and control of rates. To accomplish this mission, the FCC has recently announced the establishment of a Public Safety and Homeland Security Bureau. It is not yet clear how the new bureau may further change the environment.

In 2004, DHS released the NIMS document, describing a standardized nationwide approach to domestic incident management that applies to all jurisdictional levels and across the functional disciplines in an all-hazards environment. Any discussion on ESF#2 leadership should clarify NCC's alignment within the NIMS Framework of coordination and command structures. Figure 3.1 represents NCCTF's interpretation of how the NCC and ESF#2 align with the NIMS Framework based on an analysis of the NIMS document and NRP ESF#2 Annex. ESF#2 related entities are shown in gray.

¹⁸ E.O. 12472, Section 1(b)(2).

¹⁹ E.O. 12472, Section 1(d)(1).

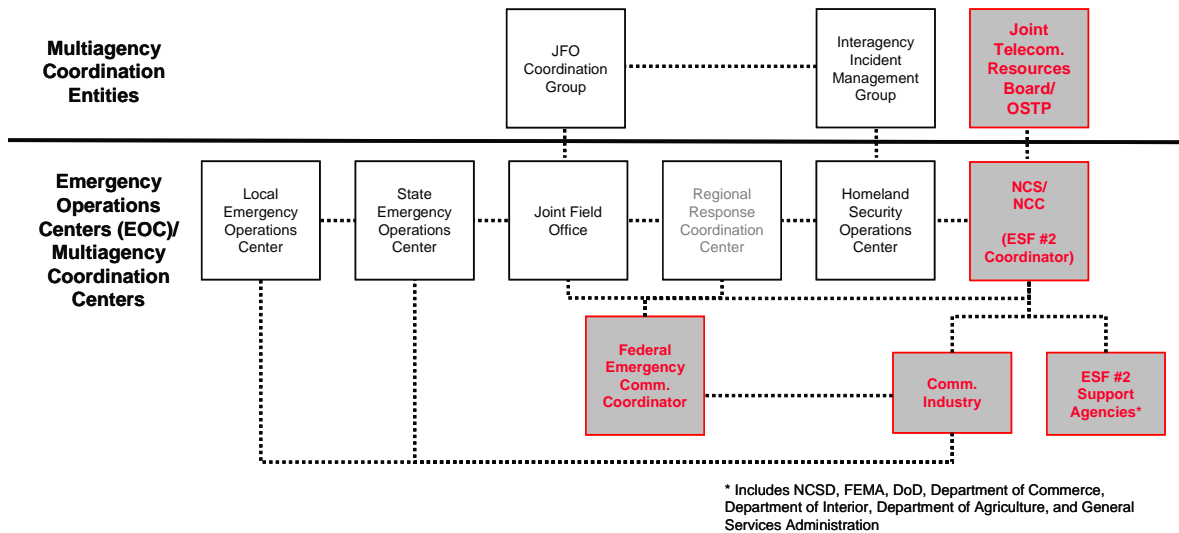
President’s National Security Telecommunications Advisory Committee

The NCS is developing an ESF#2 Federal Operations Plan to provide supplemental detail to the NRP. All ESF#2 support agencies, including the Federal Emergency Management Agency (FEMA), General Services Administration (GSA), DOD, FCC, and others must give their full attention to this matter and, when it is completed, comply with the plan. In particular, the FECC must be acknowledged by all Federal entities as the lead of ESF#2 for the region.

As written, the NRP ESF#2 Annex states, “Conflicts regarding NS/EP telecommunications priorities and resources that cannot be resolved at the [Joint Field Office (JFO)] by the Federal Coordinating Officer (FCO) and the FECC are passed to the NCC for coordination with the Joint Telecommunications Resources Board (JTRB).” The update of the ESF#2 Annex should clearly articulate that the NCC escalates issues to OSTP (via the Manager or Deputy Manager of the NCS). This escalation process should inform appropriate DHS leadership but not seek permission because the NCS and NCC perform the ESF#2 functions on behalf of OSTP. The intent of ESF#2 as written appears to support this. However, clarification could greatly assist the new Manager of the NCS (the incoming Assistant Secretary for Cyber Security and Telecommunications) and reduce the opportunities for delays in recovering communications that support NS/EP services. To accomplish the requirements under E.O. 12472, the NCC needs clear escalation processes and policy interpretations that support the involvement of the private sector.

During the Hurricane Katrina response, numerous NCC member requests hit dead ends or went unfulfilled because inadequate processes were in place for escalating issues to resolution or were delayed as a result of policy interpretations. A potential partial solution for this problem is the use of a REMEDY–like trouble-ticketing system that would help track and escalate incidents raised to the NCC for resolution or assistance. This type of system also would provide the NCS with a valuable forensic data set for developing situational awareness reports and analysis after an event.

Figure 3.1 ESF#2 Alignment with NIMS Framework



For the NCC to more effectively respond to NS/EP incidents, the following steps should be taken within the next year.

- **The Secretary of Homeland Security, the Director of the Office of Science and Technology, the Secretary of Defense, and other ESF#2 Federal support agencies should develop and implement policies and procedures with respect to: (1) managing and escalating requests from the NCC, and (2) the delineation of authorities and responsibilities when ESF#2 is invoked.**
- **ESF#2 Federal support agencies should support the development of and comply with the ESF#2 Federal Operations Plan.**
- **The NCC should facilitate this process by creating a common procedure and taxonomy that multiple Government stakeholders can follow when working with the NCC and its members.**
- **DHS and ESF#2 support agencies must acknowledge the FECC as the lead for ESF#2 in the region.**
- **DHS must clarify the NCC's alignment within the NIMS framework.**
- **DHS in collaboration with other NCC stakeholders need to develop a process for escalating issues to DHS leadership and the White House and communicating status updates.**
- **NCC should institute a trouble ticket system to track requests for assistance.**

3.1.4 Incident Management/Emergency Response

Incident management and response is one of the most valuable functions of the NCC. Most NCC activities focus on planning operations to respond to an incident of national significance. An incident of national significance can be declared once State and local authorities request assistance, more than one Federal department or agency becomes substantially involved, or the Secretary of Homeland Security is directed to manage a domestic incident by the President.²⁰

After one of these triggers has occurred, the NRP should be followed. ESF#2–Communications ensures the provision of Federal communications support to Federal, State, and local response efforts following a Presidentially declared major disaster, emergency, or extraordinary situation under the NRP. The NCCTF has determined that many incident response problems arise when Government responders do not follow the processes laid out in the NRP; a similar problem occurred during the 2005 hurricane season.²¹ Additional work is needed to clearly articulate the private sector's role in the NRP and the NIMS. Furthermore, an awkward linkage exists between

²⁰ *National Response Plan*. December 2004. pg. 4.

²¹ *GAO-06-365R Preliminary Observations on Hurricane Response*, February 1, 2006.

the Cyber Annex and ESF#2 Annex, which could result in confusion and potential authority issues between DHS and OSTP.

As part of this process, it is critical that a single entity—the NCC—maintain responsibility for communications coordination during a disaster, with remaining entities working within their various NRP-delineated roles and responsibilities.

Regional Coordination: One challenge during major disaster response efforts has been effective coordination at the regional level. Per NIMS, the Federal Government organizes its response coordination structure regionally. The *National Telecommunications Management Structure (NTMS)*, NCS Directive 3-4, May 4, 1992,²² called for a “Regional Emergency Management Team Communications Functional Group/Regional Coordinating Center (REMT CFG/RCC).” The REMT CFG/RCC was to be composed of regionally based Federal and communications industry representatives capable of serving as an alternate NCC. The task force recognized that the NTMS was designed to provide a survivable coordinating management structure during a catastrophic event; however, recent response experiences during the 2005 hurricane season demonstrate that when regional emergencies occur, a similar structure would improve coordination on the regional level.

The NSTAC recommends that OSTP and the Homeland Security Council join with the C-SCC and IT-SCC to support an industry-led task force, with the primary goal of planning a regional communications and IT coordinating capability in the Gulf Coast and Southeastern regions before the 2006 hurricane season. Subsequently, the task force will determine the best approach for a long-term regional communications and IT coordinating capability that can serve all regions of the Nation. The task force would need to address the following issues: (1) how industry should coordinate regional response; (2) what funding sources might be required for this regional capability; (3) whether the capability should be virtual or based from a brick-and-mortar facility; (4) whether current Federal, State, local, and tribal authorities participate in or otherwise support such industry coordination; and (5) how a regional coordination capability could best garner recognition and support from industry and Government entities. In addition, the task force will examine how to assist in the DHS efforts in building integrated homeland security capabilities, including incorporating dedicated communications industry personnel with direct NCC linkages into the regional field offices. This effort would assist in achieving not only Secretary Chertoff’s goal of establishing a core disaster workforce able to take full advantage of DHS assets, resources, and capabilities, but also the White House’s goal of ensuring situational awareness by establishing rapid deployable communications and instituting a structure for consolidated operational reporting to DHS.

The NCCTF suggests that the regional communications and IT coordinating capability be led by the FECC, within or as a virtual capability of the JFO. This kind of arrangement would significantly improve the ability of the Government and private sector to respond to major incidents.

²² The task force assumes that this 1992 directive is currently in force. See Appendix E for the text of the directive.

In addition to regional coordination capabilities, industry members have reported that they have been unable to include representation at the JFO during incidents of national significance as a result of Government space limitations. Prior plans, including the NTMS Directive, included processes for industry participation in response activities, but the NRP includes no such processes. During Hurricane Rita in September 2005, the JFO and the State Emergency Operations Center (EOC) were collocated in Austin, Texas, which allowed for improved coordination among Federal, State, and local authorities and industry responders.

The communications industry must be present at the JFO, and this need must be considered as the site for the JFO is being selected. The FECC should coordinate, and the JFO should accommodate, the incorporation of on-site communications industry personnel with direct linkages with the NCC to provide for regional company-to-company and industry-to-Government information sharing and coordination.

Local Coordination: The NCCTF also determined that many incidents of national significance begin as localized events and are therefore managed locally, at least initially. Meanwhile, for incidents that remain local, NCCTF members have encountered expectations that the NCC will coordinate response. Communications companies become involved at the local level through their responsibility to support their customers, with initial response and coordination handled by representatives in the field. The NCC provides an escalation capability for the companies to address issues that cannot be handled at the local levels. As the situation intensifies, corporate processes will escalate the issue, and NCC representatives will be incorporated into response activities. NCCTF members suggest that NCC industry members establish a formal process for local industry coordination.

Reporting: The reporting process became an issue during the 2005 hurricane season. Under current procedures, the industry partners of the NCC provide detailed information about network restoration issues, verbal and written, at regularly scheduled intervals. The NCC culls this data and provides detailed situation reports during emergencies multiple times daily (depending on the level of activity) to the DHS National Infrastructure Coordinating Center; Homeland Security Operations Center; Assistant Secretary for Infrastructure Protection; and occasionally, the White House Situation Room directly. DHS, in turn, submits a high-level summary of the communications sector status, including other infrastructure statuses, to the EOP. Other agencies (e.g., FCC, DOD, National Guard) added to the confusion by collecting different information at the Federal and local levels at various intervals, resulting in conflicting data and directing resources away from handling restoration issues. During the hurricane after-action process, the EOP stated that it was receiving conflicting and incomplete reports regarding the communications status. The NCCTF concluded that to expedite the information flow, the NCC should submit its situation reports directly to the EOP concurrently with transmissions to other stakeholders; those stakeholders should contact the NCC and NCC industry members directly with questions. Furthermore, all aforementioned stakeholders requesting restoration data need to work together to set common requirements for situation reports and reporting cycles to address the data consistency issue and reduce the burden on industry.

Training and Exercises: The task force believes the NCS-prepared and -sponsored ESF#2 Emergency Response Training and Exercise program should be improved, with a focus on enhancing coordination among industry members and Federal, State, and local responders during

incidents of national significance. The goal would be to help all parties become more comfortable with the NRP process, the ESF#2 process, and the underlying communications infrastructure and how it functions. The program would be collaboratively developed, broadly participatory, and regularly evaluated. The exercises themselves should be modeled on the level of detail and professionalism demonstrated by military programs and should include participation by communications and IT firms. As noted in the *NSTAC Report on Next Generation Networks*, the key to this program's success will be the implementation of lessons learned into future activities. Industry must be involved from the inception of the process, including creating objectives for the exercise. Some companies might require compensation if involved in the planning process.

National Special Security Event (NSSE) Coordination: Unlike most other incidents of national significance, NSSEs provide Government with an opportunity for advanced planning. During the coordination process for past NSSEs, the NCC has identified gaps in communications between Federal level planning and private sector planning around these events. In June 2004, the NCC issued a report, *Preparing for a National Special Security Event*, which described service provider and NCC preparation activities for NSSEs. The report recommends engaging the NCC from the outset of the event management process, involving the NCC members in development of requirements to support communications for the event. Despite repeated requests by industry to be involved in the coordination of communications requirements for NSSEs, the task force found that the NCC and the private sector are neither consistently invited nor allowed to be fully involved in the planning process.

Cyber Incident Coordination: The NCCTF and the NGNTF jointly sponsored a meeting of SMEs on August 30, 2005, to discuss incident management in next generation networks. Attendees emphasized that improved relationships between communications and IT companies and Government would also be helpful. The NRP Cyber Incident Annex guides response activities for cyber events, yet it is not widely understood; and it does not enable an understanding of a cyber "incident of national significance" or the relationship between the private sector and the Federal Government. The National Cyber Security Division (NCS) takes the lead in addressing these activities with support from the United States Computer Emergency Readiness Team (US-CERT), the Interagency Incident Management Group, the National Cyber Response Coordination Group, and the NCS. One finding of the SME meeting was that the NCC should reach into the IT vendor community; however, the NCC has neither a pre-established relationship with all of the vendors nor a mechanism by which it can communicate with them. Although the NRP Cyber Incident Annex recognizes the importance of coordinating with the private sector during events and the limitations of Federal authority to exert control over cyberspace, it does not specify mechanisms for coordinating with the private sector during events or specify industry's role in the response effort. The reunification of communications and IT into a single sector would improve the NCC's access to the IT vendor community if a cyber incident occurred by expanding formal relationships and improving mechanisms for communication between communications and IT vendors.

For the NCC to more fully prepare for incidents that affect NS/EP communications, the following steps should be taken over the next year.

- **The Office of Science and Technology Policy and the Homeland Security Council will join with the C-SCC and the IT-SCC to support an industry-led task force with the primary goal of planning a regional communications and information technology coordinating capability in the Gulf Coast and Southeastern regions prior to the 2006 hurricane season. Subsequently, the task force will determine the best approach for a long-term regional communications and information technology coordinating capability that can serve all regions of the Nation. The task force should primarily be made up of industry representatives, as well as Federal, State, and local Government representatives.**
- **DHS should plan for the regional communications and information technology coordinating capability to be within or a virtual capability of the JFO. The NCC should modify the ESF#2 Annex and operations plan to account for this requirement.**
- **DHS should collocate JFOs with the EOC during crises whenever possible to improve coordination with State and local officials.**
- **The NCC should disseminate its situation reports to the EOP Situation Room concurrently with transmissions to other Government stakeholders.²³**
- **DHS should identify the NCC as the single point of focus for communications sector information dissemination during a crisis, work with all relevant stakeholders to identify key data points needed, and agree to a process to cut down on repeated requests for incident and response data.**
- **The NCS and General Services Administration (GSA) should include communications service providers in the planning and execution of emergency response training exercises.**
- **DHS should fully engage the NCC and its industry members in NSSE planning process.**
- **DHS should revise the NRP Cyber Incident Annex to clarify what constitutes an Internet-related “incident of national significance” and what role the Government would serve in the event such an incident occurs.**

²³ E.O. 12472, Section 1 (b) (2) states that “. . .the mission of the NCS shall be to assist the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in . . . the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order [Executive Office Responsibilities]; and the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.”

- **The NCC must develop a Concept of Operations (CONOPS) document for how the NCC responds to cyber events.**
- **DHS should consider designating a senior member of the Office of General Counsel or an appropriate advisor from the Secretary's office to be on-call to respond to potentially complex legal or jurisdictional issues that may arise from cyber or communications crises that could trigger response under either ESF#2 or the Cyber Annex. Such an individual would work directly with the Secretary's Office, the Assistant Secretary for Cyber Security and Telecommunications, and the leadership from the NCC and NCSA, to eliminate possible confusion and ensure an appropriate Federal response.**

3.1.5 Policy

HSPD-7 mandated a review of NS/EP communications policy to be led by the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs. Any major changes in NS/EP policy could affect NCC operations. The NSTAC recognizes that the scope of NS/EP has changed as a result of convergence and next generation architecture. For example, nontraditional communications providers played a role during the Hurricane Katrina response activities and those companies should also participate in communications response planning and be recognized for their role in response efforts.

For the NCC to prepare for potential policy changes, the following steps should be taken over the next year.

- **DHS will provide the NCC with a status update on the HSPD-7-mandated review of NS/EP policy.**
- **DHS should emphasize prioritization as its key mission, focusing on the key needs and missions of the Federal Government, that all companies can follow and incorporate into business continuity plans.**

3.2 Three-Year Roadmap Actions

During the next three years, the NCC should focus on key issues of revisiting its value proposition and modifying its organizational structure and incident management in accordance with the combination of the communications and IT sectors.

3.2.1 The New Value Proposition

September 11 and Hurricane Katrina have been major catalysts to growth and change around information sharing and crisis coordination and disaster response capabilities. Since September 11, communications companies working in the NCC have realigned coordination from DOD to DHS, and continued working with FEMA as that relationship evolved. In addition, network operators and service providers have changed, yet much of the NCC membership

remains the same. In addition, as companies exist in the new network environment and “professionalization” of crisis response in a post-September 11 environment, it is important to reexamine the NCC’s value proposition.

The NSTAC recognizes that the current environment is undergoing significant changes and must be continually reviewed to determine its effect on the operations and value of the NCC. The task force determined that over the next three years, the value proposition should be revisited to reassess the value Government receives from the organization and the value received by resident and nonresident private sector representatives. During the process, alternative organizational models and methods could be evaluated, such as benefits of a virtual operations center and other collaborative models as membership and missions expand. Other issues to be assessed include the impact on information sharing with the influx of new companies and participants into the NCC, the potential for different types of membership for steady-state versus incident management and response, and the evolution of direct coordination and mutual aid.

The NSTAC recognizes that the current environment is undergoing significant changes and by waiting a couple years to revisit these issues, it might gain a better understanding of the impact changes might have on the effectiveness and value of the NCC. To that end, the NSTAC recommends that the Secretary of Homeland Security be directed to lead an effort with other Government stakeholders, including the OSTP and NORTHCOM, to examine the value received from the NCC relationship and, if sufficiently supported, commit the resources necessary to strengthen and support the organization and its mission. In parallel, the NCC should examine the value proposition of membership to the Government and private sector.

To ensure that the NCC organization continues to have value to both industry and Government participants, the following steps must take place over the next three years.

- **DHS will lead an effort with other Government stakeholders (including OSTP, DOD, and others) to examine the value received from the NCC relationship and, if sufficiently supported, commit the resources necessary to strengthen and support the organization and its mission.**
- **The NCC will examine the value proposition of membership, to both the Government and the private sector.**
- **The NCC should assess the impact on information sharing if the NCC membership is increased, and should assess the possibility that membership growth may jeopardize the culture of trust, as well as mechanisms to maintain trust in the face of necessary growth.**
- **The NCC should review the short-term goals and directives set forth above, and should evaluate the success of the NCC in meeting those requirements and needs.**
- **The NCC should examine the impact of direct, company-to-company mutual aid and coordination on the role of the NCC.**

3.2.2 IT and Communications

As previously mentioned, HSPD-7 defined communications and IT as separate sectors; the NCCTF believes the sectors, once joined as the I&C sector, are inseparable and should be rejoined from a policy perspective. As communications companies and their vendors have long been NCC members, it makes sense that as the NCC grows to include Internet, satellite, and data service providers, so too should their vendors join. The NCCTF therefore recommends that the sectors' respective ISACs and SCCs engage in a dialogue, with the intent to combine to improve incident response coordination, enhance the capability to make threat/vulnerability linkages between the sectors, and preserve resources.

The mission of the IT ISAC, the IT sector information-sharing hub, is comparable to the NCC's information sharing and analysis mission.²⁴ The primary operational mission of the IT ISAC, as defined in its organizational documentation, is to "report and exchange information regarding incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices, and other protective measures." Secondary missions include participation in the development and execution of exercises simulating attacks against infrastructure and leading an industry-wide process to evolve the structure and technology for a secure information-sharing conduit. In addition, the communications sector has also established a policy-oriented C-SCC that includes many private sector members of the NCC and other relevant communications sector entities.

In the NCCTF's view, a combined NCC–IT ISAC organization would provide value in the following ways:

- Provide enhanced support to the NS/EP community by increasing coordination with nontraditional communications providers (e.g., ISPs, unlicensed wireless service providers);
- Improve incident response coordination during cyber events by having a broader network of communications service providers, managed security service providers, and equipment and software manufacturers;
- Expand the scope of information sharing between the communications and IT sectors on a broad array of incidents, threats, attacks, vulnerabilities, solutions, and best practices; and
- Preserve industry and Government resources by avoiding duplication of effort.

The expanded NCC would be a cross-sector industry/Government facility with a round-the-clock watch and would have additional virtual operations capabilities that could be elevated to full strength during emergencies. As also discussed in the *NSTAC Report on Next Generation Networks*, such a center would improve coordination between industry and Government among communications and IT industry members. In this three-year period, members should assess which sectors, if any, should be invited to participate either in a virtual or physical capacity during a crisis. In the future, the electric power sector might be invited to participate, as well as transportation or oil and gas. Any evolution or change would require development of a

²⁴ See Appendix F for more information on the IT ISAC.

CONOPS document to outline the processes, roles, and responsibilities of the combined sectors in response to cyber events, as well as incidents of national significance and other issues.

Response to recent events has shown that the NCC faces a lack of sufficient resources to plan for and manage very large events, as well as blended physical/cyber events. It is recognized that the proposed expansion of the NCC to include IT sector members will place further strain on the NCC's resources. Therefore, the NCC must be able to scale appropriately to respond to multiple events and multiple sectors, including augmentation from NCS member organizations. The NCCTF suggests that DHS ensure that the NCC has the resources to effectively prepare and respond to incidents of national significance.

The proposed combination of the two sectors would coincide with the integration of cyber and communications security missions within DHS. In the Second Stage Review, Secretary Michael Chertoff proposed the establishment of an Assistant Secretary position for cyber security and telecommunications to "centralize the coordination of the efforts to protect the technological infrastructure."²⁵ Logically, the NCS and NCSD will be brought together under the new. The evolution of the NCC's organizational structure to integrate with the two sectors should coincide with the integration of the NCS and NCSD, including US-CERT. Because the organizational structure might change with the sectors combining, the operating structure and operating procedures would need to evolve as they have with past mission and functional modifications; however, the NCCTF elected not to make recommendations in this area because much of the structural change envisioned will be made by Government, with industry responding to meet the situation.

For the NCC to reflect the reality of a converged communications industry and effectively plan and respond to incidents of national significance, the following steps should be taken during the next three years.

- **The NCC should reach out to the IT ISAC to engage in a dialogue aimed at bringing the two sectors and bodies closer together, if not integrating completely.**
- **The NCC should combine with the IT ISAC to maximize cooperation between the communications and IT sectors as they continue to converge.**
- **The NCC Watch and the IT ISAC Watch should combine to facilitate more effective response to cyber events.**
- **The C-SCC and the IT-SCC should explore the benefits of combining to preserve resources.**
- **DHS should provide the resources for the NCC to plan for and manage both physical and cyber events, and to accommodate the NCC's expansion to include the IT community.**

²⁵ "Statement of Secretary Michael Chertoff, U.S. Department of Homeland Security, Before the United States Senate Committee on Commerce, Science, and Transportation." July 19, 2005.

<http://www.dhs.gov/dhspublic/display?theme=45&content=4643&print=true>.

- **The NCC must develop a CONOPS document for responding incidents of national significance, including cyber events, which includes the participation of the IT sector.**
- **The NCC should integrate with US-CERT to more effectively respond to cyber events.**

3.2.3 Industry Analysis

As mentioned, NCC industry members must have a greater role in NCS analysis efforts from the beginning of the process, rather than participating at the final review only after analyses have been completed. This will improve the accuracy and effectiveness of these threat and vulnerability analyses. To facilitate this greater inclusion of industry, formal contracts may be necessary between member companies and the NCS.

For the NCS to improve its analysis function, DHS should work to put contracts into place with the NCC's industry partners to allow for their full participation in infrastructure analyses.

3.3 Five-Year Roadmap Actions

Within five years, the NCC should focus on expanding its relationships with those sectors with which it shares critical interdependencies (e.g., electric power sector) and with international cyber watch centers. The NCCTF also identified ongoing actions to expand the NCC's role in international activities.

3.3.1 Incident Management/Emergency Response

Over the next five years, the NCC should engage in a review of the relationships it maintains with its membership and continue to refine or enhance the value proposition to the Government and the private sector. Assuming the NCC has effectively integrated IT communications providers, it should begin to focus on other closely related sectors. For example, the NSTAC established the Telecommunications and Electric Power Interdependency Task Force (TEPITF) to examine NS/EP issues associated with communications and electric power interdependencies; this task force involved participation from the electric power industry and improving relationships with the sector. Additional collaboration or new processes might be needed to facilitate incident response. In the future, there will be a need to further enhance these relationships in the NCC.

For the NCC to effectively plan for and respond to incidents with cross-sector implications, the following steps should be taken within five years.

- **The NCC should expand its relationships with operations centers for other sectors with critical interdependencies, such as the energy sector.**

- **The NCC industry and Government members should make a concerted effort to establish formal agreements within the sectors on how each will improve incident response and coordination.**
- **The industry-led regional coordinating capability task force should determine details for the incorporation of all the regional communications coordination capabilities.**

3.3.2 International

NCCTF members agree that the NCC will continue to have a predominantly domestic focus. However, the communications infrastructure, including wireline, wireless, and satellite communications, is inherently international, with international cooperation becoming increasingly necessary during incidents. The global nature of the NGN means that methods for managing incidents of national significance may require international cooperation.²⁶ Industry has led the way internationally, with global interconnected networks, and Government must respond to that with appropriate plans for international incident response. The NCCTF believes that within five years, it is likely that an international operations center for the communications infrastructure will come into existence, and the NCC should be a part of that.

US-CERT coordinates with domestic and international organizations, including international CERTs. Meanwhile, the NCSA maintains an ongoing, real-time dialogue with US-CERT partners through the US-CERT portal and performs outreach to the international community. The NCC should be part of this structure because the communications infrastructure it supports is integral to networks, domestically and internationally.

The NCC participates in international activities through NATO, the ITU, and with Canada on various crisis coordination, mutual assistance, and CIP issues. As the NCC increases its role in cyber response activities, which are often inherently international, there will be a need to strengthen its international relationships to improve response coordination.

Many major U.S. communications providers have international components to their businesses, as most communications networks are inherently international. Although U.S. local exchange carriers have entered into voluntary mutual aid agreements with one another to help provision equipment, supplies, or personnel during an emergency, the *Tampere Convention on the Provision of Telecommunications Resources for Disaster Mitigation and Relief Operations*²⁷ provides a legal instrument for sharing communications resources by removing regulatory and political barriers on the use and import of communications equipment during international disasters. The United Nations treaty went into force after 30 countries ratified the convention on January 8, 2005. The United States signed the agreement in November 1998, but the Senate has not ratified the agreement. Though the treaty has not been ratified, the DOD has worked through the United Nations to provide communications resources during disasters. The NCC could be an additional POC for assisting in international emergency communications response efforts.

²⁶ NSTAC's Next Generation Networks Task Force Report, March 2006.

²⁷ <http://www.reliefweb.int/telecoms/tampere/index.html>.

The NCC also should work with the NCS to ensure NS/EP requirements are considered in the standards-making process. At the 10th Global Standards Collaboration (GSC) meeting in August 2005, hosted by the European Telecommunications Standards Institute (ETSI), the GSC adopted a resolution on emergency communications to encourage further standardization activities and collaboration in national, regional, and international activities. Specific findings and recommendations are as follows:

- Encouraging cooperation on developing standards applicable for existing and future systems, including priority access to emergency numbers and by emergency personnel;
- Encouraging cooperation on emergency communications activities, such as Project MESA, and providing forums to collect aggregated Government user requirements;
- Encouraging the harmonization of terminology, such as use of the term “emergency communications” instead of “emergency telecommunications,” including the widest range of new systems, services, and technologies;
- Drawing attention to the need to examine the characteristics of emergency communications over packet-based networks; and
- Enhancing collaborative efforts at the international level to make efficient use of resources.

As incident response efforts expand globally, the Assistant Secretary for Cyber Security and Telecommunications, on behalf of NCC concerns, should enhance participation in these standards organizations to ensure future systems are capable of meeting the needs of NS/EP users.

For the NCC to effectively plan for incident response in an increasingly international environment, the following steps should be taken when applicable.

- **The NCC should engage with the US-CERT and the NCSD on international coordination, working to be included in the organizations dialogue with international counterparts.**
- **The Assistant Secretary for Cyber Security and Telecommunications should enhance participation in regional and international standards efforts to provide input into the requirement collection process, especially related to priority services in the packet-based network environment.**

3.4 Potential Roadblocks

Numerous possible roadblocks exist for each roadmap area. These roadblocks are in areas in which the NCCTF might have been unable to recommend specific actions as remedies.

Organizational Structure

- *Limited company resources for participation in industry-Government groups:* Company participation in the NCC and related groups is pro bono. As detailed in Section 2.4.2, companies participate for various reasons, including information-sharing opportunities

and an ability to directly request Government assistance in emergencies. Recently, industry members were asked to participate in additional industry-Government groups, such as the SCC. This additional participation can be costly to industry, and corporations are hesitant to contribute additional resources when there is not necessarily a clear return.

- *A clear value proposition:* Concern has been expressed that industry gives more than it receives to DHS in the event of a crisis. It is critical that the NCC and its members agree on a value proposition that encourages DHS to give a clear benefit to the private sector in exchange for its participation in these activities.
- *Hesitancy of some IT/communications companies to work in close coordination with Government:* The communications sector has traditionally been heavily regulated, but the IT sector has seen little regulation; companies that do not currently have a close relationship with Government, particularly in the less-regulated IT area, may be wary that such a relationship may lead to regulation.
- *Lack of Government resources allotted to NCC missions:* As detailed in Section 3.1.4, the NCC determined during Hurricane Katrina that it did not have sufficient resources to respond to such an event. Meanwhile, the NCCTF has recommended expanding the NCC's scope to include the IT industry and improving its involvement in exercise programs. For the NCC to successfully accomplish its current and expanded missions, **an increase in resources will be essential.**

Information Sharing and Analysis

- *Lack of data protection assurances:* The creation of DHS has raised questions about how private-sector information given to Government is shared within Government and protected from disclosure. Members have determined that the information they provide to Government is not always treated as confidential. In addition to finalizing rules for PCII, DHS must clarify its policy for the use and protect other voluntarily provided information outside the PCII program.
- *Risk related to revealing vulnerability information:* Many industry members do not want to potentially put customers at risk by revealing vulnerability data. Combined with dwindling trust among industry NCC members and an unclear DHS policy for protection of industry information, this issue has generated significant concern among industry members.

Incident Management/Emergency Response

- *Gap between expectations and reality for tactical coordination at local levels:* The NCC's mission is geared toward incidents that affect NS/EP communications. However, NCCTF members have periodically encountered expectations that the NCC will respond with tactical coordination for much more localized incidents. The NCC must find a way to reconcile these expectations with the reality of its mission.
- *Increased demand for outage, disruption, or incident reporting by DHS and FCC, as well as DOD, the National Guard, and other agencies:* Since the inception of DHS, the NCCTF has found that NCC industry members frequently are interrupted during incident response activities by requests for customer outage information from the FCC and DHS agencies. This takes valuable time and resources from the NCC's core activities. If outage reporting is set to be an additional NCC responsibility, additional resources may be necessary during incident response to handle such public affairs requests.

Policy

- *Potential changes to NS/EP policy as a result of the HSPD-7 NS/EP communications policy review:* Any major changes to NS/EP policy resulting from the aforementioned review of HSPD-7 (see Section 3.1.5) would likely have an impact on NCC programs. For the NCC to properly prepare for such changes, it would be helpful for DHS to keep the NCC apprised of the review's progress.

3.5 Conclusion

The NCC's next five years will bring opportunities and challenges, many of which have been described in this report. The task force has outlined more than 40 recommendations and steps that can be taken over the next five years to take advantage of opportunities, such as realizing intersections with the IT sector, and to address challenges in information sharing, training, and response.

The response to Hurricane Katrina underscored the importance of national-level sector coordination, and it highlighted many areas in which operations can be improved. Some of the recommendations in this report overlap with other after-action documents, including the White House Katrina Report, titled *The Federal Response to Hurricane Katrina Lessons Learned*. For example, the White House recommended revisions to the NRP and NIMS, as well as improvements in training on related procedures and processes.²⁸ The NSTAC's recommendations should be incorporated into those processes, particularly in regard to issues such as "who's in charge" of the NCC, as well as incident response training for Federal responders and industry personnel. Similarly, the NSTAC's recommendation to initiate a task force to develop a regional coordination capability should be synchronized with the development of Homeland Security Regions proposed in Recommendation 4 of the White House's report. Meanwhile, the NSTAC and the NCC should be consulted and should receive status reports on the NS/EP communications policy review and on the development of a National Emergency Communications Strategy, as discussed in Recommendations 33 and 34.

In addition to Presidential recommendations offered in Section 4, the NSTAC proposes a roadmap for the future (see Appendix C) to guide DHS and the NCC in implementing the recommendations and steps discussed in this report.

4.0 RECOMMENDATIONS TO THE PRESIDENT

Based on the NCCTF's analysis of issues facing the NCC, the NSTAC makes the following recommendations, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, and other existing authorities, that the President—

²⁸ Recommendations 1 and 2 in *The Federal Response to Hurricane Katrina Lessons Learned*.

- **Direct the Secretary of Homeland Security, the Director of the Office of Science and Technology, the Secretary of Defense, and other ESF#2 Federal support agencies to develop and implement policies and procedures with respect to: (1) managing and escalating requests from the NCC, and (2) the delineation of authorities and responsibilities when ESF#2 is invoked.**

To implement this recommendation—

- ESF#2 Federal support agencies should support the development of and comply with the ESF#2 Federal Operations Plan.
 - The NCC should create a common procedure and taxonomy that multiple Government stakeholders can follow when working with the NCC and its members.
 - DHS should emphasize prioritization as its key mission, focusing on the key needs and missions of the Federal Government that all companies can follow and incorporate into business continuity plans.
 - DHS and ESF#2 support agencies must acknowledge the FECC as the lead for ESF#2 in the region.
 - DHS must clarify the NCC's alignment within the NIMS framework.
 - DHS, in collaboration with other NCC stakeholders, should develop a process for escalating issues to DHS leadership and the White House and communicating status updates.
 - The NCC should institute a trouble-ticket system to track requests for assistance.
 - The NCC should disseminate its situation reports to the EOP Situation Room concurrently with transmissions to other Government stakeholders.
 - DHS will provide the NCC with a status update on the HSPD-7-mandated review of NS/EP policy.
- **Direct the Office of Science and Technology Policy and the Homeland Security Council to join with the C-SCC and the IT-SCC to support an industry-led task force with the primary goal of planning a regional communications and information technology coordinating capability in the Gulf Coast and Southeastern regions prior to the 2006 hurricane season. Subsequently, the task force will determine the best approach for a long-term regional communications and information technology coordinating capability that can serve all regions of the Nation. The task force should primarily be made up of industry representatives, as well as Federal, State, and local Government representatives.**

To implement this recommendation—

- DHS should plan for the regional communications and IT coordinating capability to be within or a virtual capability of the JFO.
 - DHS should collocate JFOs with the EOC during crises whenever possible to improve coordination with State and local officials.
 - The industry-led regional coordinating capability task force should determine details for the incorporation of all the regional communications coordination capabilities.
- **Direct the Secretary of Homeland Security to expand the NCC to include both communications and IT companies and organizations. This would be a cross-sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies.**

To implement this recommendation—

- The NCS should work with NCC industry members to clarify the process for membership as it pertains to the NS/EP function.
- The NCC must accept the new mission statement, proposed by the NCCTF, to more clearly define its vision, mission, and functions.
- The NCC must establish a working group to facilitate the transition to an NCC that includes broad representation from within the existing IT sector. This group will address structural, funding, and operational issues.
- The NCC must facilitate the ability of nontraditional communications providers to respond to NS/EP incidents.
- The NCS should convene a conference for communications and IT providers to plan for an improved focus on cyber issues, including preparing a vision on how to combine the NCC and IT ISAC.
- DHS should begin planning for a multi-industry coordinating center that would incorporate and be modeled on the NCC. The center would initially focus on Communications and IT Sectors.
- The NCC should conduct outreach to enhance membership in underrepresented communications subsectors, including cable network operators, ISPs, satellite operators, broadcast infrastructure operators, and unlicensed wireless operators.
- DHS should provide the resources for the NCC to plan for and manage physical and cyber events and to accommodate the NCC's expansion, including the IT community.

- The NCC should reach out to the IT ISAC to engage in a dialogue aimed at bringing the two sectors and bodies closer together, if not integrating completely.
 - The NCC should combine with the IT ISAC to maximize cooperation between the communications and IT sectors as they continue to converge.
 - The NCC Watch and the IT ISAC Watch should combine to facilitate more effective response to cyber events.
 - The C-SCC and the IT-SCC explore the benefits of combining to preserve resources.
 - The NCC should expand its relationships with operations centers for other sectors with critical interdependencies, such as the energy sector.
 - The NCC industry and Government members should make a concerted effort to establish formal agreements within the sectors on how each will improve incident response and coordination.
- **Direct the Secretary of Homeland Security to engage the private sector in critical infrastructure protection activities by increasing the flow of threat information to the private sector, facilitating private sector participation in impact analyses, and clarifying policies for the protection of private sector information.**

To implement this recommendation—

- DHS should clarify its policy with respect to the use of private sector information and those persons or organizations that will have access to such information.
- The NCS should enter into agreements to broaden its collaboration with communications service providers before and throughout the impact-analysis process. Such collaboration would significantly enhance the value and validity of the analysis.
- The NCS should involve industry experts at an earlier stage in the threat, vulnerability, and impact analysis processes in order to produce more accurate assessments.
- DHS should increase the flow of threat information or issues of concern through the NCC, including information regarding Government-owned assets or activities that might potentially jeopardize industry or Government assets.
- NCC members should improve information sharing among industry members and between industry and Government. The focus in this effort should be (1) reducing risk through NDAs; (2) partitioned information-sharing systems; (3) improved modeling capabilities; and (4) indemnification issues.

- DHS should work to put such contracts into place with the NCC's industry partners to allow for their full participation in infrastructure analyses.
- **Direct the Secretary of Homeland Security to improve the ESF#2 Emergency Response Training and Exercise program, with a focus on enhancing coordination among industry members and Federal, State, and local responders during incidents of national significance. This program should focus on sector interdependencies for both physical and cyber threats, and would aim to produce actionable results. Industry must be involved from the earliest planning stages.**

To implement this recommendation—

- The NCS and GSA should include communications service providers in the planning and execution of emergency response training exercises.
- DHS should identify the NCC as the single focus point for communications sector information dissemination during a crisis, should work with all relevant stakeholders to identify key data points needed, and should agree to a process to limit repeated requests for incident and response data, or conflicting information.
- **Encourage the Secretary of Homeland Security to improve the Federal Government's cyber response strategy to delineate roles and responsibilities of Government and the private sector in the NRP, aligning communications and cyber operations centers, and enhancing relationships with international CERTs.**

To implement this recommendation—

- DHS should revise the NRP Cyber Incident Annex to clarify what constitutes an Internet-related "incident of national significance" and what role the Government would serve in the event such an incident occurs.
- The NCC must develop a CONOPS document for how the NCC responds to cyber events.
- The NCC must develop a CONOPS document for responding to incidents of national significance, including cyber events, which includes the participation of the IT sector.
- The NCC should integrate with US-CERT to more effectively respond to cyber events.
- The NCC should engage with US-CERT and the NCSD on international coordination, working to be included in the organizations' dialogue with international counterparts.
- The Assistant Secretary for Cyber Security and Telecommunications should enhance participation in regional and international standards efforts to provide input into the requirement collection process, especially related to priority services in the packet-based network environment.

- DHS should consider designating a member of the Office of General Counsel or an appropriate advisor from the Secretary's office to be on-call to respond to potentially complex legal or jurisdictional issues that may arise from cyber or communications crises that could trigger response under either ESF#2 or the Cyber Annex. Such an individual could work with the new Assistant Secretary, leadership from the NCC and NCSD, and the Secretary's Office to eliminate possible confusion and ensure an appropriate Federal response.
- **Direct the Secretary of Homeland Security and other Government stakeholders to examine the value received from the NCC relationship and, if sufficiently supported, commit the resources necessary to strengthen and support the organization and its mission.**

To implement this recommendation—

- The NCC will examine the value proposition of membership, to both industry and Government.
- The NCC should assess the impact on information sharing if the NCC membership is increased, and should assess the possibility that membership growth may jeopardize the culture of trust, as well as mechanisms to maintain trust in the face of necessary growth.
- The NCC should review the short-term goals and directives set forth above, and evaluate the success of the NCC in meeting those requirements and needs.
- The NCC should examine the impact of direct, company-to-company mutual aid and coordination on the role of the NCC.

APPENDIX A

**TASK FORCE MEMBERS, OTHER PARTICIPANTS, AND GOVERNMENT
PERSONNEL**

TASK FORCE MEMBERS

Verizon Communications, Inc.	Mr. James Bean (Chair)
Sprint Nextel Corporation	Mr. John Stogoski (Vice Chair)
AT&T, Inc.	Mr. Harry Underhill
BellSouth Corporation	Ms. Cristin Flynn Goodwin
Cingular Wireless LLC	Mr. Kent Bowen
Computer Sciences Corporation	Mr. Guy Copeland
CTIA—The Wireless Association	Mr. Chris Guttman-McCabe
Lockheed Martin Corporation	Dr. Al Dayton
Lucent Bell Labs	Mr. Richard Krock
Microsoft Corporation	Mr. Phil Reitingner
Nortel International, Inc.	Dr. Jack Edwards
Qwest Communications	Mr. Thomas Snee
Raytheon Company	Mr. Frank Newell
SAIC, Inc.	Mr. Hank Kluepfel
The Boeing Company	Mr. Robert Steele
United States Telecom Association	Mr. David Kanupke
VeriSign, Inc.	Mr. Michael Aisenberg

OTHER PARTICIPANTS

AT&T, Inc.	Ms. Rosemary Leffler
BellSouth Corporation	Mr. David Barron
Cingular Wireless LLC	Mr. Jim Bugel
Microsoft Corporation	Mr. Paul Nicholas
Qwest Communications International, Inc.	Mr. Jon Lofstedt
Sprint Nextel Corporation	Ms. Allison Growney
Telecommunications Industry Association	Mr. Dan Bart
Telecommunications Industry Association	Mr. David Thompson
The George Washington University	Dr. Jack Oslund
Verizon Communications, Inc.	Ms. Ernie Gormsen
Verizon Communications, Inc.	Mr. Roger Higgins

GOVERNMENT PERSONNEL

Defense Information Systems Agency	Ms. Hillary Morgan
Department of Energy	Mr. John Greenhill
Department of Homeland Security/ National Cyber Security Division	Mr. Michael Lombard
Department of Homeland Security/ Infrastructure Partnerships Division	Ms. Christina Watson
Federal Reserve Board	Mr. Charles Madine
General Services Administration	Mr. John Migliaccio
General Services Administration	Mr. Thomas Sellers

President's National Security Telecommunications Advisory Committee

Department of Homeland Security/ National Communications System	Mr. Thomas Falvey
Department of Homeland Security/ National Communications System	Mr. Jeffrey Glick
Department of Homeland Security/ National Communications System	Mr. John O'Connor
Department of Homeland Security/ National Communications System	Mr. Don Smith
Department of Homeland Security/ National Communications System	CAPT Thomas Wetherald
Office of Management and Budget	Ms. Kim Johnson
Office of Science and Technology Policy	Ms. Linda Haller Sloan
Office of Science and Technology Policy	Mr. Mark LeBlanc

APPENDIX B
NCCTF INTERIM REPORT



**The President's National Security
Telecommunications Advisory Committee**

NCC 2010 Vision and Mission

**National Coordinating Center for
Telecommunications (NCC) Task Force (NCCTF)
Interim Report to the President's
National Security Telecommunications
Advisory Committee**

May 2005



NCCTF Interim Report

Introduction

- **As the Department of Homeland Security (DHS) continues to grow and evolve, the National Coordinating Center for Telecommunications (NCC) must reconsider its structure, organization, and approach to keep pace with rapid legal and regulatory changes**
- **In light of these changes, the President's National Security Telecommunications Advisory Committee Industry Executive Subcommittee requested that the task force convene to study the long-term direction of the NCC**



NCCTF Interim Report

Specific Tasking

The NCCTF was directed to determine where the NCC will be in one, three, and five years, including:

- The NCC's role in the Sector Coordinating Council (SCC) framework
- The process by which the industry members of the NCC should continue to partner with the Government
- The structure of the NCC

The task force will focus significant attention on issues involving information sharing, analysis, and protection across the communications industry and the communications infrastructure in general



NCCTF Interim Report

Other Issues Under Consideration

- The strain on business resources for member companies due to involvement in numerous industry groups as well as increasing demands for outage reporting
- The NCC's continued support of the communications requirements in the new National Response Plan (NRP) including cybersecurity requirements
- The NCC's response to, and participation in, the DHS National Incident Management System (NIMS)
- Policy and strategy, planning and training, and membership expansion



NCCTF Interim Report

Current Status

- Responding to DHS' interim National Infrastructure Protection Plan (NIPP), the NCCTF and SCC Working Group together have finalized an approach for organizing a Communications Infrastructure SCC (CI-SCC)
 - SCC will be separate from the NCC with a close NCC relationship
 - SCC will be policy-focused, and industry-only
 - Briefing to the membership in May – for approval
- Task force has focused primarily on one-year and three-year goals
- Task force will now shift focus to five-year goals
- Task force developed assumptions concerning future of NCC
- Task force finalized vision and mission statements



NCCTF Interim Report

Task Force Assumptions

- The NCC is a single entity with multiple functions
- Presidential Executive Order 12472, with its focus on national security and emergency preparedness (NS/EP), will continue to be the main driver of the NCC
- The CI-SCC will be implemented as a separate, industry-only, entity from the NCC that functionally supports an element of the overall NCC mission
- The NCC will continue its all-hazards approach to incident management
- Membership will expand to cover a wider range of the communications infrastructure sector
- The analysis function of the Information Sharing and Analysis Center (ISAC) must be enhanced
- The communications infrastructure and information technology sectors will work more closely together over the next several years



NCCTF Interim Report

NCC 2010 Vision Statement

The NCC will be a "... flexible, inclusive, and trusted partnership for all industry and Government organizations focused on preserving the operations of the Nation's communications infrastructure"



NCCTF Interim Report

NCC Mission Statement

The joint industry-Government NCC provides an all-hazards operations center and security enhancement framework with which to plan for, coordinate and respond to Communications Infrastructure Sector (CIS) events in support of the [National or overall?] NS/EP Mission (E.O. 12472); including NS/EP communications services, CIS information and analysis (i.e., CIS-ISAC), and critical infrastructure protection (CIP) functions

- **NS/EP Communications Services Function:** Assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency
- **CIS-ISAC Function:** Avert or mitigate impact upon the communications infrastructure on behalf of the private sector by collecting, analyzing, and sharing information on threats, vulnerabilities, intrusions, and anomalies from the communications industry, Government, and other sources
- **CIP Function:** Enhance physical and cyber security of the Nation's critical communications infrastructures by facilitating cooperation, information sharing, and system-to-system interaction among the critical infrastructures and between the Government and the private sector



NCCTF Interim Report

NCCTF Next Steps

- Review the authorities relevant to the NCC
- Develop a value statement for the NCC
- Consider how expansion of the NCC Industry membership could affect the NCC's structure
- Review structural options for the NCC
- Alignment around sector segments?
- Consider methods to expand Government participation from non-DHS entities
- Visualize the future threat environment and the NCC's Role
- Develop information-sharing requirements with Government



NCC Value Statement

NCC membership creates value for industry

- Direct access to shared information on threats, vulnerabilities, and restoration plans
- Increased communication with other key industry members involved in maintaining the communications infrastructure and with Government representatives involved in setting policy
- Opportunity to provide valuable service to the industry and key Government partners

NCC membership creates value for Government

- Direct contact with members of the communications infrastructure industry for purposes of damage assessment and restoration during NS/EP events
- Strong relationships with industry members allow for more effective CIP planning and policy decisions



NCCTF Long-Term Issues

- **Information Sharing:** How can the NCC receive threat information faster? What information does the NCC need to receive from the Government in order to improve the analysis function of the ISAC?
- **Structure:** Should the structure of the NCC be altered?
- **Looking ahead:** What will the industry look like in five years? What is the future threat environment?



NCCTF Next Steps

- **Next NCCTF meeting:** June 7, 9:00 a.m., Lucent Bell Labs
- **Finalize NCC value statement**
- **Expand on long-term plans and goals**
- **Review structural options for NCC**
- **Refine approaches for membership expansion**
- **Prepare document for DHS detailing the NCC's information-sharing requirements**

APPENDIX C

**NCC ROADMAP FOR THE FUTURE
RECOMMENDED ACTIONS LIST**

President's National Security Telecommunications Advisory Committee

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years
HSC	Join with industry in sponsoring regional coordination task force					
OSTP	Join with industry in sponsoring regional coordination task force					
	Develop and implement policies and procedures delineating authorities and responsibilities when ESF#2 is invoked					
	Develop a process for managing and escalating NCC requests to DHS leadership and the White House					
DHS	Develop and implement policies and procedures delineating authorities and responsibilities when ESF#2 is invoked					
	Acknowledge the FECC as the lead of ESF#2 in the region					
	Clarify NCC's alignment within the NIMS framework					
	Develop a process for managing and escalating NCC requests to DHS leadership and the White House					
	Plan for the regional coordinating capability to be within or a virtual capability of the JFO					
	Collocate JFO with EOC during crises whenever possible					
	Emphasize prioritization as its key mission					
	Expand the NCC to include IT					
	Begin planning for multi-industry coordinating center					
	Engage the private sector in CIP activities					
	Clarify policy on use of private sector information					

President's National Security Telecommunications Advisory Committee

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years	
	Increase flow of threat information through NCC	█	█	█	█	█	
	Put contracts into place to allow for industry participation in analyses	█	█	█			
	Improve ESF#2 Emergency Response Training and Exercises	█	█	█	█	█	
	Identify the NCC as the single point of focus for information dissemination during a crisis	█					
	Improve the Federal Government's cyber response strategy	█	█	█	█	█	
	Revise the NRP Cyber Incident Annex	█					
	Consider designating a member of the Office of General Counsel to respond to legal/jurisdictional issues that arise from cyber or communications crises	█					
	Provide the NCC with a NS/EP policy review update	█					
	Examine the value received from the NCC relationship			█		█	
	NCS	Clarify the process for membership as it pertains to NS/EP	█				
		Convene a conference to plan for improved focus on cyber	█				
Provide resources for the NCC to plan for and manage all incidents		█	█	█	█	█	
Enter agreements with comm. service providers to collaborate on impact analyses		█					
Involve industry experts at earlier stage of threat, vulnerability, and impact analyses		█					
Continue to participate in regional and international standards efforts		█	█	█	█	█	
NCC	Modify ESF#2 Annex and operations plan to account regional coordinating capability to be within or a virtual capability of the JFO	█					

President's National Security Telecommunications Advisory Committee

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years
	Create a common procedure and taxonomy	█				
	Institute a trouble ticket system	█				
	Disseminate situations reports to EOP Situation Room concurrently with transmissions to other Government stakeholders	█				
	Accept proposed mission statement	█				
	Establish a transition working group	█				
	Facilitate the ability of nontraditional comm. providers to respond to NS/EP incidents	█				
	Conduct outreach to enhanced membership	█	█	█	█	█
	Engage in dialogue with IT ISAC	█	█	█	█	
	Improve information sharing among members	█	█	█	█	█
	Include industry in planning and execution of exercises	█	█	█	█	█
NCC	Develop a CONOPS for how the NCC responds to cyber events	█				
	Continue to participate in regional and international standards efforts	█	█	█	█	█
	Assess impact of information sharing if the NCC membership is increased		█	█		
	Review short-term goals and directives to evaluate success of NCC in meeting requirements and needs		█	█		
	Examine the impact of direct, company-to-company mutual aid and coordination on the role of the NCC		█	█		
	Combine with IT ISAC			█		

President's National Security Telecommunications Advisory Committee

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years
	Combine NCC Watch and IT ISAC Watch			█		
	Develop a CONOPS for responding to incidents of national significance with participation of the IT Sector			█		
	Integrate with US-CERT			█		
	Engage with US-CERT and NCSD on international coordination			█	█	█
	Examine the value proposition of membership			█		█
	Expand relationships with operations centers for other sectors				█	█
	Establish agreements within the sectors on how to improve incident response and coordination				█	█
GSA	Include comm. service providers in planning and execution of emergency response training exercises	█	█	█	█	█
ESF#2 Federal Support Agencies	Participate in the development of policies and procedures on the delineation of ESF#2 roles and responsibilities and request escalation process	█				
	Support the development of and comply with the ESF#2 Federal Operations Plan	█				
C-SCC / IT-SCC	Sponsor regional coordination task force	█	█	█	█	█
	Focus regional coordination task force work on Gulf Coast Region	█				
	Determine long-term regional coordination capability		█	█	█	█
	Determine details for incorporating regional coordination capabilities		█	█	█	█
	Explore benefits of combining SCCs to preserve resources			█		

APPENDIX D

**MEMBER EXPECTATIONS OF THE NATIONAL COMMUNICATIONS
SYSTEM (NCS) AND THE NATIONAL COORDINATING CENTER (NCC)**

INTRODUCTION

Beginning with the emergence of the National Coordinating Center (NCC) on January 3, 1984, guided by earlier Presidential Memorandums in 1963 and Executive Orders in 1984, the major providers of communications services to the U.S. Government joined together to utilize the synergies and strengths of control inherent to a gathering of such undeniable experience and knowledge. With the pending breakup of the Bell System, the Government had quickly come to the realization that the protection and cooperation that they had previously enjoyed with one or two dominant carriers was soon to be challenged through the fragmentation of the nation's communication system and the expected proliferation of new service providers. The obvious solution was to establish an organization of corporate leaders who could coordinate, offer advice, and represent their respective companies to the Executive Office of the President and other Government agencies, notably the Department of Defense. It was generally accepted that this would be an unprecedented gathering of competing corporate managers asked to cooperate and to share information which many considered sensitive and proprietary; an equally unprecedented level of trust and sharing quickly developed among those initial members of industry and their new NCC Government partners. It is important to recall that at the time, the primary focus of the U.S. Government was on physical security, in large part due to the Cold War.

Many changes have taken place during the ensuing 21 years of NCC operations; including changes in technology, such as the transition to Next Generation Networks and the accompanying increase in cyber threats, and regulatory policies that have led to significant corporate restructuring. Of equal significance is the September 11th driven refocusing of the U.S. Government and the private sector to respond to asymmetrical domestic threats to the Nation, the establishment of the Department of Homeland Security, the transfer of the NCS, which includes the NCC, from the Department of Defense to the Department of Homeland Security, and the efforts to redefine the nature of the Government/industry partnership.

Today the NCC is comprised of over 30 corporations which represent a range of communications from service provider to equipment manufacturers, as well as seven Government department and agency members. The achievements and reputation of the industry/Government partnership have been actively acknowledged by nine Administrations and 11 U.S. Congresses and, although many of the corporate participants and several Government participants have changed, the basic mission statement of the NCS and the NCC remains the same, *"...Assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in: (1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery and reconstitution."*

To that basic mission, additional responsibilities have been accepted by the NCC constituent. For example, the incorporation of the NCS "all hazard" response planning and, the Department of Homeland Security's heightened attention to threaten domestic terrorism.

Each company and Government member has come to the table with total commitment on a pro-bono basis; and, with that total commitment come varying corporate expectations.

Each corporate member recognizes, as the owners and operators of over 90% of this nation's critical communications infrastructure that they have the ultimate responsibility of assuring the stability and dependability of the communication network nationally and internationally. For over 20 years, the communication sector has accepted this responsibility and has developed sources and data points which help to assure a proactive environment of security relative to risks and threats to those assets. Those risks and threats have stretched from natural events such as, weather, earthquake, and flood to those of the "Cold War Era" and to more recent changes in the social and political environment that have presented the sector with risks of terrorism throughout the domestic theater. Significant events such as the Hinsdale, Illinois, central office fire, the Oklahoma terrorist bombing, the terrorist crashing of an airplane into the Pentagon, and two separate World Trade Center terrorist bombings have tested the capabilities of this partnership. Each time it has proven to be up to the task.

The NCC partnership continues to reflect the original commitments of 1984, and while industry and Government members have similar historical expectations, several have identified new and additional expectations brought on by the need for heightened protection against the risks of terrorism.

A recent survey that was taken of the Government and industry members of the NCC is discussed in the main body of this report. While expectations varied from company-to-company and within the Government contingency, the overwhelming expectation was for increased flows of information from the public sector agencies. Following as a close second was the industry's desire to be acknowledged as the capable and principal steward of this nation's communication network and its desire to become a true partner of Government rather than simply a portal of sector information. The following antidotal responses to the survey reflect the wide range, but similar theme primarily of industry member expectations:

SURVEY RESULTS

- An industry member wants an increased flow of terrorist threat information from the intelligence community; feeling that this expectation constitutes a major justification for their company's commitment to provide resources to this organization. Without that reciprocity in information sharing, the value of participation in the NCC is diminished.
- Another has a clear expectation for the Public Sector Intelligence Agencies to identify specific threats and for The Department of Homeland Security to allow the industry to identify vulnerabilities based on those specific threats. Each entity, neither qualified to assume the other's role, should allow each to perform the function for which it is best suited.
- In addition to a desire for an increased flow of terrorist threat information, industry members would like to see better communication regarding Government-owned assets or activities that may potentially jeopardize industry assets (and vice versa). For example, "U.S. Objects" operating in close proximity to commercial satellites. It would be in the best interests of both the Government and commercial satellite operators to provide for a greater degree of situational awareness than exists today to help protect both our and the Government's critical infrastructure in space.

- A Government member expressed expectations of more industry developed capabilities to assist Government in developing a cohesive network of industry capabilities to assist the public sector communications controllers relative to impending concerns. This may be likened to establishing a more cross sector-like relationship with the interdependent public sector.
- Another Government partner has expectations of the NCC assisting its sector with information in which they could better utilize resources in future network and services development. The efforts of the National Security Telecommunications Advisory Committee (NSTAC) and the Next Generation Networks (NGN) task forces were cited as an effective role for the NCC and it was noted that future efforts in other technologies would be helpful. This partner also looked for informative technology evolution within the membership of the NCC.
- Corporate members expect the NCC to continue supporting the civil communications community relative to national environmental impacts to the communication sector in response to events such as hurricanes, floods, fires, and earth quakes. While the NCC initial role would be acknowledged as national security and emergency preparedness (NS/EP), by sustaining the national network, NS/EP services that are linked to civil communications are also maintained and recovered.
- It was generally expected by all of the participants, that the NCC mission would remain focused on NS/EP, while noting that the original definition of the NS/EP was evolving and in the future might envelop public sector original terms such as Critical infrastructure (CI) and critical infrastructure protection (CIP). They offered in support of this view, the recent discussions which have linked CI with those infrastructures which support national security (NS) services and CIP as the emergency preparedness (EP) components of the terms NS/EP. If this were to be generally accepted, the differentiation of CIP and NS/EP might prove to be artificial and incorrectly approached as separate areas of concern.
- Several members expressed expectations that the NCC would actively evolve to fully represent the emerging technologies such as the Wi-Fi community, the national cable services, and both wireline and wireless advancements. They are expecting a wider and deeper representation of the communication sector.

CONCLUSIONS

Satisfied expectations are a measure of successful endeavors and realized goals. Unmet expectations generally lead to disappointment, dissatisfaction, and often to disengagement. Twenty years of cooperative success reflect the achievement of expectations for both the Government and industry parties of the NCC. Over that period of time, one must acknowledge that expectations for each entity have passed through many changes. Review and adjustments in relationships, processes, and policies have each contributed to that continued success. Now it is again, a time for reconsideration.

Industry is seeking a re-establishment of “full partnership” with the Government sector. Structural changes within the federal sector seem to have distracted the nurturing of the historical pairing of industry and Government. The industry sector expects the Department of Homeland

President's National Security Telecommunications Advisory Committee

Security to acknowledge the excellent planning and protection that the private sector has afforded the nation's communication system in the past. Government, in turn, is seeking industry assistance to allow it to exercise greater oversight of the critical infrastructure and to arrange for Government protection for those assets against terrorist threats, if required. Industry expects a flow of threat information to come from the Government sector and that the resulting vulnerabilities to be identified by the private sector, with each sector performing in its areas of expertise.

APPENDIX E

**NCS DIRECTIVE 3-4:
NATIONAL TELECOMMUNICATIONS MANAGEMENT STRUCTURE**

President's National Security Telecommunications Advisory Committee



COMMAND, CONTROL,
COMMUNICATIONS AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, DC 20301-3040


313A
OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
13
DDA
08 AUG 1992
NA

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF DEFENSE FOR SECURITY POLICY
DIRECTOR, INFORMATION SYSTEMS FOR COMMAND, CONTROL,
COMMUNICATIONS AND COMPUTERS, U.S. ARMY
DIRECTOR, SPACE AND ELECTRONIC WARFARE, U.S. NAVY
DEPUTY CHIEF OF STAFF, COMMAND, CONTROL,
COMMUNICATIONS AND COMPUTERS, U.S. AIR FORCE
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND
COMPUTERS, U.S. MARINE CORPS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND
COMPUTERS, JOINT STAFF
DIRECTORS, DEFENSE AGENCIES

SUBJECT: Implementation of National Communications System
Directive 3-4

National Communications System Directive (NCS D) 3-4, National Telecommunications Management Structure (NTMS), dated May 4, 1992, (attached) has been issued under the authority of Executive Order 12472 by the Executive Office of the President. NCS D 3-4 establishes the NTMS, describes its components, and broadly describes the administrative responsibilities of the Manager, National Communications System (NCS) and participating NCS member agencies.

Defense components are required to support the NTMS pursuant to paragraph 7.a. of NCS D 3-4. For additional information on the implementation of NCS D 3-4, or to identify operating/command centers to support the NTMS, contact the NCS NTMS Program Office, telephone DSN 222-8506.


John G. Grimes
Deputy Assistant Secretary
Of Defense (Defense-Wide C3)

Attachment

CC:
Manager, NCS

May 4, 1988

NCS 1-4

NATIONAL COMMUNICATIONS SYSTEM
Washington, D.C. 20305-2010

NCS DIRECTIVE 1-4

TELECOMMUNICATIONS OPERATIONS

National Telecommunications Management Structure (NTMS)

1. **Purpose.** This directive establishes the National Telecommunications Management Structure (NTMS), describes its components, and broadly describes the administrative responsibilities of the Manager, NCS and participating NCS member organizations.
2. **Applicability.** This directive is binding on the Executive Agent, NCS; NCS Committee of Principals and member organizations; and other affected Executive entities. This directive is not intended to interfere with the special operational or security requirements of any agency during normal or wartime situations.
3. **Authority.** This directive is issued under the authority of Executive Order No. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984, 49 Federal Register 13471 (1984); White House Letter, National Security Telecommunications Advisory Committee (NSTAC) Activities, July 11, 1988; and NCS Directive 1-1, "National Communications System (NCS) Issuance System," November 30, 1987.
4. **References.**
 - a. The Communications Act of 1934, as amended, Section 706 (47 U.S.C. 151 et seq.).
 - b. National Emergencies Act of 1976 (50 U.S.C. 1601 et seq.).
 - c. Executive Order 12472 of April 3, 1984, "Assignment of National Security and Emergency Preparedness Telecommunications Functions."

-Office of Primary Responsibility: NCS-PP
-Distribution: NCS

May 4, 1992

NCSO 3-4

5. Definitions.

a. National Telecommunications Management Structure (NTMS). The NTMS is an emergency telecommunications management structure consisting of national and regional management elements and government and telecommunications industry operating centers that, when activated, shall provide emergency telecommunications management services in response to national security and emergency preparedness (NS/EP) requirements and objectives in accordance with references a. and b.

b. National Telecommunications Coordinating Network (NTCN). The NTCN provides the essential communications connectivity to support NTMS elements.

c. Emergency Preparedness Management Information System (EPMIS). The EPMIS is the telecommunications management information system designed to support NTMS operations at national and regional levels.

d. National Coordinating Center (NCC). The NCC is a jointly staffed and operated government and telecommunications industry center. The NCC assists in the initiation, coordination, restoration and reconstitution of the Federal Government's NS/EP telecommunications service requirements.

e. National Emergency Management Team (NEMT). The NEMT is a functionally organized, national level emergency management team composed of representatives from the Executive Branch of the Federal Government and selected industries.

f. National Emergency Management Team Communications Functional Group (NEMT CFG). The NEMT CFG is one of the functional groups of the NEMT, and is composed of Office of Science and Technology Policy (OSTP), Office of the Manager, NCS (OMNCS), NCS member organization and telecommunications industry representatives. The NEMT CFG is to be activated by national authorities in response to those crises and national emergency situations in which the President may invoke the provisions of Section 706 of the Communications Act of 1934, as amended. When so activated, the NEMT CFG will provide policy, direction and guidance for NS/EP telecommunications management, and serves as the highest level of the NTMS.

g. Regional Emergency Management Team Communications Functional Group/Regional Coordinating Center (REMT CFG/RCC). The REMT is the functionally organized regional equivalent of the

May 4, 1992

NCSD 3-4

NEMT. The NEMT CFG/RCC is the NEMT functional group composed of regionally based Federal field establishment and telecommunications industry representatives. It is the NTMS organizational element tasked to provide direction and guidance for NS/EP telecommunications management in the Region. The NEMT CFG/RCC is also capable of serving as an alternate NCC.

h. NTMS Government and Industry Operating Centers (OCs). Government and telecommunications industry facilities constitute the basic operating and coordinating organization for the nation's telecommunications management infrastructure. The NTMS OCs are selected to coordinate technical telecommunications activities at the local level in response to guidance and direction from the NEMT CFG/RCC to which assigned.

(1) Industry OCs manage and coordinate the restoration and reconstitution of the telecommunications services provided.

(2) Government OCs coordinate communications support, and manage/operate communication facilities.

6. Policy. It is the policy of the United States to develop and implement a survivable and enduring telecommunications management structure to support national security and emergency preparedness requirements for use after the invocation of Section 706 of the Communications Act of 1934, as amended. The overall governing objective of the NTMS, as established herein, is to provide for a survivable and enduring functionally organized telecommunications management structure capable of coordinating the recovery and reconstitution of the nation's telecommunications infrastructure to meet essential NS/EP needs.

a. NTMS Components. The NTMS shall be composed of the NCC, the NEMT CFG, NEMT CFG/RCCs and NTMS OCs.

b. Activation, Direction and Control. The NTMS shall be activated by and respond to the guidance and direction of the Director, OSTP, in the execution of the functions of the President under Section 706 (a), (c)-(e), of the Communications Act of 1934, as amended, should the President issue implementing instructions in accordance with the National Emergency Act (50 U.S.C. 1601).

c. Coordinating Instructions.

(1) In all instances prior to the invocation of Section 706 of the Communications Act of 1934, as amended, the NCC shall monitor the status of the nation's telecommunication resources and respond to NS/EP requirements as directed by the

]

May 4, 1998

WCSD 3-4

Director, OSTP, and the Manager, NCS, or their designated representatives.

(2) Upon invocation of Section 706, the Director, OSTP, shall assume direction and control of national telecommunication resources and determine priorities for their allocation and use. The NTMS shall assist the Director, OSTP, in the exercise of his emergency authority relative to policy direction and management of national telecommunications resources.

7. Responsibilities.

a. NCS Member Organizations Participating in NTMS:

(1) Will support the implementation and operation of the NTMS, as mutually agreed to by the participating NTMS organizations and the OMCNS.

(2) Will assist the OMCNS with government NTMS Operating Center nominations.

(3) Will for those Operating Centers selected, assist in preparations to include necessary modifications for equipment installation, logistics support, equipment and life support supplies storage, and personnel selection and training.

(4) Will assist the OMCNS with the planning and conduct of NTMS tests, exercises and evaluations when requested and as scheduled by the NCS exercise master plan.

b. The NCS Committee of Principals and Executive Agent:

(1) Will consider and approve other NTMS issuances.

(2) Will review and provide comments regarding NTMS operating concepts, plans and policies to the Executive Office of the President.

c. The Manager, NCS:

(1) Will provide overall NTMS program management.

(2) Will ensure the funding for the NTMS.

(3) Will develop NTMS policies, plans and procedures as the designated focal point for NEMT CPG and REMT CPG/RCC operational matters in coordination with OSTP.

May 4, 1992

NCSO 3-4

(4) Will coordinate NTMS operational issues and requirements with OSTP, NCS member organizations and telecommunications industry entities participating in the NTMS.

(5) Will coordinate NTMS program activities, as appropriate, with the Executive Office of the President; Executive Agent, NCS; NCS Committee of Principals; NCS member organizations and the telecommunications industry.

(6) Will provide for planning, implementation and management of the NTMS program.

(7) May propose subjects for and develop new NTMS issuances, and propose changes in existing issuances.

(8) Will forward NCS NTMS issuances and any comments thereon to the NCS Committee of Principals; Executive Agent, NCS; and/or Executive Office of the President, as required.

(9) Will implement test and exercise programs and develop procedures for the evaluation of the NTMS capability to meet national security and emergency preparedness telecommunications requirements.

d. Federal Emergency Management Agency:

(1) Will assist the OMMCS with NTMS implementation and planning in support of the NEMT and RENT CFG/RCCs.

(2) Will assist the OMMCS with NTMS activities and exercises when the NEMT and RENT CFG/RCCs are to be employed.

(3) Will assist the OMMCS and the telecommunications industry in establishing procedures for connectivity with FEMA FRCs.

e. General Services Administration:

(1) Will provide assistance to the OMMCS with NTMS implementation and planning in support of the NEMT and RENT CFG/RCCs.

(2) Will provide the RENT CFG/RCC Leader and assist in staffing the NEMT and RENT CFG/RCCs.

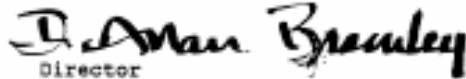
(3) Will provide assistance to the OMMCS with RENT CFG/RCC planning, staff selection, training, exercises and other activities.

President's National Security Telecommunications Advisory Committee


May 4, 1992

NCS 1-4

8. Authorizing Provisions. NCS circulars, manuals, handbooks, and notices implementing this directive are hereby authorized.
9. Effective Date. This directive is effective immediately.
10. Expiration. This directive will remain in effect until superseded or cancelled.



Director
Office of Science and Technology Policy
Date: May 4, 1992


Assistant to the President for
National Security Affairs
Date: May 4, 1992

Summary of Changes: Initial Issuance.

APPENDIX F
IT ISAC CONOPS

IT ISAC MISSION/VISION

INTRODUCTION:

This document sets out an operational mission statement, defining the roles and relationships for the IT ISAC within the information technology sector, within the larger infrastructure community, and between the sector and relevant agencies of Government and other institutions.

HISTORICAL NOTE:

Since their inception in 1998 following the promulgation of PDD-63, the industry organizations known as information sharing and analysis centers or "ISACs" have had an uneven course in establishing acceptance and legitimacy for their potential and promise as sources and agents of accurate, unique actionable data regarding the condition of critical infrastructures essential to America's national and economic security.

Eleven "keystone" sectors identified in the report of the President's Commission on Critical Infrastructures in 1998 were described as essential to economic activity and security; of these, the Information Technology sector was singled out as having an evolving "first among equals" role, potentially surpassing even electric power as an infrastructure upon which every other will come to depend in order to operate.

In the wake of the September 11 tragedies, both the National Government and the sectors which had established or explored creation of sectoral information sharing organizations have sought to mature the operational model, legal framework and authority and governmental mechanism for generating, sharing and operationalizing private sector data regarding condition, threats and attacks against these key infrastructures.

In the ICT sector, the process of infrastructure organization evolution has been marked by the early aggressive development of the I/T ISAC.²⁹ But the process of achieving legitimacy for ISACs both within their sectors and with Government agencies has been uneven. The umbrella PCIS has evolved and spawned a cross-ISAC council, which has since 2003 engaged with the Department of Homeland Security. Legislation to provide a Congressional imprimatur on the ISAC concept and provide clarity for the relationships between ISACs and other industry information sharing organizations and Government agencies was introduced in Congress in 2000 and became Title II of the Homeland Security Act in 2003.³⁰ In ICT specifically, the establishment of a clear role for the ISAC has been complicated by several factors, including the pre-existing posture of a telecommunications information sharing organization with a long history and deep relation to Government bodies—the National Communications System, operating until 2002 under the auspices of the Defense Information Systems agency at DOD , and, since the inception of the Department of Homeland Security within that bodies IA/IP

²⁹ *Incorporation of IT ISAC.*

³⁰ *HAS, Title II, and bill nos. of House and Senate original information sharing acts.*

Directorate, and also by the existence of a parallel industry organization with a self declared role in Internet information sharing, the Internet Security Alliance.³¹

SUMMARY OF THE IT ISAC's MISSIONS:

The Board of Directors of the IT ISAC, operating both under guidance from the membership and in consultation with other sectors has defined two broad areas of operation.

First and foremost, the IT ISAC exists to provide time, actionable data regarding conditions, attacks, threats, remedies and other observed facts regarding the information technology infrastructures owned, operated or entrusted to the stewardship of its members.

Second, in consultation with its sector members, other infrastructure organizations, agencies of Government and other institutions, the IT ISAC will define and recommend policies, practices, investments and other measures appropriate to the secure, stable, reliable and available operation of the IT infrastructure.

OPERATIONAL MISSION:

As set out in its organizational documents, the primary purpose of the IT ISAC is to “report and exchange information” regarding “...incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures...” which its members acquire in the course of their operation of these industrial assets. As primary sources of this information, the ISAC's members view themselves as authoritative sources for this data.

Under the structures established by the Homeland Security Act³², HSPD 7³³ and HSPD 12³⁴, the Information Analysis/Infrastructure Protection directorate of the Department of Homeland Security is the primary recipient of IT ISAC-developed data. Regulations established pursuant to Title II of the HSA, creating the Protected Critical Infrastructure Information (PCII) program³⁵, further define the organization, labeling, transmission and scope of use of information transmitted by ISACs to DHS.

As of this writing, a primary consideration in the continuing viability of ISACs as institutions and the utility of their primary information submission role is the Department's still-evolving program for reception, analysis and utilization of industry developed data.

Ancillary to its primary operational mission are a unique set of tasks for which the IT ISAC possesses singular capabilities. Examples include:

1. **Exercises:** Among the ongoing obligations of the DHS is the conduct of exercises to simulate attacks against the infrastructure and the responses from industry and Government institutions. IT ISAC has and will continue to offer its members' expertise

³¹ ISA website.

³² HSA sector table.

³³ HSPD-7.

³⁴ HSPD-12.

³⁵ PCII Interim Regulations.

to the development of such exercises and on request will participate in, observe, analyze, or otherwise support simulations and exercise.

2. **Information sharing conduit:** Notable among the many concerns shared by all ISACs is the continuing issue of the appropriate mode and structure of data sharing between ISACs (and other industry organizations) and DHS (and other primary Government data recipients); in particular, the creation of a confidential secure channel for transmission of critical infrastructure information stands as the most important shared objective. In response to this concern, an important new operational task undertaken by the IT ISAC is the leadership of an industry-wide process, relying on the IT sector's unique expertise, to evolve the structure and technology for such a secure channel for information sharing.

POLICY MISSION:

In addition to ancillary operational tasks such as participation in exercises and the development of a secure channel, the IT ISAC will undertake tasks in the policy arena that support its primary information sharing mission. This includes participation in policy-making proceedings that influence the statutory, regulatory or general policy environments within which critical infrastructure information sharing occurs.

Through its Policy Committee, the IT ISAC has and will continue to comment on regulatory proposals from the DHS and other agencies.³⁶ The ISAC may, from time to time comment directly, through its members, in combination with other ISACs or other organizations or surrogates on legislation, regulations and policies. It will participate in the inter-ISAC Council.

As of Q4 2004, the IT ISAC Policy Committee is engaged in the following activities:

- Engagement, along with other ISACs in discussions with DHS IA/IP regarding the representation of critical sectors to the Department, including the relation of ISACs to "sector coordinating committees."
- Participation in ISAC Council processes on private sector-wide policy development, on issues including:
 - secure, authenticated channels for information sharing
 - participation of private sectors in Government sponsored simulations and exercise
- Continuing refinement of DHS regulations and policies on PCII sharing
- Dialogue with DHS IA/IP on the role of the IT sector in the development of TOPOFF III, a proposed National Cyber Security exercise and other simulations
- Development of private sector led cross-sector exercises and simulations

³⁶ *IT ISAC comment on draft PCII regulations.*