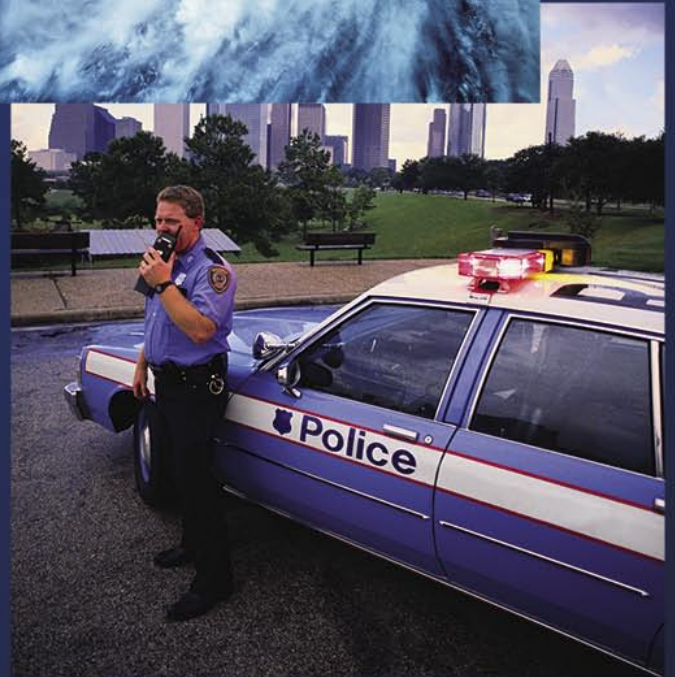
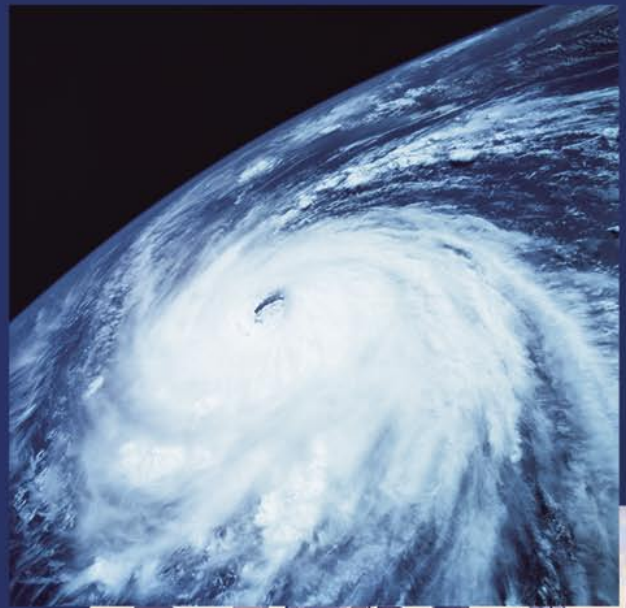




NSTAC XXIX Reports



“NSTAC: Enhancing National Security and
Emergency Preparedness through Communications”

The President's
National Security Telecommunications
Advisory Committee



NSTAC XXIX
Reports

August 2006

Table of Contents

NSTAC XXIX Reports

NSTAC Report to the President on the Emergency Wireless Protocol

January 31, 2006

NSTAC Letter and Report to the President on Legislative and Regulatory Issues

Federal Support to Telecommunications Infrastructure Providers in National Emergencies Designation as “Emergency Responders (Private Sector),” January 31, 2006

NSTAC Report to the President on Telecommunications and Electric Power Interdependencies

People and Processes: Current State of Telecommunications and Electric Power Interdependencies, January 31, 2006

NSTAC Report to the President on Next Generation Networks

March 28, 2006

NSTAC Report to the President on Next Generation Networks

Appendices, March 28, 2006

NSTAC Report to the President on the National Coordinating Center

May 10, 2006

NSTAC XXIX Correspondence to the President

NSTAC Letter to the President on Emergency Communications and Interoperability

April 12, 2006

NSTAC Letter to the President on the National Coordinating Center

April 12, 2006

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE



**NSTAC Report to the President on the
Emergency Wireless Protocol**

January 31, 2006

For information on this report, please contact the

National Communications System

nstac1@dhs.gov



NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

March 1, 2006

The President
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

Your National Security Telecommunications Advisory Committee (NSTAC) continues to evaluate the lessons learned from Hurricane Katrina. We are writing to bring to your attention the first of several NSTAC recommendations that would strengthen the ability of telecommunications providers to respond even more effectively to future hurricanes and other natural or manmade events.

National security and emergency preparedness (NS/EP) communications are those telecommunication services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that 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. The provision of NS/EP communications to support the incident management structure defined in the National Response Plan (NRP) requires that the supporting communications infrastructure is quickly returned to working order after an incident. However, the restoration of service necessary to deliver NS/EP services is contingent upon the ability of telecommunications infrastructure providers to quickly access and repair damaged facilities.

Unfortunately, initial legal and policy interpretations in the aftermath of Katrina significantly delayed the restoration of the basic communications infrastructure. Specifically, the major policy challenges resulted from (1) the lack of recognition of telecommunications infrastructure providers as emergency response providers in the *Homeland Security Act of 2002* and the NRP, and (2) inconsistent interpretations of the *Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)*. Strict interpretations of the law and these policy documents determined that telecommunications infrastructure providers were not emergency responders and were not entitled to assistance under the Stafford Act, which precluded key providers from receiving Government assistance in accessing restricted areas and obtaining fuel, water, power, billeting, and workforce and asset security.

To ensure the expeditious restoration of critical telecommunications infrastructure after a natural disaster or terrorist attack, your NSTAC recommends that you take action to designate telecommunications infrastructure providers as "Emergency Responders (Private Sector)." The National Weather Service forecasts that the 2006 hurricane season, beginning on June 1, 2006, will be as destructive as the 2005 season. Implementing these recommendations before the hurricane season or a potential terrorist attack will enable Federal agencies to render non-monetary assistance to telecommunications infrastructure providers to facilitate recovery of the very communications central to incident management efforts.

Accordingly, the NSTAC recommends that, no later than June 1, 2006, you establish and codify the term Emergency Responder (Private Sector) to include telecommunications infrastructure providers and ensure non-monetary assistance, including accessing restricted areas and obtaining fuel, water, power, billeting, and workforce and asset security, to them by—

- Directing the Department of Homeland Security to modify the NRP and its Emergency Support Functions to designate telecommunications infrastructure providers as Emergency Responders (Private Sector) and to establish protocols and procedures for the way in which Federal, State, local, and tribal Governments should work with telecommunications infrastructure providers before, during, and after a national disaster,
- Issuing appropriate Presidential guidance to define Emergency Responders (Private Sector) under the Stafford Act and other authorities as appropriate to align with the broadened definition of national defense in the 2003 amendments to the *Defense Production Act (DPA) of 1950*. Specifically, the guidance should make clear that key response personnel of critical telecommunications infrastructure owners and operators should be defined as Emergency Responders (Private Sector) and should receive non-monetary Federal assistance under the Stafford Act, and
- Directing the Secretary of Homeland Security to work with Congress to align the Stafford Act and other appropriate legislative authorities with the DPA by codifying the designation of private sector telecommunications infrastructure providers as Emergency Responders (Private Sector) and by codifying the official interpretation that for-profit telecommunications infrastructure providers should receive non-monetary Federal assistance.

The adoption of these recommendations will help expedite the recovery and restoration of essential NS/EP communications after a natural disaster or terrorist attack. The attached report sets forth the findings and conclusions of our evaluation. Thank you for the opportunity to advise you on this vital matter and the NSTAC would be pleased to work with you to carry out these recommendations.

Sincerely,



F. Duane Ackerman
Chairman

Copy to:

The Vice President
Secretary of State
Secretary of Defense
The Attorney General
Secretary of Transportation
Secretary of Energy
Secretary of Homeland Security
Director, Office of Management and Budget
Assistant to the President for National Security Affairs
Assistant to the President for Homeland Security
Assistant to the President for Science and Technology
Chairman, Federal Communications Commission
Under Secretary for Preparedness, Department of Homeland Security
Assistant Secretary for Infrastructure Protection, Department of Homeland Security/Manager, National Communications System
Director, Federal Emergency Management Agency, Department of Homeland Security
Director, Office of Legislative and Intergovernmental Affairs
NSTAC Principals and Industry Executive Subcommittee Members

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE



**NSTAC Report to the President on
Legislative and Regulatory Issues**

***Federal Support to Telecommunications Infrastructure
Providers in National Emergencies***

Designation as "Emergency Responders (Private Sector)"

January 31, 2006

Table of Contents

1	Introduction	1
2	Background	1
3	Examination	4
	3.1 Security for Private Facilities	4
	3.2 Priority Access to Critical Resources	5
	3.3 Priority Site Access Authorization	5
	3.4 Legal and Regulatory Issues	6
	3.4.1 The Stafford Act	6
	3.4.2 The Defense Production Act	7
	3.4.3 The National Response Plan	7
4	Findings	8
	4.1 The Stafford Act and Legal Interpretation of Federal Assistance	8
	4.2 The Stafford Act and TIPs as Emergency Responders (PS)	8
	4.3 The NRP and TIPs as Emergency Responders (PS)	9
5	Conclusion	9
6	Recommendations	11
Appendices		
A	Task Force Members, Other Participants, and Government Personnel	A-1

1 Introduction

The President's National Security Telecommunications Advisory Committee (NSTAC), in recognition of the importance of protecting and restoring vital services following natural or man-made disasters, is charged with providing the President "advice in the identification and solution of problems which the Committee considers will affect national security telecommunications capability."¹ On August 29, 2005, Hurricane Katrina made landfall near New Orleans, Louisiana, as a Category 4 hurricane and battered the Gulf Coast region of the United States. Most notably, the storm surge breached the levees that protected New Orleans from Lake Pontchartrain, and most of the city was subsequently flooded by the lake's waters. In addition, the Mississippi Gulf Coast was devastated. The storm and ensuing flooding resulted in severe damage to the wireline and wireless communications infrastructure throughout the area. Electric power no longer functioned, switches were damaged by flooding, and critical personnel could not gain access to many sites. Because of the storm's unprecedented destruction to the infrastructure, recovery and restoration teams were faced with numerous challenges. Civil unrest that arose in the wake of the disaster seriously impeded recovery and restoration efforts. The NSTAC examined the response to Hurricane Katrina and the implications of that response for vital national security and emergency preparedness (NS/EP) communications.

The Federal Government recognizes the significance of the telecommunications infrastructure in providing essential communications during and after a natural disaster or terrorist attack. The President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003, affirms that "the Government and critical infrastructure industries rely heavily on the public telecommunications infrastructure for vital communications services." Communication is at the foundation of the Nation's ability to respond to a catastrophic event because the stability of the telecommunications infrastructure helps to ensure the protection and restoration of other infrastructures.

The NSTAC realizes that because the private sector owns the vast majority of the critical telecommunications infrastructure, industry and the Federal Government must work together to protect and restore this infrastructure during and after a catastrophic event. Consistent with its charge, the NSTAC investigated whether the current legal and regulatory framework hindered the coordination of the restoration of critical telecommunications infrastructure efforts between the Federal Government and telecommunications infrastructure providers² (TIP) in the aftermath of Hurricane Katrina.

2 Background

Since its inception, the NSTAC has addressed a wide range of policy issues regarding the importance of protecting and restoring the Nation's telecommunications infrastructure to maintain vital NS/EP functions in the event of a national disaster. Hurricane Katrina caused unprecedented damage to the national telecommunications infrastructure and TIPs had to quickly respond and restore the infrastructure to expedite emergency response to the devastated areas. However, in their response and restoration efforts, many TIPs had difficulty accessing vital resources needed to repair essential infrastructure and could have shortened their response times with non-monetary assistance from the Federal Government. This difficulty was attributed in large part to differing interpretations of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) [Public Law 93-288, as amended], which were intensified by the National Response Plan's (NRP) unclear description of the Federal Government's role in providing support to TIPs during disaster relief efforts.

The Stafford Act is the legislative vehicle through which the Federal Government provides disaster relief to State, local, and tribal Governments; individuals; families; and some private nonprofit organizations through the federally administered Disaster Relief Fund. The Act grants the President authority to declare an area a natural disaster, thereby expediting Federal assistance through the Federal Emergency Management Agency (FEMA) to States during catastrophes such as

Hurricane Katrina.³ With the recent transfer of FEMA to the Department of Homeland Security (DHS), existing ambiguities in the Stafford Act became subject to new analysis by DHS lawyers.

Several sections of the Stafford Act indicate that the Act does not preclude Federal assistance to TIPs. Section 5170(b)(3), for instance, allows Federal departments and agencies to “provide assistance essential to meeting immediate threats to life and property resulting from a major disaster” including, “Performing on public or private lands or waters any work or services essential to saving lives and protecting and preserving property or public health and safety.” Additionally, 5170(b)(4) allows Federal agencies to make “contributions to State or local Governments or owners or operators of private non-profit facilities for the purpose of carrying out the provisions of this subsection,” and Section 5172 allows the President to make contributions to private nonprofit facilities if “the facility provides critical services (as defined by the President) in the event of a major disaster.” As a result of new interpretations regarding the applicability of the Stafford Act to for-profit entities, restoration efforts were stalled. The Federal Government’s ability to provide assistance to TIPs was hindered, preventing the private sector from reacting to Katrina with the same efficiency with which it had responded in previous disasters.

Once an incident has been declared a national disaster, support extended under the Stafford Act is coordinated through the protocols established in the NRP, which was developed pursuant to the Homeland Security Act of 2002 (HSA) [Public Law 107-296]. As mandated under Homeland Security Presidential Directive 5, Management of Domestic Incidents, the NRP does not have force of law; rather, its guidelines are intended to provide a firm national framework for streamlining incident management activities by improving disaster management coordination among Federal, State, and local jurisdictions and private sector entities. To facilitate this coordination, the Government incorporated mechanisms, known as emergency support functions (ESF), describing the type of Federal support available and delineating the roles of the ESF Coordinator and support agencies in administering aid to the public and private sector. Table 2-1⁴ lists the 15 ESFs.

Several sections of the plan allude to the importance of partnering with and providing resources to TIPs to ensure NS/EP communications during response and recovery efforts. For example, ESF-2 gives specific guidance regarding industry and Government coordination by instructing Federal officials to “[work] with the telecommunications industry” to “restore and reconstruct telecommunications facilities as the situation permits.”⁵ Recognizing that restoration of damaged critical telecommunications infrastructure requires resources, the NRP calls on the National Communications System Manager to “[coordinate] with ESF-12 regarding telecommunications industry requests for support under the Electric Service Priority initiative, emergency fuel resupply, and safe access for telecommunications work crews into disaster areas.”⁶ ESF-13 helps provide public safety resources when State and local Governments are overwhelmed. Instances in which Federal security support is appropriate are as follows:

- ▶ “Badging and Credentialing: Assisting in the establishment of a consistent process for issuing identification badges to emergency responders and other personnel needing access to places within a controlled area;”
- ▶ “Site Security: Providing security forces and establishing protective measures around the incident site, critical infrastructure, and/or critical facilities;” and
- ▶ “Force Protection: Providing for the protection of emergency responders and other workers operating in a high-threat environment.”⁷

ESF-7 complements the support provided in ESF-13 by offering resources to Federal, State, local, and tribal jurisdictions in the form of “relief supplies, facilities space, office supplies, office space, telecommunications, security services, and personnel required to support immediate response activities.”⁸ References to coordination with the private sector in the ESFs are bolstered in the Private-Sector Coordination Support Annex to the NRP, which reiterates DHS’s responsibility to “facilitate coordinated incident response planning

ESF	Description	Lead Agency
1. Transportation	Providing civilian and military transportation	Department of Transportation
2. Communications	Providing telecommunications support	National Communications System
3. Public Works and Engineering	Restoring essential public services and facilities	U.S. Army Corps of Engineers, Department of Defense
4. Fire Fighting	Detecting and suppressing wildland, rural and urban fires	U.S. Forest Service, Department of Agriculture (USDA)
5. Information and Planning	Collecting, analyzing, and disseminating critical information to facilitate the overall Federal response and recovery operations	FEMA
6. Mass Care	Managing and coordinating food, shelter and first aid for victims; providing bulk distribution of relief supplies; operating a system to assist family reunification	American Red Cross
7. Resource Support	Providing equipment, materials, supplies, and personnel to Federal entities during response operations	General Services Administration
8. Health and Medical Services	Providing assistance for public health and medical care needs	U.S. Public Health Service, Department of Health and Human Services (HHS)
9. Urban Search and Rescue protocols and procedures	Locating, extricating, and providing initial medical treatment to victims trapped in collapsed structures	FEMA
10. Hazardous Materials	Supporting Federal response to actual or potential releases of oil and hazardous materials	Environmental Protection Agency
11. Food	Identifying food needs; ensuring that food gets to areas affected by disaster	Food and Nutrition Service, Department of Agriculture
12. Energy	Restoring power systems and fuel supplies	Department of Energy
13. Public Safety and Security	Securing facilities and resources	DHS and Department of Justice
14. Long-Term Community Recovery and Mitigation	Assessing social and economic community impact	USDA, Department of Commerce, HHS, DHS/Emergency Preparedness and Response (EPR)/FEMA, Department of Housing and Urban Development, Department of the Treasury, and Small Business Administration
15. External Affairs	Establishing emergency public information and protective active guidance	DHS/EPR/FEMA

Table 2-1 Emergency Support Functions in the NRP

with the private sector at the strategic, operational, and tactical levels.”⁹

The NRP also designates “emergency response providers” and “emergency responders” who are eligible for specific support described in the ESFs, such as the credentialing and force protection measures mentioned above. Specifically, it identifies emergency response providers using the statutory definition from the HSA, which focuses on Government entities.¹⁰ However, the plan does not completely overlook the importance of the private sector in emergency response. In Appendix 3, the NRP makes one reference to “private sector emergency response providers”¹¹ separately from the “emergency response providers” described in the HSA. Although the plan seems to allow for a private sector emergency response provider designation, it neither elaborates on this concept nor lists specific entities who qualify as such. Furthermore, it also does not clarify whether any support will be available to private sector emergency response providers or whether any such support provided would be commensurate with that granted to other emergency response providers.

3 Examination

Immediately following the storm, industry and Government response and infrastructure restoration efforts were addressed through the National Coordinating Center (NCC), which, under the NRP, is designated as the Federal office for national telecommunications domestic incident management. However, as a result of the unprecedented destruction to the infrastructure, the NCC and other recovery and restoration teams in the private sector faced numerous new and unforeseen operational challenges. To analyze these challenges, the NSTAC examined the way in which TIPs responded to Hurricane Katrina’s damage, the difficulties they faced during their restoration efforts, and the legal and regulatory environment in which industry and the Federal Government conducted emergency response. The Committee also investigated how legally designating TIPs as “Emergency Responders (Private Sector) (PS)” would aid in accomplishing their task of restoring telecommunications infrastructure.¹²

3.1 Security for Private Facilities

Following Hurricane Katrina, civil unrest ensued in New Orleans, and TIPs were in need of security protection to safely move into the affected areas. TIPs initially reached out to the Government for security protection; however, interpretations of the Stafford Act limited industry’s ability to receive Government security assistance from the National Guard. For example, one carrier noted that it was repeatedly denied security protection from the National Guard through official channels at its fixed facilities and while conducting convoy operations to move emergency equipment and personnel into New Orleans. The carrier was eventually able to obtain some security assistance from the National Guard informally, but this was sporadic and resulted in delays. Another carrier was unclear on how Northern Command perceived its role in providing security assistance to TIPs. The carrier was overwhelmed with requests for granular detail about the restoration process over several weeks. The request for data diverted the carrier’s resources from the restoration efforts and obliged it to focus on responding to data requests. It was informed later that regardless of the data, no assistance would be provided. The lack of protection for communications disaster response personnel delayed industry’s response to the disaster. Several companies then resorted to private security services to protect their workers and equipment but were subsequently informed that armed private security personnel were not permitted to carry weapons in Louisiana if they were not licensed by the State of Louisiana. Unfortunately, the process of engaging and retaining private security service providers gave rise to delays in restoration. For example, in one case, the use of private security delayed restoration efforts 5 days. This included time necessary to execute contracts for services, travel time to the disaster area, and time necessary to set up support infrastructure (e.g., sleeping accommodations, showers, toilet facilities) for these additional personnel in the disaster area. State licensing requirements also contributed to delays in many cases.

Although ESF-13 applies to “Federal-to-Federal support or Federal support to State and local authorities,” it assigns some responsibility for public safety and security to the private sector.¹³ Accordingly,

ESF-13 does not distinguish between the public and private sector when declaring that the Federal Government can provide security assistance for response and recovery activities “where locally available resources are overwhelmed or are inadequate, or where a unique Federal capability is required.”¹⁴ Once the need is determined, ESF-13 activates Federal security assistance aimed at “providing security forces and establishing protective measures around the incident site, critical infrastructure, and/or critical facilities.”¹⁵ Unfortunately, in several instances, this standard was not applied to TIPs even though they were restoring critical infrastructure.

3.2 Priority Access to Critical Resources

Interpretations of the Stafford Act and lack of specificity of the language in ESF-7 and ESF-12 hindered industry’s ability to obtain priority access to necessary resources (e.g., fuel, water, power, vehicles, food and shelter) that were typically provided by the Federal Government to entities who were recognized and treated as official emergency responders. In addition, TIPs faced challenges trying to provide housing for their personnel restoring the infrastructure. There was a lack of coordination with and support from the Federal Government to secure housing for company personnel who were called in to help restoration efforts. In one instance, FEMA requested information detailing a carrier’s temporary housing requirements. The carrier provided this information, but then FEMA declined to offer housing support to the carrier since the housing was on a Federal parcel. In some cases, FEMA commandeered rooms in local hotels that were previously secured by carriers for their restoration teams, and billeting at military bases was not allowed for TIPs. Industry was again delayed in its recovery process because of a lack of housing for its restoration crews.

In addition, the hurricane’s damage left TIPs with limited energy options. Although most companies had extensive plans in case of power outages, the lack of civil order coupled with the extent of the destruction severely impaired companies from carrying out those plans. Specifically, several cellular sites were equipped with backup generators with enough fuel to last for 2 to 3 days, but a number of those generators were stolen.

Fuel suppliers contracted to maintain those sites were often unilaterally commandeered and, in some cases, State officials redirected fuel tankers intended for telecommunications facilities to other locations.

3.3 Priority Site Access Authorization

The day after Hurricane Katrina hit, industry repair crews ready to begin restoring service could not obtain permission from officials to enter the disaster area, preventing telecommunications services from being restored as quickly as they should have been. TIPs had difficulty gaining access to restricted facilities, which significantly hindered quick response. Specifically, inconsistent access authorization policies delayed crews and burdened incident management teams. For example, FEMA letters authorizing access to restricted areas were changed repeatedly. Wireless technicians and emergency response workers were consequently delayed in getting access to damaged cell sites because local law enforcement agencies were not aware of FEMA authorization, did not respond appropriately to access letters, or did not know when they were able to allow recovery crews into the areas. Furthermore, predelivery of equipment necessary for the timely recovery of wireless critical infrastructure also was not permitted into secure locations near the expected impacted areas. This included equipment that was crucial to establishing wireless coverage in the areas where Federal, State, and local agencies were staging their operations. The changing interpretations of FEMA authorization letters and varying interpretations of those who were eligible to access restricted areas caused TIPs substantial delays in their recovery and restoration efforts. In addition, the ESF-13 guidelines did not provide badging and credentialing procedures that would have substantially helped TIPs gain needed access to sites where critical telecommunications infrastructure was located.

The NSTAC has previously examined access and credentialing issues and has made recommendations to remedy gaps in the current policy. In 2003, the NSTAC recommended to the President that he “direct the appropriate departments and agencies to...coordinate with industry to develop a plan for controlling access at the perimeter of a disaster area in coordination with State and local Governments.”¹⁶ This recommendation was especially important given

that perimeter access laws are, in general, beholden to State and local regulation. Unfortunately, as the NSTAC indicated in a 2005 report, there is currently “no standard Government policy...for private sector use in planning activities for any perimeter control issues.”¹⁷ Therefore, the Committee recommended that the President direct appropriate agencies to work with industry “to develop a national plan for controlling access at the perimeter of a national special security event or a disaster area.”¹⁸ Gaining access to critical areas, however, remains a salient issue for TIPs. The NSTAC Telecommunications and Electric Power Interdependency Task Force has recently reiterated the need to improve access to disaster areas by implementing the perimeter access measures noted in its Trusted Access report and has asked the President to direct the appropriate Government agency to include site access “as part of the Emergency Responder planning process to ensure priority restoration to critical telecommunications...”¹⁹ The persistent policy lapse has created an environment in which the Federal Government may task TIPs with certain recovery activities without facilitating coordination with State and local officials charged with implementing jurisdictional perimeter access laws. The recent hurricane response efforts in the Gulf region demonstrated that vital telecommunications restoration efforts were stalled as a result of this situation.

3.4 Legal and Regulatory Issues

Many companies turned to the Federal Government for support because the civil unrest, coupled with the unprecedented level of damage from the storm and subsequent flooding hindered their access to the disaster site and to necessary resources, thus impairing their ability to repair the damaged critical infrastructure on their own. When requesting support from the Federal Government, many companies were unable to receive assistance because Federal agencies indicated that they did not have the authority to provide them support under the Stafford Act, and the NRP did not guide an interpretation that would enable that support.

3.4.1 The Stafford Act

The legal predicate for interpreting the authority of the Federal Government to provide assistance to TIPs is the Stafford Act. Congress stated that its intent in creating the Act was “to provide an orderly and continuing means of assistance by the Federal Government to State and local Governments in carrying out their responsibilities to alleviate the suffering and damage which result from such disasters by,” among other things, “achieving greater coordination and responsiveness of disaster preparedness and relief programs.”²⁰ The Act acknowledges the need for robust coordination; however, it does not clearly address coordination with the private sector. The Stafford Act provides assistance to “State or local Governments for the repair, restoration, reconstruction, or replacement of a public facility damaged or destroyed by a major disaster and for associated expenses incurred by the Government.”²¹

Although the language of the statute does not specifically preclude the private sector from receiving resources under the Act, it does not clearly grant the Federal Government authority to provide assistance to private entities, apart from nonprofit organizations. It states that the President can provide resources to “a person that owns or operates a private non-profit facility damaged or destroyed by a major disaster for the repair, restoration, reconstruction, or replacement of the facility and for associated expenses incurred by the person.”²² In addition, the law states that the President can “coordinate all disaster relief assistance (including voluntary assistance) provided by Federal agencies, private organizations, and State and local Governments.”²³ Section 5170(b)(3) of the Act also allows Federal departments and agencies to “provide assistance essential to meeting immediate threats to life and property resulting from a major disaster.”

This permission to “render assistance” to prevent loss of life or other serious harm stems from a long-standing tradition embodied in policy, regulation, statute, and international obligation. Indeed, the focus of this discussion is properly on the existence of present

authority to assure participation by necessary private sector infrastructure stewards in actions directed at such life saving activity, rather than eligibility of private sector entities for reimbursement.

Among relevant existing authority directing the rendering of assistance to prevent loss of life are the multilateral and unilateral maritime treaty obligations under which the Coast Guard and military are obligated to render assistance to vessels in distress.²⁴ Interpretation of policy implementing United States bilateral treaties such as the Treaties of Commerce, Friendship, and Navigation in place with dozens of Nations incorporate a “right of assistance entry” for vessels and aircraft.²⁵ All ship and aircraft commanders are obligated to assist those in danger of being lost at sea. This long-recognized duty permits assistance entry to render emergency assistance to those in danger or distress at sea. In general, military commanders are permitted to render such assistance to prevent loss of life upon request of civil authorities pursuant to Department of Defense policy for Immediate Response Authority.²⁶

Absent from the Stafford Act is any direct reference to Federal assistance to “for-profit” entities, and it does not recognize that TIPs, which own about 80 percent of the Nation’s critical infrastructure, play a critical recovery role in disasters to address the threats to public health and safety, life, and property.

3.4.2 The Defense Production Act

The NSTAC examined other laws that have been amended to reflect the importance of critical infrastructure in NS/EP efforts. For example, the Defense Production Act (DPA) of 1950 [Public Law 81-774] provides DHS the authority to redirect production and distribution of certain response and incident management resources. The DPA is the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. Among other things, the DPA authorizes the President to demand that companies accept and give priority to Government contracts that the President “deems necessary

or appropriate to promote the national defense.”²⁷ The term “national defense” has traditionally been interpreted very narrowly and generally only included those elements supporting military operations.

In 2003, Congress passed the Defense Production Act Reauthorization Act of 2003 [Public Law 108-195], which was amended to broaden the definition of “national defense” to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. The broader definition specifically includes “restoration” and “preparedness” as part of national defense because of the central role critical infrastructures, such as telecommunications, play in the overall security of the Nation. There is close relationship between the DPA and the Stafford Act. However, when the DPA was amended, there was no parallel effort to modernize the definitions in the Stafford Act, which may have contributed to some of the confusion in responding to Hurricane Katrina.

DPA authorities are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or man-caused event. The Department of Commerce has redelegated DPA authority under Executive Order (EO) 12919, National Defense Industrial Resource Preparedness, as amended, to the Secretary of Homeland Security to place and, upon application, to authorize State and local Governments to place priority-rated contracts in support of Federal, State, and local emergency preparedness activities. Essentially, this provision allows the Federal Government to assist a private infrastructure provider in obtaining goods or services necessary to protect, restore, or prepare the infrastructure for an extraordinary event.

3.4.3 The National Response Plan

The NRP is not a legally binding document, but it is an essential policy document that provides an all-hazards framework for the Nation to manage domestic incidents and guides the implementation of the Stafford Act. Federal, State, and local Governments did not provide assistance to TIPs through the NRP because the plan does not specifically identify or include private sector entities that are involved in restoring vital communications

infrastructure as emergency responders in ESFs. Appendix 3 of the NRP notes that the HSA includes “private sector emergency response providers” as components of terrorism preparedness efforts, but it does not specifically include TIPs in this category of emergency responders. Private sector emergency response providers are referenced in the NRP but are not fully integrated into the ESFs, which provide details regarding how Federal agencies are to provide support to all levels of Government and other jurisdictions.

4 Findings

The NSTAC finds that private TIPs need non-monetary Federal assistance and support during a national disaster to facilitate the response, recovery, and restoration of our Nation’s critical infrastructure. This support includes priority access to restricted disaster sites, fuel, power, water, billeting, and workforce and asset security. The NSTAC finds that a reasonable interpretation of the Stafford Act, in conjunction with modifications to the NRP and its ESFs that recognize TIPs as “Emergency Responders (PS),” would greatly facilitate and enhance the national response, recovery, and restoration of the Nation’s critical infrastructure after a national disaster.²⁸

4.1 The Stafford Act and Legal Interpretation of Federal Assistance

The NSTAC finds that the provisions of the Stafford Act, when taken as a whole [see 42 U.S.C. Sec. 5170, et. seq. (2005)], support a legal interpretation that establish that Federal assistance may lawfully be provided to TIPs during the recovery and restoration periods of a disaster. The Government attempts to address immediate threats to public health and safety before, during, and following a disaster, and telecommunications facilities and services are key to achieving this goal. Roughly 80 percent of the Nation’s telecommunications critical infrastructures are privately owned and operated and cannot be recovered and restored without TIPs. Accordingly, it is reasonable to interpret the Act to permit Federal assistance to TIPs for the security and critical resources necessary to recover and restore telecommunications facilities for the benefit of the affected community. The Stafford Act, while not authorizing grant assistance to for-profit entities, does not preclude Federal assistance to

for-profit entities to address “immediate threats to life and property” and public health and safety following a disaster. The Committee believes that because TIPs own and operate private facilities necessary for maintaining emergency services determined critical to either the disaster response or the health and safety of the community, they should qualify for non-monetary Federal assistance.

The NSTAC is aware of legal guidance from FEMA set forth in an e-mail memorandum from the FEMA Assistant General Counsel to DHS on September 9, 2005, that provides a legal interpretation of the Stafford Act consistent with the NSTAC’s interpretation that would provide TIPs Federal resources “to complete the Federal mission of assisting with immediate threats to life and property...”²⁹ The NSTAC, in accordance with FEMA’s guidance, believes that such assistance granted to the privately owned facility would not be provided for the benefit of the specific facility but for the health and safety of the community as a whole and would help ensure the continuity of Federal operations support to the disaster. Difficulty arose in the post-Hurricane Katrina disaster response when FEMA did not interpret the Stafford Act in the same manner as the NSTAC and the recent FEMA guidance. Immediately after Hurricane Katrina, neither FEMA nor other Federal, State, and local Government personnel were willing to recognize TIPs’ restoration efforts as a Federal mission, even though ESF-2 states that TIPs support the Federal mission, and accordingly, the disaster assistance was not provided. Reluctance by FEMA or DHS to grant Federal assistance to TIPs is perplexing in light of the request by FEMA and the Federal Government for a list of top assets from TIPs. If the Federal Government recognizes that TIPs have assets that are critical to the Federal mission, then it should follow that non-monetary Federal assistance to help TIPs protect those assets is necessary and appropriate.

4.2 The Stafford Act and TIPs as Emergency Responders (PS)

The NSTAC also finds that the Stafford Act does not directly recognize the role of private TIPs in the recovery and restoration of NS/EP services and functions in disasters. The statute does not mention critical TIPs, nor does it adequately provide for direct

assistance to for-profit entities during a disaster. This lack of recognition led to confusion, differing interpretations, and a lack of consensus among Government officials during Hurricane Katrina, significantly delaying the disaster response. NSTAC finds that specific recognition and designation of TIPs as “Emergency Responders (PS)” in the statute will help eliminate future statutory confusion and will make future disaster response, recovery, and restoration of essential telecommunications facilities and services faster and more efficient.

The NSTAC’s examination revealed that during and following Hurricane Katrina, TIPs faced numerous problems because of a lack of communication, coordination, and understanding of the existing legal and regulatory framework. In the aftermath of Hurricane Katrina, Federal authorities asked and expected TIPs to repair networks damaged by Katrina, but they did not provide TIPs with the vital resources necessary to do so. Had those private sector companies received the support they requested, the communications problems among first responders, civilians, and Federal officials could have been at least partially alleviated. Providers of critical NS/EP telecommunications infrastructures worked through a patchwork of Federal, State, and local authorities and jurisdictions each with varying interpretations of statutes governing cooperation and coordination with the private sector. Confusion about roles and responsibilities was pervasive, and industry expressed concern that the existing legal and regulatory environment is not conducive to ensuring an effective response to disasters.

4.3 The NRP and TIPs as Emergency Responders (PS)

The NSTAC finds that the NRP does not clearly delineate the roles and responsibilities of State and local Governments vis-à-vis TIPs, nor does it recognize and identify TIPs as Emergency Responders (PS). The NRP was not properly leveraged because State and local Governments were not aware of the numerous protocols that identified their roles and responsibilities in the event of a disaster, such as Hurricane Katrina. Even if the plan had been adequately used in the aftermath of Hurricane Katrina, the NSTAC finds that the NRP and its ESFs could be enhanced with protocols that identify TIPs as Emergency Responders

(PS), which would clarify their roles and responsibilities in repairing critical infrastructure. Federal, State, and local Government officials did not view TIPs as essential components of the emergency response effort; therefore, these officials did not help to facilitate assistance to TIPs so that telecommunications infrastructure could be quickly restored.

Although the concept of private sector emergency responders is referenced in Appendix 3, the NRP neither clarifies this concept nor expands on it elsewhere in the plan. Moreover, references to emergency response providers in the HSA and NRP focus on Government entities, rather than the private sector. TIPs would be in a position to better assist the Government in restoring key telecommunications infrastructure if the term Emergency Responder (PS) were categorized in the NRP with a definition that delineates qualifying entities, including TIPs. The definition should also clarify that Emergency Responders (PS) are eligible to receive non-monetary emergency support commensurate with that granted to other emergency response providers.³⁰

5 Conclusion

The NSTAC concludes that differing interpretations of the Stafford Act and lack of a designation of TIPs as Emergency Responders (PS) in the interpretation of and in the Act itself as well as in the NRP prevented the Federal Government from authorizing assistance to the private sector, which hindered TIPs in repairing critical infrastructure in the aftermath of Hurricane Katrina. It is essential that private sector TIPs have emergency access to resources needed to restore critical infrastructure in the event of a large-scale natural disaster or terrorist attack to ensure proper NS/EP communications. The Federal Government amended the DPA in 2003 to specifically include critical infrastructure protection and restoration as part of national defense and provide the ability of the Federal Government to prioritize goods and services to assist in restoration of infrastructures. Unfortunately, no corresponding changes were made to the Stafford Act. The current policy, legal, and regulatory landscape should be

clarified to eliminate confusion and modified to provide adequate preparation and planning mechanisms for the Federal Government and TIPs to work together to respond to a catastrophic event.³¹

The NSTAC concludes that the Stafford Act should be officially interpreted to permit direct nonmonetary assistance to TIPs during a disaster to aid in the speedy response, restoration, and recovery for the benefit of public safety, health, property and life.³² TIPs should be legally designated as Emergency Responders (PS), named and defined as such in the Stafford Act, and should be treated as Emergency Responders (PS) who receive non-monetary assistance under the Act.³³ This designation would result in a requirement that TIPs be included in the Federal, State, regional, and local emergency planning process and would allow them priority access to restricted areas to restore essential infrastructure.³⁴ Designation of TIPs as Emergency Responders (PS) during Hurricane Katrina would have enabled companies to receive security protection from the National Guard, priority access to critical resources, and priority site access authorization. Designating TIPs as Emergency Responder (PS) in the Stafford Act will eliminate the legal and regulatory hurdles experienced in the Hurricane Katrina disaster and will significantly expedite industry's response efforts in future disasters.

The NSTAC also concludes that the NRP should be modified to identify TIPs as Emergency Responders (PS) and to establish a protocol with them to facilitate priority site access and access to critical resources during a disaster. The HSA and NRP include definitions of emergency response providers but reserve the designation for Government entities. Accordingly, the NSTAC believes that a separate designation is needed for TIPs. Under the HSA and NRP, emergency response providers perform roles and responsibilities specific to Government that are distinct from the those of private sector emergency response personnel. A separate classification of Emergency Responder (PS), which includes TIPs, is necessary to clarify the legal status of TIPs and enable them to best restore key infrastructure after an emergency or national disaster.

TIPs are necessary components of an emergency response effort, and recognizing that the NRP provides a unified incident management framework for all disciplines, TIPs should be integrated into the all-hazards approach to provide a truly comprehensive plan. The NRP should be modified to establish a protocol that incorporates the roles and responsibilities of TIPs in the event of a natural disaster or terrorist attack. This protocol should detail with whom TIPs should correspond at the Federal, State, and local levels and should also provide the proper credentialing process to allow TIPs access to critical sites as Emergency Responders (PS). The NSTAC acknowledges that other efforts are underway to establish comprehensive and effective credentialing procedures. An Emergency Responder (PS) designation for TIPs will help identify individuals authorized to access disaster sites and to receive the appropriate credentials. New protocols established within the NRP and ESF framework should clarify response actions and help create a culture where TIPs have a legal status as Emergency Responders (PS) and are treated as such by Federal, State, and local Government officials. Accordingly, the DHS Office of Grants and Training and the Office of Legislative and Intergovernmental Affairs should play a central role in identifying the implications of the Emergency Responder (PS) designation and then work with State and local Government stakeholders to follow through on the execution of this designation so that the Emergency Responders (PS) designation for TIPs can be implemented effectively.

The NSTAC recommends that the President designate TIPs as Emergency Responder (PS) through three different mechanisms. First, the President should direct DHS to modify the NRP and its ESFs to designate TIPs as Emergency Responders (PS) and to establish interfaces between Federal, State, and local Government, and private sector TIPs. This designation should be formalized by including a protocol in ESF-2, and other ESFs as appropriate, that establishes the way in which TIPs are to work with Federal, State, local, and tribal Governments during and after a national disaster.

Second, because of the urgency of this problem, the President should issue appropriate guidance to clarify differing interpretations of the Stafford Act. This guidance should officially interpret 42 U.S.C. § 5170 (2005) and establish that private sector TIPs are eligible to receive nonmonetary Federal assistance under the Stafford Act. The Directive should name these entities as Emergency Responders (PS) eligible for non-monetary disaster relief in the aftermath of a national disaster to ensure the stability of the Nation's telecommunications infrastructure.

Finally, the President should direct the Secretary of Homeland Security to work with Congress—specifically, the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs—to amend the Stafford Act to designate TIPs as Emergency Responders (PS) who are eligible to receive Federal assistance under law. Permanent codification of the Emergency Responder (PS) designation should eliminate any future differing interpretations of the Act and will support the establishment of a permanent protocol under the NRP-ESF framework where Federal, State, and local Governments interface with TIPs for emergency planning, response, recovery, and restoration. The President should coordinate this amendment to the Stafford Act with other ongoing efforts to modify the Act's language in the wake of Hurricane Katrina.

The NSTAC recommends that the President implement all three mechanisms to better prepare the Nation for future events such as Hurricane Katrina. The National Weather Service forecasts that the 2006 hurricane season, beginning on June 1, 2006, will be as destructive as the 2005 season; therefore, it would be helpful to implement these recommendations before this date.

6 Recommendations

NSTAC Recommendations to the President

Based on its findings, the NSTAC recommends that, no later than June 1, 2006, in accordance with the responsibilities and existing mechanisms established by EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, and other existing authority, the President establish and codify the term Emergency Responder (PS) to include TIPs and ensure non-monetary assistance, including accessing restricted areas and obtaining fuel, water, power, billeting, and workforce and asset security, to them by—

- ▶ Directing the DHS to modify the NRP and its ESFs to designate TIPs as Emergency Responders (PS) and to establish protocols and procedures for the way in which Federal, State, local, and tribal Governments should work with TIPs before, during, and after a national disaster,
- ▶ Issuing appropriate Presidential guidance to define Emergency Responders (PS) under the Stafford Act and other authorities as appropriate, to align with the broadened definition of national defense in the 2003 amendments to the DPA. Specifically, the guidance should make clear that key response personnel of critical telecommunications infrastructure owners and operators be defined as Emergency Responders (PS) and should receive non-monetary Federal assistance under the Stafford Act, and
- ▶ Directing the Secretary of Homeland Security to work with Congress to align the Stafford Act and other appropriate legislative authorities with the DPA by codifying the designation of private sector TIPs as Emergency Responders (PS) and by codifying the official interpretation that for-profit TIPs should receive Federal assistance.

Footnotes

- 1** EO 12382, President's National Security Telecommunications Advisory Committee, September 13, 1982.
- 2** For this report, telecommunications infrastructure providers are those entities who own and operate infrastructure and/or provide enabling software, hardware, and/or services for the purposes of providing "telecommunications" as defined in and consistent with the definition found in National Communications System Manual 3-1-1—namely, "the transmission, emission, or reception of intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio visual or other electronic, electric, electromagnetic, or acoustically coupled means, or any combination thereof."
- 3** The NSTAC acknowledges that proposed legislation exists to amend the Stafford Act and the Homeland Security Act of 2002; however, the Committee does not take a position on any specific bill.
- 4** FEMA. "Your Guide to FEMA." April 2005. <http://www.training.fema.gov/emiweb/dfto/docs/Your%20Guide%20to%20FEMA.doc>
- 5** NRP, ESF-2.
- 6** Ibid.
- 7** NRP, ESF-13.
- 8** NRP, ESF-7.
- 9** NRP, Private Sector Coordination Support Annex.
- 10** 6 U.S.C. § 101(6)(2005) states, "the term 'emergency response provider' includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities." The NRP's definition in Appendix 1, Glossary of Key Terms, inserts "and tribal" following "local" and notes that "emergency response providers" are "also known as 'emergency responders.'"
- 11** NRP, Appendix 3, Authorities and References.
- 12** The Committee considered the advantages of designating TIPs as "Emergency Responders (PS)" to remove all doubt as to whether TIPs could receive Federal disaster relief under the Stafford Act and require them to be included in Federal, State, regional, and local emergency planning processes. This designation would also make TIPs eligible to priority access to restricted disaster sites in accordance with official credentialing procedures.
- 13** NRP, ESF-13
- 14** NRP, ESF-13.
- 15** Ibid.
- 16** NSTAC, Vulnerability Task Force, Trusted Access, January 2003, p. 10.
- 17** NSTAC Trusted Access Task Force, Screening, Credentialing, and Perimeter Access Controls, January 2005, p. 6.
- 18** NSTAC Trusted Access Task Force, Screening, Credentialing, and Perimeter Access Controls, January 2005, p. 9.
- 19** NSTAC Telecommunications and Electric power Interdependency Task Force, People and Processes: Current State of Telecommunications and Electric Power Interdependencies, January 2006, Section 6.0.
- 20** 42 U.S.C. § 5121 (2005).
- 21** 42 U.S.C. § 5172(a)(1)(A) (2005).
- 22** 42 U.S.C. § 5172(a)(1)(B) (2005).
- 23** 42 U.S.C. § 5170(a)(2) (2005).
- 24** International convention for the safety of life at sea, 1974, with annex. International Maritime Organization <http://www.imo.org/home>.

25 Statement of Policy by the Department of State, Department of Defense (DoD), and United States Coast Guard Concerning the Exercise of the Right of Assistance Entry of 8 August 1986. This policy statement is implemented within the DoD by CJCSI 2410.01B. This instruction specifically deals with assistance entry by aircraft for life-threatening and nonlife-threatening situations.

26 The Immediate Response Authority permits commanders to take immediate action to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions. Commanders may take whatever action the circumstances reasonably justify. As soon as practical, the commander rendering assistance shall report the fact of the request from civil authorities, the nature of the response, and any other pertinent information through the chain of command. In the case of civil disturbances, which may result from a terrorist act, military commanders may rely on this authority, which is contained in DoDD 3025.12 [MILITARY ASSISTANCE FOR CIVIL DISTURBANCES (MACDIS)]. See also DoDD 3025.15 [MILITARY ASSISTANCE TO CIVIL AUTHORITIES] and DoD Directive 3025.1 [MILITARY SUPPORT TO CIVIL AUTHORITIES (MSCA).]

27 50 U.S.C. App. 2071(a) (2002).

28 The term Emergency Responder (PS) should not be confused with the term First Responders, which includes fire, police, and other governmental personnel who arrive immediately at a disaster site to help protect public safety, health, welfare, and property. Rather, Emergency Responders (PS) are TIP personnel who need access to disaster sites to repair, restore, and reconstitute privately owned and operated critical infrastructure facilities.

29 FEMA E-mail Memorandum from Assistant General Counsel to FEMA personnel, September 9, 2005: Guidance, "Reimbursable Security Costs Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act." This guidance contains a propriety marking indicating that the contents of the guidance should not be disclosed to persons other than the original addressees of the e-mail. However, the NSTAC companies received a copy of the guidance through the Telecommunications Information Sharing and Analysis Center process.

30 The NSTAC companies are willing to work with DHS to establish a definition of Emergency Responders (PS) and to identify the personnel who are included in this definition.

31 The NSTAC companies are willing to work with DHS to establish processes and procedures for implementing the new designation of TIPs as Emergency Responders (PS) in the Stafford Act.

32 The NSTAC is not recommending that for-profit companies receive monetary cost reimbursement pursuant to the Stafford Act; rather, it recommends that TIPs receive designation as Emergency Responders (PS), which would permit them to receive priority access to disaster sites and access to critical resources necessary for the response and recovery effort such as security, fuel, water, and billeting.

33 The NSTAC companies are willing to work with DHS to establish a definition of Emergency Responder (PS) and to identify the personnel who are included in this definition.

34 The NSTAC's Telecommunications and Electric Power Interdependency Task Force (TEPITF) came to a similar conclusion in their report, "People and Processes: Current State of Telecommunications and Electric Power Interdependencies." However, the TEPITF's definition of Emergency Responder includes both telecommunications and electric power professionals who are the key response personnel of critical infrastructure owners and operators.

Appendix A

Task Force Members,
Other Participants, and
Government Personnel

Task Force Members

Telcordia Technologies, Inc.

Ms. Louise Tucker, Chair

Lockheed Martin Corporation

Mr. Gerald Harvey, Vice Chair

AT&T, Inc.

Ms. Rosemary Leffler

Mr. Harry Underhill

BellSouth Corporation

Mr. David Barron

The Boeing Company

Mr. Robert Steele

Computer Sciences Corporation

Mr. Guy Copeland

Lucent Technologies

Mr. Michael Garson

Microsoft Corporation

Mr. William Guidera

Nortel

Mr. Raymond Strassburger

Northrop Grumman Corporation

Mr. Scott Freber

Qwest Communications

International, Inc.

Mr. Jeffery Hackman

Rockwell Collins, Inc.

Mr. Kenneth Kato

Sprint Nextel Corporation

Mr. Michael Fingerhut

VeriSign, Inc.

Mr. Michael Aisenberg

Verizon Communications, Inc.

Mr. Dennis Guard

Mr. Michael Hickey

Other Participants

AT&T, Inc.

Mr. Adam McKinney

BellSouth Corporation

Mr. Lloyd Nault

Cingular Wireless LLC

Mr. James Bugel

CTIA—The Wireless Association

Mr. Christopher Guttman-McCabe

Edison Electric Institute

Mr. Laurence Brown

George Washington University

Dr. Jack Oslund

Lucent Technologies

Ms. Selma Munden

Microsoft Corporation

Mr. Paul Nicholas

North American Electric Reliability

Council

Mr. Louis Leffler

Qwest Communications

International, Inc.

Mr. Jon Lofstedt

Science Applications International Corporation

Mr. Henry Kluepfel

Sprint Nextel Corporation

Mr. Tim Bowe

Ms. Allison Growney

Mr. John Stogoski

Telecommunications Industry Association

Mr. William Belt

Verizon Communications, Inc.

Mr. Drew Arena

Government Participants

Department of Defense

Ms. Hillary Morgan

Department of Homeland Security

Mr. Thomas Falvey

Mr. Jeffrey Glick

Mr. Frank Lalley

Mr. Thad Odderston

Mr. Eric Werner

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE



**NSTAC Report to the President on
Telecommunications and Electric Power
Interdependencies**

*People and Processes: Current State of Telecommunications
and Electric Power Interdependencies*

January 31, 2006

Table of Contents

Executive Summary	ES-i
1 Introduction	1
1.1 Overview	1
1.2 Long-Term Issues	2
2 Status of Previous NSTAC Recommendations	2
2.1 Previous NSTAC Recommendations	3
2.2 NSTAC Recommendation Analysis	3
3 Priority Restoration	4
3.1 Electric Power and Telecommunication Priority Restoration Process	4
3.1.1 Electric Power	4
3.1.2 Telecommunications	5
3.2 Impacts of Natural Disasters and Human Attacks on Telecommunications and Electric Power Service	6
3.2.1 September 11, 2001	6
3.2.2 2003 Blackout	6
3.2.3 Hurricane Activity	7
3.3 Emergency Communications During Outage Situations	8
3.4 Implications of Changing Telecommunications Network Design	8
4 Information Sharing and Liability	8
4.1 Current Information Sharing Environment	8
4.2 Levels of Information Sharing	9
4.3 Liability Issues	10
5 Conclusions	11
6 Recommendations	12
Appendices	
A Electro-Magnetic Pulse	A-1
B Task Force Members, Other Participants, and Government Personnel	B-1

Executive Summary

In the wake of the terrorist attacks of September 11, 2001, the 2003 North American blackout, and the recent devastating hurricane seasons, the interdependencies between the telecommunications and electric power sectors have become increasingly apparent. In response, the President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) convened a task force in the spring of 2005 to investigate national security and emergency preparedness (NS/EP) issues associated with the interdependencies between these two sectors. This task force, the Telecommunications and Electric Power Interdependency Task Force (TEPITF), is charged with examining NS/EP concerns surrounding operational issues between the two sectors and how these interdependencies will affect the future of the telecommunications network.

This report addresses the Administration's concerns that telecommunications and electric power interdependencies may create additional vulnerabilities, particularly in emergency response situations. It establishes a baseline of the current state of interdependencies between the two sectors using the people involved and the processes between them as the lens for critical evaluation. This report presents the NS/EP concerns associated with the interdependencies of the telecommunications and electric power sectors, focusing on the current operational issues between the sectors and how the interdependencies will affect both infrastructures.

People and Processes: Current State of Telecommunications and Electric Power Interdependencies is the first of two reports that the NSTAC is developing to address interdependencies between the two sectors. This report examines three main topics: (1) past NSTAC recommendations; (2) priority restoration; and (3) information sharing and liability.

From its deliberations, the task force drew several conclusions regarding interdependencies between the telecommunications and electric power sectors. In reviewing past NSTAC recommendations, the task

force concluded that interdependencies are increasing in importance to industry and Government. However, because the main focus has been dependencies, significant work remains in regard to understanding the implications of interdependencies.

Next, on the basis of its review of priority restoration, the task force determined that the most useful element of the sectors' emergency restoration relationship is the open dialogue between the points of contact at the local level. Furthermore, key response personnel from telecommunications and electric power service providers could be designated as Emergency Responders, similar to First Responders. This classification would allow telecommunications and electric power service providers to be involved in the Federal, State, regional, and local emergency planning processes; to actively participate in emergency operation centers (EOC) during emergency events; and through the effective use of credentialing, gain timely and secure access to restricted areas to restore their critical assets. Another imperative is the timely fuel supply replenishment process for electric power generators at critical telecommunications and electric power service providers' internal communications network assets. Further, emergency response communication between telecommunications and electric power sectors may be improved at the local level by enabling the EOCs to interoperate without relying on the public commercial telecommunications infrastructure.

The task force also concluded that effective information sharing models are not prevalent at the level of Emergency Responders. Collaboration between the two sectors is most important at the regional and local levels to ensure the rapid recovery of both sectors. The Telecommunications and Electricity Sector Information Sharing and Analysis Centers (ISAC) are logical candidates to coordinate information sharing at the broadest and highest levels between the two sectors, ideally serving as a resource for each sector to use when communications are difficult at the local level and guidance is needed on how to proceed. Additionally, the task force found that liability issues related to information sharing have not been considered at the local level of communications.

On the basis of these conclusions, the NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies to—

- ▶ Define and establish the term “Emergency Responder” within the National Response Plan and other appropriate plans, guidance, directives, and statutes.
- ▶ Ensure that key response personnel of critical infrastructure owners and operators in the telecommunications and electric power sectors be designated as Emergency Responders, and included in local, regional, State, and Federal Government emergency plans.
- ▶ Include fuel supply to critical telecommunications and electric power infrastructures as part of the Emergency Responder planning process to ensure that fuel deliveries receive adequate priority, access, and security during a disaster.
- ▶ Foster and promote effective emergency coordination structures to ensure reliable and robust communication between the two sectors and local, regional, State, and Federal Governments.
 - Review examples of proven priority restoration models at the State and regional levels. Encourage States and metropolitan regions without effective models to improve and update their existing frameworks.
 - Encourage effective information sharing models at the local/regional Emergency Responder levels, both in advance of a natural disaster and during the emergency restoration period. When developing these models, liability issues should be considered.

1 Introduction

1.1 Overview

An understanding of the significant interdependencies between the telecommunications and electric power infrastructures is a critical component of the Nation's security preparedness. The destructive hurricane seasons of the past several years, coupled with the events of September 11, 2001, have clearly demonstrated the dependence of the telecommunications network on the electric power grid while also highlighting the successes and shortcomings in incident management and recovery. Experiences such as these have exposed not only the relationship between these two sectors but also the critical role these two sectors play in supporting the reliability and resiliency of the other critical infrastructures. In addition, as the communications network becomes increasingly distributed, issues of reliability and ease of communication and coordination between the telecommunications and electric power industries will become ever more important and challenging during disaster recovery efforts.

The NSTAC recognition of, and reflection on, the existence of these critical interdependencies notably predates recent attention. In 1987, the Committee established the first Energy Task Force to develop recommendations to mitigate the effects of electric power outages on telecommunications. Following this effort, the NSTAC established a follow-on Energy Task Force charged to support the Office of the Manager, National Communications System (OMNCS) in its efforts with the Department of Energy (DOE) to develop criteria and a process for identifying NS/EP telecommunications facilities that qualify for electric power restoration and priority fuel distribution. More recently, Mr. F. Duane Ackerman, Chairman and Chief Executive Officer, BellSouth and Chair of the President's NSTAC, highlighted interdependency concerns between the two sectors in his speech at the Research and Development Exchange Workshop in October 2004, specifically noting the need for enhanced battery technology.

Following the NSTAC XXVIII Meeting in Washington, DC, on May 11, 2005, and per the guidance of the Committee of Principals, the IES established the TEPITF in 2005 to study NS/EP issues associated with the interdependencies between the telecommunications and electric power sectors. To ensure thorough investigation of the issues, the task force invited representatives from the United States (U.S.) electric power sector and Canadian power entities to participate in task force deliberations.

Until recently, the NSTAC's considerations of the power industry focused on the dependencies of the telecommunications and electric power sectors. This report, however, focuses on the interdependencies and establishes a baseline of the current state of interdependencies between the sectors. As such, the people and the processes related to the inter-sector interdependencies have been closely examined. Using this critical link as a lens for evaluation, this report presents NS/EP concerns associated with the interdependencies of the telecommunications and electric power sectors, focusing on the current operational issues between the two sectors and how the interdependencies affect both infrastructures. It gives particular attention to natural and human-made disasters, following a "cause-neutral" approach to the issue of service outages. The report analysis focuses on post-incident recovery and anticipatory mitigation issues with respect to interdependencies.¹

People and Processes: Current State of Telecommunications and Electric Power Interdependencies is the first of two reports that the NSTAC is developing to address interdependencies between the two sectors. The subsequent report will address long-term issues, focusing on technology and engineering solutions the two industries must consider to address the expected increasing interdependencies and manage them effectively.

The key issues addressed in this report are as follows:

- **NSTAC Recommendation Overview:** What actions have been taken by the Executive Branch on previous NSTAC recommendations regarding the electric power sector? Which recommendations that have not been acted upon remain relevant?

- ▶ **Priority Restoration:** Where does the telecommunications network fall in the electric power sector's queue of priority restoration? Who is primarily responsible for restoration of service problems when both sectors are involved? How do the people who restore service and respond to outages within each sector work together during emergencies?
- ▶ **Information Sharing and Liability:** How much information is currently shared between the two sectors' ISACs? What information should be shared between the ISACs? What, if any, are the liability issues stemming from interdependencies between the two sectors?

1.2 Long-Term Issues

Preliminary discussion of long-term issues includes the following:

- ▶ **Telecommunication Industry Changes:** Have technology-driven changes in the telecommunications sector (e.g., ubiquitous deployment of wireless, terrestrial transition to fiber optic networks, provision of broadband services by the energy sector, distributed network elements, and increased complexities through the introduction of next generation networks) created new kinds of interdependency vulnerabilities? Are the vulnerabilities newly created, on a larger scale, more of the same, or potentially reduced?
 - ▶ **Loss of Core Infrastructure of the Electric Power Grid and/or Telecommunications Networks:** Events damaging the core telecommunications sector's or electric power sector's infrastructure could induce prolonged outages. Threats such as electro-magnetic pulse (EMP), solar flares, and coronal mass emissions, or a coordinated attack triggering causative agent failure might transcend the destructive effects experienced from hurricanes; the September 11, 2001 attacks; and the August 2003 blackout. Therefore, the effects of these threats on the core infrastructure will be investigated to characterize unique interdependencies between the sectors during the recovery process.
- ▶ **Power Industry Changes:** Since deregulation, the electric power industry has undergone significant changes. The North American Electric Reliability Council (NERC) was established in 1968 to help ensure the reliability, adequacy, and security of the bulk electric system in North America. In 2005, the many policies that the industry had developed over decades were adapted and approved as 91 mandatory standards. The 2005 Energy Legislation will lead to formation of an Electric Reliability Organization.
 - ▶ **Restoration:** What are the physical and logical interdependencies between the two infrastructures in the aftermath of a very long outage?
 - ▶ **Science and Technology (S&T) Solutions:** What programs or projects underway in the Federal Government research labs represent potential solutions to existing and new interdependency vulnerabilities? What new S&T initiatives should be undertaken? In addition to extending battery life, what new S&T initiatives should be undertaken?
 - ▶ **Spectrum Policies:** To what extent are Federal policies concerning spectrum allocation, including the lack of dedicated spectrum for internal utility systems, hampering the ability to restore electric power as quickly and safely as possible?
 - ▶ **Interdependency Between the Sectors:** What, if any, actions can/should the President take to lessen the critical interdependencies between the telecommunications and electric power sectors during a prolonged emergency?

2 Status of Previous NSTAC Recommendations

NSTAC consideration of the relationship between the telecommunications and electric power sectors is not a recent development; however, consideration formerly centered on the study of dependencies as opposed to interdependencies. Relatively little follow-up research has been undertaken. The following section provides further detail on the status of past NSTAC recommendations.

2.1 Previous NSTAC Recommendations

Since its establishment in 1982, the NSTAC has made three distinct sets of recommendations pertaining to the dependency between the telecommunications and electric power sectors. First, research into dependencies began with the NSTAC's response to a Government request for industry's perspective on the options available to industry and Government for improving the EMP survivability of the Nation's telecommunications networks. On December 12, 1984, the NSTAC provided several policy recommendations on EMP to the President.² Second, in 1987, the NSTAC Telecommunications Systems Survivability Task Force concluded that the telecommunications industry would be extremely vulnerable to an extended electric power outage and recommended to the President that the Government initiate a study to identify options for ensuring electric power survivability as it related to telecommunications. Third, following the President's reply, the NSTAC formed the Energy Task Force. That task force, with participation from DOE, the National Communications System (NCS), and NERC, examined dependencies between the electric power and telecommunications sectors after a major earthquake. In 1988, the task force recommended:

- ▶ Further research on the impact of a major earthquake on the electric power, telecommunications, and transportation systems; and
- ▶ The establishment of a nationwide process for restoring electric power and distributing energy supplies during major emergencies.

As presented in the *Energy Task Force Final Report–1993*, the Energy Task Force's recommendations between its establishment in 1988 and its conclusion in 1993 included the following:

- ▶ Continued support of the operation, administration, and management of DOE's Telecommunications Electric Service Priority (TESP) program initiative.

- ▶ The assignment of Federal responsibility to establish a program for ensuring priority availability of fuel supplies for telecommunications companies during emergencies.
- ▶ The development of a program for assigning electric power restoration priorities to NS/EP telecommunications users and providers to accomplish the soonest possible service restoration.

2.2 NSTAC Recommendation Analysis

Since the NSTAC task force recommendations were issued in the early 1990's, neither the telecommunications nor electric power industries, nor the Federal Government has undertaken a formal interdependency study. In December 1993, however, the DOE initiated the TESP program with support from the NCS and NSTAC, giving the NCS Federal responsibility for administering this program. In 1996, the NCS created a TESP database with data supplied from the telecommunication facilities and power companies, which included telecommunications facilities serving critical State Government sites and power company information for each area. By 2001, TESP was no longer in use because it was difficult to keep such data current. In 2004, the NCS revived the TESP and initiated a Draft TESP Memorandum of Agreement (MOA) between the Telecommunications and Electricity Sector ISACs.

The Draft TESP MOA is under revision to become a Memorandum of Understanding (MOU) that will provide a framework for problem resolution. The purpose of this framework is to ensure that the electric and telecommunications industries work together to mitigate the effects of electric power outages on NS/EP telecommunications functions after an NS/EP event. The ISACs supporting inter-sector coordination will be parties to the MOU. The MOU acknowledges that preplanning and response coordination must be conducted at the local level. When local forces need assistance in these efforts, they may seek support from their respective ISACs. The ISACs will work together to assist the field forces in resolving the issue.

Other bodies have continued to study EMP effects. On July 22, 2004, the EMP Commission presented findings to Congress stating that “EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences.”³ The EMP Commission showcased the severity of this issue, aiming to catalyze debate and focus within the United States Congress.

Although some of these recommendations, as discussed above, remain valid, the current environment related to the interdependencies between the two sectors has changed drastically. Earlier recommendations focused on electric power service rather than development of a substantive incident management process, which both sectors believe is necessary. Given the significant loss of life and damage to personal property and economic impact caused by recent disasters, the TEPITF is taking a fresh look at the interdependencies between the two sectors. At the conclusion of its study, the task force will issue recommendations for the President that are relevant to the current environment, with a view toward mitigating the risks created by the sector interdependencies.

3 Priority Restoration

The events of September 11, 2001; the 2003 North American blackout; and the destructive 2004–2005 hurricanes, although differing in terms of geographic areas and duration of time, collectively demonstrated the validity of the shared concerns of the electric power and telecommunications sectors with respect to the priority restoration process.

3.1 Electric Power and Telecommunication Priority Restoration Process

3.1.1 Electric Power

Much like the telecommunications sector, the electric power sector incorporates an extremely complex network of generation, transmission grid, and distribution assets. The transmission grid, possibly the most complex element, includes more than 150,000 miles of transmission lines, delivers electricity from more than 850,000 megawatts of generation crossing the boundaries of utilities and States, and connects to systems in Canada and Mexico. Electric power service providers (EPSP) comprise investor-owned utilities,

municipal utilities, cooperatives, and Government-owned entities. In accordance with State laws and public utility regulations, EPSPs individually develop and maintain their priority restoration plans for outage recovery activities related to their own networks. These plans typically focus on taking the appropriate action to restore service to emergency and life support services, critical infrastructures, and the largest number of customers. EPSPs use outage management systems (OMS) to help detect outages and nonfunctioning assets, manage customer calls, prioritize emergency repairs, manage resources, and dispatch crews. Typically, the first priority addresses transmission line and substation outages, because local networks supplying power to customers cannot function unless the large transmission assets supplying power to the area are functioning. The next priorities are to restore power to emergency services and critical life support facilities, such as hospitals, police and fire stations, emergency call centers, and EOCs, as well as key infrastructures, including critical telecommunications, water, and sewerage assets; and to resolve dangerous situations, such as downed live wires. Then, the distribution feeder lines that supply the largest number of customers are addressed.

EPSPs vary significantly in their dependence on commercial telecommunication services for emergency operations (voice and data) communications and coordination, including OMS. Many have invested heavily in their private internal voice and data communication systems—such as radios, fiber optics, and microwave networks—for reliability coverage supporting mission-critical functions, such as process control systems, supervisory control and data acquisition (SCADA) systems, generation facilities, transmission grids, and the distribution network, including emergency response communications. Many of these systems include redundant internal elements, such as control centers served by both fiber and microwave to ensure reliability. Most EPSPs also have well-developed internal voice communication networks for dispatching crews for emergency repair operations as part of their OMSs, although they may rely on commercial wired networks for primary everyday communications because of their coverage over a large area and low cost. When crews come in from other areas to assist the local EPSPs in recovering

from extreme emergency events, the local EPSPs may have limited internal system capacity to communicate adequately—with their own crews and with other company outage crews who have come to provide mutual aid. Where interoperable communications are impossible among EPSPs responding to a major outage, visiting crews generally will use their own internal radios under Special Temporary Authority from the Federal Communications Commission.

With regard to data communications for operating mission-critical functions such as SCADA, generation facilities, bulk power transmission and distribution networks, the range of reliance on internal communications networks varies greatly. Although some EPSPs rely on internal private networks for all mission-critical data communication functions, others rely heavily on commercial telecommunications networks for elements of their internal data communications networks. In addition, if primary and backup private internal or commercially leased data networks are lost for mission-critical functions, the EPSP can typically dispatch key response personnel with voice communication devices (e.g., radio) to critical electric power assets to operate in manual mode at some minimal level. Other key participants, such as regional transmission organizations, independent system operators, and NERC Regional Reliability Center coordinators, rely heavily on the use of a variety of telecommunications mechanisms such as commercial telecommunications services and the Internet.

Many EPSPs' private internal communications networks are protected from power outages through long-term backup generation facilities. These facilities are often designed to provide power for private communications systems for up to two weeks without refueling but can operate indefinitely if the fuel supply is not interrupted. These backup capabilities, which are not economical or feasible for commercial networks, are required by utilities to ensure reliable communications in emergencies.

3.1.2 Telecommunications

Telecommunication service providers' internal priority restoration plans are similar to those of the electric power industry, but prioritization of restoration activity is driven specifically by those customers, emergency services, life support, and critical infrastructures that have joined the NCS' Telecommunications Service Priority (TSP) program. The NCS manages this Federal program, which enables telecommunications users to obtain priority treatment, including provisioning of new circuits and restoration of existing circuits, from service providers to meet NS/EP telecommunications requirements. Typically, entities eligible for TSP status are responsible for providing services for the following purposes, which are grouped in the following tiers for restoration assignment: (1) linking national security leadership; (2) maintaining the national security posture and U.S. population attack warning systems; (3) preserving public health, safety, and law and order; (4) upholding public welfare and the national economic posture; and (5) providing emergency support.⁴ Electric power service ranks in priority below the third tier. EPSPs have not significantly participated in the TSP program, having made very few applications for priority restoration.

Telecommunications service providers depend highly on electric power for continued delivery of service, particularly as the electronics equipment in the network has become less centralized and more distributed. For this reason, telecommunications service providers institutionalized the use of battery backup and mobile emergency generators as sources of short-term power during emergency situations. Electric power backup for the various elements (sites) supporting the infrastructure varies greatly from one site, or type of site, to another. Some sites have extensive emergency backup capabilities, and thus can support normal service for extended periods. Other sites have minimal emergency backup capabilities that might provide only a limited level of service, ranging from several hours to one day. Key assets such as central offices, access tandems, telco hotels, collocation facilities, and mobile switching centers typically have battery backup that is augmented by emergency generators. Such large sites can typically operate on backup power indefinitely if the fuel supply is not interrupted. Less centralized

telecommunications assets, such as remote terminals, radio towers, and optical regeneration huts, typically have battery backup for only a few hours. Portable generators must be deployed to these sites before the batteries discharge and service is interrupted. These generators are typically small and have fuel tanks that must be topped off frequently. Perimeter controls and curfews often pose impediments to keeping the generators functioning.

3.2 Impacts of Natural Disasters and Human Attacks on Telecommunications and Electric Power Service

In responding to the major outages between 2001 and 2005, the telecommunications and electric power sectors increasingly improved their coordination during the restoration process.

3.2.1 September 11, 2001

The events of September 11 revealed the vulnerabilities of the telecommunications and electric power sectors, as well as the dependency of other sectors on these two infrastructures. The aftermath of the attacks carried out on September 11 also highlighted the interdependencies between the two sectors during an emergency event as the sectors interacted to restore telecommunications and electric power service. A key finding by all sectors was that the terrorist attack in New York City,⁵ although site specific, spread its impact over a fairly large area. The financial markets experienced interruption of service worldwide, whereas the electric and telecommunications disruptions were relatively localized. In developing their emergency plans, many New York business enterprises had relied on being able to move their critical functions only a few blocks down the street to resume operations; but they found those plans were inadequate when activated.

On that day, the Nation experienced a disaster transcending anything any in recent history. The physical destruction resulting from falling debris and dust, the interruption of water supplies and transportation services, compounded by numerous other factors, aggravated the destructive impact on telecommunications, electric power, the financial services sector, and others. Temporary or backup generators could not continue operations in the extremely dusty and dirty air conditions caused by the fall of the World Trade Center towers,

and many temporary backup generators were not designed to operate continuously for several days. Also, replenishing fuel to these facilities became problematic when access to Lower Manhattan was restricted. The lessons learned from the aftermath of September 11 have caused many sector planners to reconsider the adequacy of their redundant systems and revisit their continuity of operations plans.

Additionally, after the terrorist attacks, the demand for cellular communications connectivity was unprecedented, at a time when many cellular infrastructure assets had been destroyed or had suffered from other consequences. This was a marked difference from past crises. In the first hours after the attacks, wireless communications continued to provide service, albeit greatly reduced, in the affected areas through the surviving assets until mobile cell towers were deployed and the range of unaffected towers was extended to augment the service. The need for functional cell towers was a top priority; hence, the deployment of mobile cell towers, including mobile backup power, was paramount to meeting First Responder needs.

The resiliency of the local electric power and telecommunications infrastructure was clearly demonstrated in the disaster response. By September 19, commercial power was restored to all networks in Lower Manhattan. Likewise, communications capabilities were sufficiently restored so that the financial markets could be reopened on the Monday following the attacks.

3.2.2 2003 Blackout

On Thursday, August 14, 2003, cascading effects caused the largest electric power blackout in North American history, leaving 50 million people without power in eight States and parts of Canada. The cities of New York, Detroit, Cleveland, Toronto, and Ottawa were affected by this power outage, which in some areas lasted for four days, although the major portion of affected customers had power restored after 30 hours. Estimates of the total impact on the U.S. economy caused by the blackout range from \$4 billion to \$10 billion.⁶ Although an extremely significant event in terms of economic impact, the blackout revealed

limited interdependency issues between the sectors because of its relatively short duration. Nonetheless, the blackout further clarified the need for effective communication between the sectors and the need to share information on priority restoration efforts. The two sector ISACs proved effective in communicating between sectors during the crisis. Had the blackout situation lasted longer, more interdependencies might have been revealed; and the inter-sector coordination process would have become even more critical.

3.2.3 Hurricane Activity

Hurricanes provide valuable examples of the most frequent type of natural disaster, usually causing extensive physical damage to the telecommunications wireline and wireless networks, and to the electric transmission and distribution grids. Commercial and private communications might be equally affected by these storms. Depending on the circumstances surrounding each storm, the impact on the elements sustaining each infrastructure varies in intensity and duration.

In some instances, commercial communications might survive hurricane damage to a much greater degree than electric power service; but the opposite can be true. Likewise, utilities' private internal networks might survive the hurricane and continue to operate or be damaged and quickly restored, yet commercial communications might remain largely unreliable, due either to infrastructure damage or excessive demand.

The hurricanes of 2004 and 2005, and the resulting recovery efforts have yielded invaluable lessons learned that can be applied to understanding the interdependencies between the telecommunications and electric power sectors.⁷ First, a general need exists for additional coordination and collaboration between the sectors at the Federal, State, regional, and local levels, both in advance of a natural disaster and during the emergency restoration period. It is particularly important for the telecommunications and electric power sectors to collaborate and coordinate on frontline operations maintenance and repair teams. Advance coordination can help to target key regional and local assets in both sectors for priority restoration and increase the likelihood of successful

communication during a crisis. Currently, the level of coordination and collaboration between the sectors varies greatly from one region to another. The primary driver for this disparity is the natural disaster threat profile for various regions. Those regions prone to hurricanes, ice storms, and earthquakes are likely to be far more engaged in preplanning than those in less disaster-prone regions. Many other factors influence the level of collaboration: the robustness of a local telecommunications provider's emergency backup power system; dependence of the electric power sector on commercial telecommunications networks for emergency repair communication; the degree to which a local electric power control area depends on commercial telecommunications for its SCADA and emergency management system; whether an effective emergency management authority (EMA) exists in the region; and senior management's level of commitment to disaster planning.

A second lesson learned is that restoration and provision of telecommunication services and electric power are critical for First Responders and restoration and recovery of all other critical infrastructures. Restoration of telecommunications and electric power must be given the highest priority after saving of life, and must include priority access to fuel, security, site access, and other logistical support such as staging areas, and food and berthing for response personnel. Key response personnel of critical infrastructure owners and operators in both sectors must be involved in planning for, and responding to, potential emergency events. If a new designation, such as Emergency Responders, and similar to First Responders, were established to facilitate priority restoration of telecommunications and electric power, it would allow the Emergency Responder designation to be applied to telecommunications and electric power professionals. They could then be included in the Federal, State, regional, and local emergency planning processes; actively participate in EOCs during emergency events; and gain access to restricted areas in a timely and secure fashion to restore their critical assets.

Third, as recommended in the NSTAC's *Trusted Access Task Force Report*, a uniform credentialing system would facilitate access for Emergency Responders and First Responders.

Fourth, First and Emergency Responders must be able to communicate effectively. Employing at least one of the following enhancements would greatly facilitate communications:

- ▶ Making existing systems interoperable across jurisdictions.
- ▶ Bringing in deployable solutions to overlay upon existing systems.
- ▶ Designating a communications and coordination hub to act as the interconnection point for disparate and non-interoperable systems. Also ensuring local forces use communications equipment that can operate on multiple frequencies and formats

Finally, the processes for fuel supply replenishment for electric power generators at critical telecommunications assets must be integrated into Emergency Responder planning; and fuel deliveries must be considered a priority during an emergency.

3.3 Emergency Communications During Outage Situations

It should be noted that any solution for the timely restoration of communications capabilities following a disaster depends first on the restoration of power. However, the safety and rapidity of restoration depend on the extensive internal private voice communication networks used by both sectors' personnel, as well as the multitude of sister utility and service personnel who come to assist in the restoration efforts.

Analysis of the interdependencies between commercial telecommunications and electric power sectors might investigate ways to improve emergency communications between the sectors during outage situations. Interoperability and integration of each sector's internal private voice communication networks for restoration could provide a construct for more

reliable communications and more rapid restoration of critical infrastructure. Leveraging the shared use of critical infrastructure networks, including those of First Responders, should also be considered.

3.4 Implications of Changing Telecommunications Network Design⁸

Developing trends in network design also raise questions about the resulting interdependencies between the telecommunications and electric power sectors. With the growth of the next generation network (NGN), the attendant growth in wireless and mobile technologies, and the dispersion of network elements, the telecommunications sector can no longer rely on 48 volt batteries in central offices to provide power to the end of the network. Instead, telecommunications infrastructure and its users will increasingly rely on commercial electric service to meet their power needs. In this environment, the telecommunications and electric power sectors will have to work closely together to ensure NS/EP services are available to respond to terrorist incidents, natural disasters, or any other event prompting activation of specialized services. The dynamic change in telecommunications network architectures and the consequential effects on the interdependency between the telecommunications and electric power sectors as a strategic issue will be addressed in a subsequent report.

4 Information Sharing and Liability

4.1 Current Information Sharing Environment

Currently, formal information sharing between the telecommunications and electric power sectors is conducted primarily through the sectors' two ISACs.

In response to President Clinton's Presidential Decision Directive 63 (PDD-63), the National Coordinating Center (NCC) was designated as the Telecommunications ISAC on March 1, 2000.⁹ As such, it aims to "facilitate voluntary collaboration and information sharing among industry and Government ISAC members in support of Executive Order 12472 and the critical infrastructure protection goals of PDD-63. The Telecommunications ISAC gathers and

analyzes all-hazards information on vulnerabilities, threats, intrusions, and anomalies in order to avert or mitigate impact upon the telecommunications infrastructure.”¹⁰

The Electricity Sector ISAC, founded in October 2000 by NERC, aims to ensure that “the bulk electric system (physical and cyber) in North America is reliable, adequate, and secure.”¹¹ This ISAC’s responsibility is to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electric sector participants in taking protective actions. The Electricity Sector ISAC also serves the electric power sector by facilitating communications among electric sector participants, the Federal Government, and other organizations responsible for critical infrastructures.

Because the ISACs were established to share information critical to their respective sectors, they are able to exchange data to analyze, make decisions, and take action based on shared information. If an emergency arises, information sharing between the two ISACs is quickly facilitated through a conference call bridge to focus coordination activities at the regional and local levels.

The ISACs further serve as facilitators, providing a critical link for communication with the Government. The Government leverages the ISACs to communicate with the telecommunications and electric power sectors, and ultimately uses this information to help form its issuances of threat levels and analysis.

The overall relationship between the sectors with regard to information sharing among the ISACs is further detailed in Section 4.3, Liability Issues.

4.2 Levels of Information Sharing

To implement effective prevention and response measures, both sectors need to be aware of the various levels of Government with which they should coordinate. To the extent possible, all levels (local, regional, State, Federal) should be represented in the information sharing process. To sustain a managed process, industry and Government components need

to continue working through the same process. Being cognizant of potential obstacles, telecommunications and electric sector professionals should continue to strive for information sharing at every level.

Information sharing among telecommunications, electric power, and Government professionals is a key issue at all levels; but reviews of natural and human-made disaster situations underscore that it is especially pivotal among local officials and Emergency Responders on the ground. Information sharing models should be in place before crises occur to maximize the effectiveness of Emergency Responders.

The importance of structured communication models at the local and regional levels is illustrated in the Washington, DC, metropolitan area, where the surrounding counties (Fairfax, VA; Montgomery, MD; and Prince Georges, MD) and the District of Columbia have established EMAs. EMAs coordinate preparedness, response, and recovery efforts for significant emergency events at the local level. EMAs act as a focal point for emergency planning, training, and the exercise of programs, and help to promote coordination and collaboration among participants in advance of an emergency event.

During significant emergency events, each EMA establishes an EOC, which coordinates all disaster recovery activities in its region. The EOC coordinates the First Responders (and could also coordinate Emergency Responders if they were established on a national level); county agencies; other key infrastructures (e.g., water, sewer, transportation); and Federal, State, and regional Government entities (such as other EMAs). Representatives from the telecommunications and electric power sectors with decision making authority and access to their key data and information technology systems (such as outage management systems) routinely participate in EOC activities.

In the case of Fairfax County, during non-emergency events, there is generally little need for coordination between the two sectors. Each entity can automatically alert the other of compromised assets, such as lines or cell towers down. Each entity is knowledgeable of its operations/emergency repair counterpart, including

emergency contact information, but in cases of normal outages, each entity rarely needs to coordinate with one of the others. However, in the case of a significant emergency, considerable extensive coordination ensues among telecommunications and electric power service providers through the EOC.

The EMA/EOC system illustrates the importance of highly coordinated information sharing on the local and regional levels, facilitating operations in crisis situations through prearranged systems that bring key people and processes together. This model is an advanced example for a metropolitan region, although it may have unique characteristics because of its proximity to, and interaction with, the Federal Government. Other areas of the country and their models need to be explored and considered.

Although the EMA/EOC example serves as an illustrative model for the importance of information sharing at the local and regional levels, such collaboration is not common in most areas of the country. Much more work needs to be done to ensure that Emergency Responders throughout the United States have access to effective information sharing systems at the local level.

4.3 Liability Issues

Information sharing as discussed above may lead to liability concerns, specifically with regard to the informal sharing of information that occurs between the telecommunications and electric power professionals who are on the ground in local crisis situations.

Emergency situations require fast, effective information sharing between the sectors to restore communications and power services to the affected areas as quickly and efficiently as possible. Although this principle is widely supported, liabilities might arise as a result of this increased flow of data. When a telecommunications company shares information with an electric power company, or vice versa, each party becomes responsible for safeguarding and protecting the information that they receive from the other party. For practitioners in both sectors to work effectively, data on specific site locations, operations and leadership contacts, and other sensitive and proprietary information must be shared.

If this information is compromised, the responsible party will likely be held liable, necessitating careful transmission of, and guarded access to, the information being shared.

The potential for liability posed by information sharing is further complicated by the priorities of Emergency Responders, who must share the necessary information as quickly as possible to reach their end goal—power/service restoration. A conflict exists between the advantages of information sharing and the possibly negative consequences and potential liability arising from quickly shared, but ultimately incorrect, information.

As an additional complicating factor with respect to potential liability, U.S. anti-trust regulation might require that information shared between two parties be made available to all. For instance, if a utility company shares information to help one communication vendor plan for restoring power, it might be obliged to make that same information available to all communications vendors in the service area. Potential liabilities can also arise if there is a perception that one company is receiving preferential treatment over another.

Although it is clear that liability concerns among Emergency Responders still need to be addressed in much greater depth, the Telecommunications and Electricity Sector ISACs have a structure in place to help protect against potential liabilities while allowing for the free flow of information between the participants.

Information sharing among the Telecommunications ISAC membership is governed by the information provider, who instructs the ISAC Watch regarding what information may be released beyond the ISAC. In the case of the Telecommunications ISAC, each company's information is owned by that company; and each company controls the information that it shares, dictating what may or may not be released outside of the ISAC and facilitating shared trust among the members. This procedure allows information to be shared among the critical participants while protecting proprietary information and shielding the ISAC from potential liability issues.

The Electricity Sector ISAC has a structured process for communications with the electric power industry and Government agencies, and a developing structure among ISACs that is guided by the ISAC Council.¹² Conference calls with participants direct the information sharing structure to be used for a specific incident. For example, in the case of a hurricane, the ISAC has enough advanced warning to set up a conference call with the major industry participants and governing agencies, including the NCC. Calls are held daily (or as needed) as the crisis unfolds to update participants on restoration/provision status from an electric power perspective, with the understanding that if information is needed by another sector, including telecommunications, the ISAC will reach out further and provide the necessary information. The communication is designed so that the sectors can keep each other informed as to any specific needs. Further, the Electricity Sector ISAC has signed an MOU with the ISAC Council. The formality of this document is still in its infancy, but it is designed to protect the proprietary information that exists in the data shared by the Electricity Sector ISAC. A reporting schema is also in place with DOE and Department of Homeland Security. Both of the aforementioned protective policies should be further enhanced by the Homeland Security Information Network, which will play a more formal role with regard to legal restrictions and simultaneously centralize the reporting process when it takes effect.

Further potential liability areas to be examined include issues that result from insufficient coordination between the telecommunications and electric power sectors during an outage; interconnection of the Canadian and U.S. power grids and its resulting impact on addressing priority categories and regulatory issues; and the increasing dependency of telecommunications services on power.¹³

5 Conclusions

On the basis of the analysis provided in this report, several conclusions emerge regarding the interdependencies between telecommunications and electric power.

Section 2

- ▶ Interdependencies are a matter of increasing importance to industry and Government. Previous work focused on dependency, but much work remains to be done with regard to understanding the issues related to interdependency.

Section 3

- ▶ Priority restoration of telecommunications and electric power is critical for First Responders, restoration of other critical infrastructures, and other response and recovery activities.
- ▶ The most useful element of a relationship between the two sectors for restoration activities during an emergency is the open dialogue between the points of contact at the lowest possible level (e.g., entity to entity).
- ▶ Due to the critical nature of telecommunications and electric power service providers, their key response personnel should be designated as Emergency Responders. This designation would allow them to be involved in the Federal, State, regional, and local emergency planning processes; actively participate in EOCs during emergency events; and be given priority access to restricted areas in a timely and secure fashion to restore their critical assets.
- ▶ As recommended by the NSTAC's Trusted Access Task Force, a nationwide credentialing program would facilitate access to a site.
- ▶ The fuel supply replenishment process for electric power generators at critical telecommunications and EPSPs' internal communications network assets is imperative.
- ▶ Emergency response communication between telecommunications and electric power infrastructures would be improved if at the lower levels, the EOCs had the ability to interoperate without depending on public commercial telecommunications services.

Section 4

- ▶ Effective information sharing models at the level of Emergency Responders are not prevalent.
- ▶ Collaboration between the two sectors is most important at the regional and local levels to ensure the rapid recovery of both sectors.
- ▶ The Telecommunications and Electricity Sector ISACs are logical candidates to coordinate information sharing at the broadest and highest levels between the two sectors, ideally serving as a resource for each sector to use when communications are difficult at the local level and guidance/advice is needed on how to proceed.
- ▶ Liability issues have not been considered at the lowest, local level of communications.

6 Recommendations

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies to:

- ▶ Define and establish the term Emergency Responder within the *National Response Plan* and other appropriate plans, guidance, directives, and statutes, including other local, State and Federal Government emergency plans.
- ▶ Ensure key response personnel of critical infrastructure owners and operators in the telecommunications and electric power sectors be designated as Emergency Responders.
- ▶ Include fuel supply, security, site access, and other required logistical support to critical telecommunications and electric power infrastructures as part of the Emergency Responder planning process to ensure priority restoration to critical telecommunications and electric power.

- ▶ Foster and promote effective emergency coordination structures to ensure reliable and robust communication between the two sectors and local, regional, State, and Federal Governments.
 - Review examples of proven priority restoration models at the State and regional levels. Encourage States and metropolitan regions without effective models to improve and update their existing frameworks.
 - Encourage effective information sharing models at the local/regional Emergency Responder level, both in advance of a natural disaster and during the emergency restoration period. When developing these models, liability issues should be considered.

Footnotes

- 1 Although the issues of robustness and reliability are important, the TEPITF will not specifically address them.
- 2 For more information, please refer to Appendix A.
- 3 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report, 2004.
- 4 NCS website: TSP Categories. <http://www.ncs.gov/tsp/tspcategories.html>
- 5 While an event of national significance, the attacks on the Pentagon did not reveal significant interdependency issues.
- 6 U.S. Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada, April 2004.
- 7 U.S. Senate Committee on Commerce, Science and Transportation Hearing: "Communications in a Disaster," September 22, 2004.
- 8 The NSTAC's NGN Task Force is studying the NGN and is examining how incident management issues will differ in a full NGN environment. The TEPITF will review the NGN Task Force reports to gain additional insight.

- 9** NCS website. <http://www.ncs.gov/ncc/>
- 10** See the National Infrastructure Protection Center Report: Highlights, January 15, 2002.
- 11** See the ISAC Council White Paper: Reach of Major ISACs. January 31, 2004.
- 12** The mission of the ISAC Council is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with Government. <http://www.isaccouncil.org/about/>
- 13** The TEPITF plans to request analysis on this issue from the Legislative and Regulatory Task Force.
- 14** 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: (1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; 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.
- 15** Telcordia GR-1089-CORE.
- 16** ANSI T1.320.

Appendix A

Electro-Magnetic Pulse

Electro-Magnetic Pulse

The NSTAC follows a risk management approach to survivability that can be partly attributed to the pioneering work of the Electro-Magnetic Pulse Survivability Committee. The recommendations the committee made to the President on December 12, 1984, included the following:

- Designate an appropriate Federal agency to serve as an industry point of contact for EMP mitigation efforts and information distribution.
- Support industry through its standards organizations in the development of electromagnetic standards that take the EMP environment into account.
- Undertake a program to improve the EMP durability of the Nation's commercial electrical power systems.

In its *Final Report on EMP*, the NSTAC found that “consistent with its cost constraints, industry should incorporate low-cost EMP mitigation practices into new facilities and, as appropriate, into upgraded programs. For those areas where a carrier/supplier recognizes that a significant improvement in EMP resistance and surveillance could be achieved, but at a cost beyond the carrier/supplier's own cost constraints, the carrier/supplier should identify such options to the Government for evaluation and possible funding.” On October 9, 1985, the NSTAC approved the EMP Final Task Force Report and forwarded a recommendation to the President, calling for a joint industry and Government program to reduce the costs of existing techniques for mitigating high-altitude EMP-induced transients and to develop new techniques for limiting transient effects. As a result, the NCS¹⁴ and industry, working with the Alliance for Industry Solutions developed a set of American National Standards Institute (ANSI) standards and Generic Requirements¹⁵ to address EMP.¹⁶

Further, based on the results of the commission-sponsored testing, an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian

telecommunications systems in the region exposed to EMP. The remaining operational networks would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services. Key Government and civilian personnel need priority access to use public network resources to coordinate and support local, regional, and national recovery efforts, especially during the interval of severe network congestion. To offset the temporary loss of electric power, telecommunications sites now employ a mix of batteries, mobile generators, and fixed-location generators. These typically have between four and 72 hours of backup power available, and thus depend on either the resumption of electrical utility power or fuel deliveries to function for longer periods of time. For some of the most critical infrastructure services, such as electric power, natural gas, and financial services, assured communications are necessary, but are not necessarily sufficient, to the survival of that service during the initial time intervals after an EMP attack. Therefore, a systematic approach to protecting or restoring key communications systems is required.

Appendix B

Task Force Members,
Other Participants, and
Government Personnel

Task Force Members

Nortel

Dr. John S. Edwards, Chair

AT&T, Inc.

Ms. Rosemary Leffler

Bank of America Corporation

Mr. Roger Callahan

BellSouth Corporation

Mr. David Barron

Computer Sciences Corporation

Mr. Guy Copeland

Lucent Technologies (Bell Labs)

Mr. Richard Krock

Lucent Technologies

Mr. Karl Rauscher

Microsoft Corporation

Mr. Philip Reitingger

Qwest Communications

International, Inc.

Mr. Jon Lofstedt

Raytheon Company

Mr. Frank Newell

Science Applications International Corporation

Mr. Henry Kluepfel

Sprint Nextel Corporation

Mr. William Hitchcock

United States Telecom Association

Mr. David Kanupke

Verizon Communications, Inc.

Mr. James Bean

Other Participants

AT&T, Inc.

Mr. Harry Underhill

American Public Power Association

Mr. Michael Hyland

BellSouth Corporation

Mr. Shawn Cochran

Cingular Wireless LLC

Mr. Kent Bowen

Edison Electric Institute

Mr. Larry Brown

Electric Power Research Institute

Mr. Thomas Kropp

Environmental Energy, Inc.

Mr. Mark Razeghi

George Washington University

Dr. Jack Oslund

Independent Electricity System Operator

Mr. Stuart Brindley

Industry Canada

Mr. John Kluver

Mr. Robert Laforest

Mr. Robert Leafloor

Institute for Defense Analysis

Mr. Gordy Boezer

Microsoft Corporation

Ms. Lynn Terwoerds

MITRE

Dr. Edward Jacques

National Rural Electric Cooperative Association

Mr. Barry Lawson

New York Independent System Operator

Ms. Bonnie Bushnell

North American Electric Reliability Council

Mr. Stanley Johnson

Mr. Louis Leffler

PEPCO, Holding Inc.

Mr. Richard Kafka

Public Safety and Emergency Preparedness Canada

Ms. Patricia Davies

Ms. Joan Edgan

Public Service Enterprise Group

Ms. Frances McCormick

Qwest Communications

International, Inc.

Mr. Thomas Snee

Southern Company

Mr. Rusty Williams

Sprint Nextel Corporation

Ms. Allison Growney

Mr. John Quigley

Texas Utilities

Mr. William Muston

United States Telecom Association

Mr. Murray Liebman

United Telecom Council

Ms. Jill Lyon

Ms. Prudence Parks

Verizon Communications, Inc.

Mr. Roger Higgins

Mr. Charles Romano

Government Personnel

Department of Energy

Mr. John Greenhill

Mr. Henry Kenchington

Department of Homeland Security

Ms. Michele Bruich

Mr. David Delaney

Lt. Col. Cheryl Edwards

Mr. Gilberto Frederick

Ms. Carolyn King

Mr. Gabriel Martinez

Mr. Chatry Perry

Lt. Col. Joanne Sechrest

Capt. Thomas Wetherald

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE



**NSTAC Report to the President on
Next Generation Networks**

March 28, 2006

Table of Contents

Executive Summary	ES-i
1 Background and Charge	1
2 The NGN	2
2.1 Introduction	2
2.2 NGN Description	3
2.2.1 Architectural and Technical	3
2.2.1.1 Packet-Based	3
2.2.1.2 Open, Layered Architecture	3
2.2.1.3 More Powerful and Varied User Devices Distributing Network Intelligence	5
2.2.2 Capabilities	5
2.2.2.1 Multi-Modal and Converged Services (Voice, Video, Data) and Data Transparency	5
2.2.2.2 Information Presented Real-Time, Time-Shifted, and Transformed	5
2.2.2.3 Greater Mobility and Ubiquity	5
2.3 Security on the NGN	5
3 NS/EP Communications and the NGN	6
4 NS/EP Functional Requirements in an NGN Environment	7
4.1 “Legacy” Functional Requirements	7
4.2 Key “New” Functional Requirements	8
5 Identity Management	10
5.1 Introduction	10
5.2 Identity Management Criticality	11
5.3 Identity Management Mechanisms, Standards, and Taxonomy	11
5.4 Resiliency of Identity Management	12
5.5 Anonymity and Identification	12
5.6 Federation, Interoperability, and Credentials	12
5.7 Commercial Technologies and Deployment	13
5.8 Trust/Social Concerns	13
6 Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services	13
6.1 Unique NGN End-to-End Service Issues	14
6.2 Common Operational Criteria	14
6.3 Local Access and Priority	15
6.4 Scope and Relative Levels of Priority	16
6.5 Internet Protocol version 6	16
6.6 Peer-to-Peer Technology	17
6.7 Meshed Network Environments and IP Security	17
7 Research and Development	18
8 Technology Lifecycle Assurance and Trusted Technology	18

9	Resilient Alternate Communications	19
10	Agreements, Standards, Policy, and Regulations	21
11	Incident Management on the NGN	23
	11.1 Introduction	23
	11.2 Unique NGN Incident Response Issues	24
	11.3 Industry Involvement Throughout the Planning Process	24
	11.4 Joint Coordination Center	25
	11.5 Exchange Program	25
	11.6 Federal Incident Management Training Academy	25
	11.7 Exercise Program	26
	11.8 Increased Research and Development Funding	26
12	International Policy	26
13	First Responders	27
14	Conclusion	27

Executive Summary

The convergence of wireless, wireline, and Internet Protocol (IP) networks into global Next Generation Networks (NGN) is changing how the Federal Government will meet its needs for national security and emergency preparedness (NS/EP) communications today and in the future. The NGN will offer significant improvements for NS/EP communications as bandwidth and software continue to improve, but the transition to the NGN presents challenges for ensuring the security and availability of NS/EP communications.

Although the complete network evolution is expected to take many years, the process is well underway. It has become clear that the scale, scope and character of the NGN will fundamentally change the way NS/EP communications are planned for, prioritized, and ultimately delivered. It is critical that this issue be addressed.

At the President's National Security Telecommunications Advisory Committee (NSTAC) XXVII Meeting held on May 19, 2004, the NSTAC Principals requested that a task force be created to address how the Government can meet NS/EP requirements and address emerging threats on the NGN. The Next Generation Networks Task Force (NGNTF) was created to:

- 1) Agree upon a high-level description of the NGN's expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely;
- 2) Identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and accountability among network participants and network layers will work; and
- 3) Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements.

The NGNTF worked extensively on these taskings, sponsoring two formal Subject Matter Experts (SME) Meetings and creating working groups to address each issue thoroughly with deep SME involvement. Ultimately, the NGNTF agreed upon nine recommendations, the implementation of which would support the ability of the NGN to meet NS/EP functional requirements while also providing greater capabilities to NS/EP users.

The NSTAC recommends that the President:

- **Identity Management:** Direct the Office of Management and Budget (OMB), the Department of Commerce (DOC), and Department of Homeland Security (DHS) to work with the private sector in partnership to build a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity "silos," allows federation between the Government and commercial domains, and supports use of Government-issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including for priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.
- **Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services:** Direct the Office of Science and Technology (OSTP), with support from the collective National Communication System agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor programs

that would foster NS/EP capabilities within the NGN, including initiatives concerning:

- A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user's NS/EP authorization and required class of service; and
 - NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into Internet Protocol (IP) version 6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IP Security for authentication and confidentiality.
- ▶ **Research and Development (R&D):** In support of the prior recommendation, direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, the National Institute of Standards and Technology (NIST), and the Department of Defense (DOD) to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/ information technology and service providers.
- ▶ **Technology Lifecycle Assurance and Trusted Technology:** Direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of: (1) technology lifecycle assurance mechanisms and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.
- ▶ **Resilient Alternate Communications:** Direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure.
- ▶ **Agreements, Standards, Policy, and Regulations:** Direct DHS, the Department of State, and DOC (including NIST and the National Telecommunications and Information Administration) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally distributed NGN environment.
- ▶ **Incident Management on the NGN:** Direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

- **International Policy:** Direct departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-U.S. companies in NS/EP incident response in the United States; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.

- **First Responders:** Direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

1 Background and Charge

Dramatically changing business models of traditional telecommunications carriers, along with new technologies, are driving fundamental changes in global communications networks. For several years, global communications networks have been in transition. Customer demands and business imperatives catalyzed a “convergence” of traditional circuit-switched networks interoperating with broadband packet-based Internet Protocol (IP) networks. For almost a decade, this convergence has been increasing and evolving toward “Next Generation Networks” (NGN). This convergence of wireless, wireline, and IP networks into the global NGN will alter the way governments and critical infrastructures meet their needs for national security and emergency preparedness (NS/EP) communications. In many cases, it has already effected change. Although the complete evolution to the NGN is expected to take many years, the process is well under way. Many networks and providers have already developed the capability to carry voice, video, text, and data transparently to many types of end-user devices, a key characteristic of the NGN. Mobile phones able to access an array of Web-based services are only one example of this enhanced ability.

The scale, scope, and character of the NGN will fundamentally change the way NS/EP communications are planned for, prioritized, and ultimately delivered. NGN networks, which are largely, packet-switched networks, differ greatly from legacy circuit-switched networks. For example, packet-switched environments place control capabilities at the network “edge” and rely heavily on intelligent devices to execute key

functions. In this new environment, confusion exists among end users concerning how their responsibilities will change. At the same time, NS/EP communications and critical business communications will be subject to an increased number of cyber threats based on inherent vulnerabilities and interdependencies known or expected to exist in the NGN. With these changes, one of the major issues facing network operators, infrastructure custodians, and NS/EP users is how best to meet NS/EP user requirements on the NGN.

The transition to the NGN presents challenges for ensuring the security and availability of NS/EP communications. Some vulnerabilities that existed in legacy networks present more of a challenge on the NGN. For example, the enhanced interconnectedness of the NGN can be used by threats to provide rapid and far-reaching propagation of malicious payload (attacks). Another vulnerability is the emulation of network control messages. Unlike legacy networks, which used separate paths to separate network control messages from normal network payload, NGN architectures have network control messages co-existing with normal payload traffic, providing more open access to threats to interfere with these messages. These and other vulnerabilities create complex risk scenarios for NS/EP communications in an NGN environment, which depends on its own components as well as other infrastructures, as Figure 1 illustrates. A further challenge is the global nature of the NGN and, thus, methods for managing incidents of national significance may require international cooperation. These concerns must be addressed.

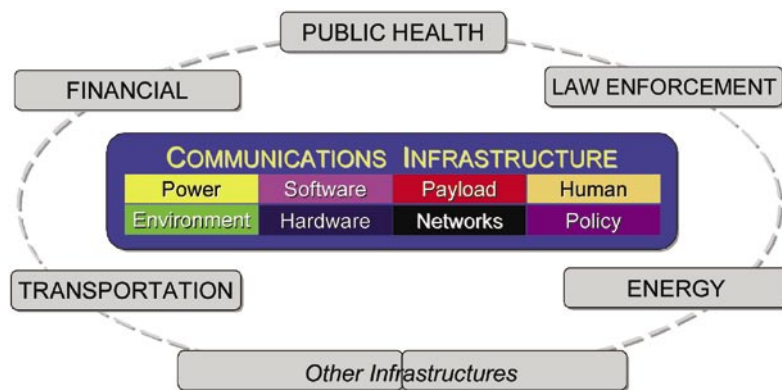


Figure 1 Communications Infrastructure Components and Dependencies¹

On the other hand, the NGN will offer significant improvements for NS/EP communications as bandwidth and software continue to improve. New communications capabilities, including greater access to data and new services, will support NS/EP functions in critical ways, enabling first responders, for example, to obtain real-time access to voice, data, and video necessary for the most effective completion of their jobs. The NGN will also naturally increase network robustness and resiliency by the nature of its mesh architecture, offering many possible paths for service and redundancy of equipment and servers. In short, the NGN can provide new capabilities and greater resiliency; to achieve these benefits, and to speed and enhance the transition to NGN, solutions must be found that address NS/EP functional requirements, especially for security and availability. Doing so requires forward-looking action by industry and Government.

Principals of the President's National Security Telecommunications Advisory Committee (NSTAC) agreed at the NSTAC XXVII Meeting held on May 19, 2004, that a task force should be created to engage subject matter experts (SME) in an examination of NS/EP requirements and emerging threats on the NGN. Accordingly, the Next Generation Networks Task Force (NGNTF) was created to:

- ▶ Agree upon a high-level description of the NGN's expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely;
 - Identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and accountability among network participants and network layers will work; and
 - Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements.

It was also agreed that the task force should explore international issues, both in terms of NS/EP functions that must be provisioned internationally, and international threats to the NGN.

The NSTAC previously examined network convergence issues via its Convergence Task Force (CTF) and Network Security Vulnerability Assessments Task Force (NS/VATF). The CTF presidential report (June 2001) analyzed the potential security and reliability vulnerabilities of converged networks. The NS/VATF report (March 2002) addressed public network policy and technical issues related to network disruptions, the security and vulnerability of the converged network control space, and needed countermeasures. Issues presented by convergence and cyber security also arose during the Financial Services Task Force examination of network resiliency to physical disruptions.

2 The NGN

2.1 Introduction

Until recently, communications networks each delivered a single type of service. Telephone networks delivered telephone service, cable television networks delivered television service, and so forth. Now public wireless networks, including both mobile telephone and wireless data networks, public fixed networks, including the public switched telecommunications network (PSTN) and other voice and data broadband networks, and private customer premises networks, including broadband user networks, are converging into the emerging global NGN, which provides a range of services.

As single-function networks disappear, open and dynamic networks are replacing them. These new networks offer greater functionality and processing capabilities and, through associated changes in the underlying transport networks and their architecture, will bring a radical change in the array and availability of services provided to end users. On the NGN, user-centric services will no longer be associated with the type of network access or transport, but rather

with the user need that is satisfied regardless of user terminal, access type, transport mechanism, or data type.² An idealized NGN will enable end users to get the information content they want, in any media/format, over any facilities, anytime, anywhere, under any condition, and in any volume.³

The NGN has the ability to significantly improve how the Government and critical infrastructures use and deliver NS/EP⁴ communications. However, the promise of enhanced NGN-based services for NS/EP users cannot be realized without significant industry and Government action. As the NGN evolves, parts of the existing networks will continue to be replaced or upgraded to the corresponding NGN components. That said, existing “legacy” networks and gateways to the NGN will exist for the foreseeable future; therefore, NGN implementations will need to interoperate⁵ with and allow for a migration path from existing networks and services.

2.2 NGN Description

The NGN will logically consist of applications that deliver services, the services provided to users, and the underlying transport networks. See Appendix C. The NGN itself is a capability that will enable many services and applications. Some services will be provided by the network and some will be external to it, but depend upon it. NGN user-centric services will be delivered over various networks, some of which, like private customer premises networks and mesh networks, lie outside the wide scope of the public network.

However, there is no single, universally accepted definition of the NGN. As used in this report, the term NGN is not intended to represent any single configuration or architecture. Instead, it represents the set of converged networks, illustrated by Figure 2, expected to arise that will transparently carry many types of data and communications and allow delivery of services and applications that are not coupled to the underlying network. However, it is possible to note several key NGN elements or attributes over which there is little, if any, dispute. These elements,

discussed in the following subsections, relate both to architectural and technical differences—how the NGN will be built and work—and the capabilities it will provide as a result.

2.2.1 Architectural and Technical

2.2.1.1 Packet-Based

In packet-based (or “packet-switched”)⁶ networks, digital information (whether video, voice, data, or a combination of these) is divided into pieces, called packets, that travel across the transport network to their destination following a set of rules implemented by the network and its protocols. This differs from how the circuit-based (or circuit-switched) PSTN works.⁷ In the circuit-based phone network, each communication receives a dedicated amount of network resources when a phone call is first set up, creating a “virtual circuit.”

2.2.1.2 Open, Layered Architecture

The NGN is being designed with an open, layered architecture, which offers multiple services virtually independent of transport.⁸ The NGN will also provide multiple transport options for a single service or communication.⁹ This layered architecture provides open and standardized¹⁰ interfaces between layers, providing layer independence. Layering, therefore, permits rapid changes or improvements to one layer of the network without having to reconstruct other layers,¹¹ enabling a more flexible and vibrant architecture for new services.

There are several models for conceptualizing the various layers of the NGN. Telecommunications providers view the NGN as having three fundamental layers: (1) application; (2) service control; and (3) transport. An alternative model is the classic, logical Internet categorization of four simple layers: (1) “physical” connection layer; (2) interconnection or “network” layer provided by IP; (3) end-to-end “transport” layer; and (4) “application” layer, or, combining the second and third layers into a three-layer construct of physical connection, packet transport, and application.

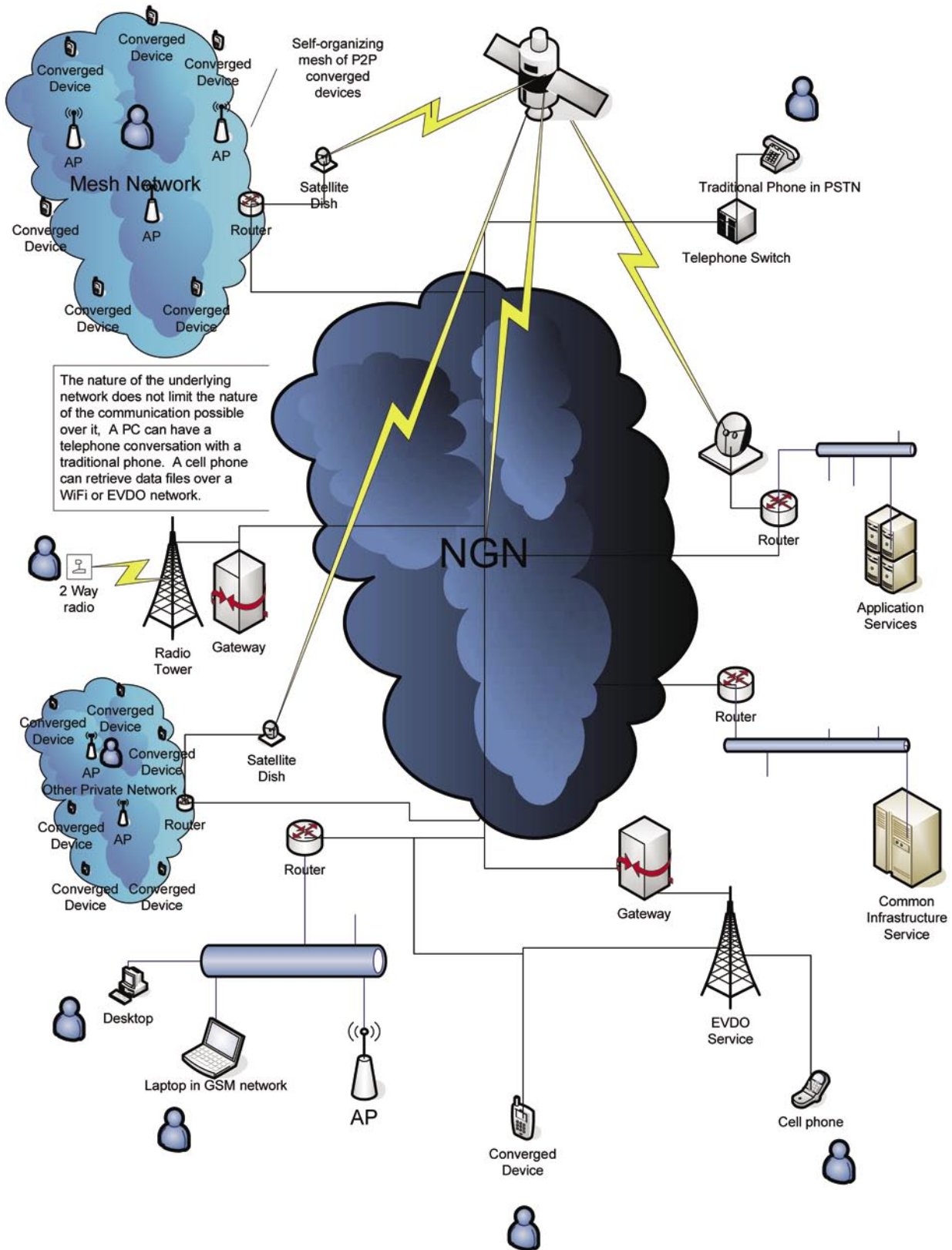


Figure 2 Network Convergence and the NGN

2.2.1.3 More Powerful and Varied User Devices Distributing Network Intelligence

The NGN's open nature permits users to connect powerful, multifunctional devices to it using NGN-provided protocols. Personal computers, personal digital assistants, powerful mobile phones running their own applications, etc., are already replacing current PSTN communications devices, the caricature of which is the old, black rotary phone. These more powerful devices, which can have control capabilities and distribute network intelligence, make applications and other software running on them of more relative importance than software on the PSTN. For example, end-to-end encryption will likely be far more common on the NGN given the ability of end-user devices to provide such encryption at either the application or end-to-end transport (e.g., via IP Security [IPsec], see Section 6.7) layers. Some devices will be able to communicate without the use of network-provided services by using peer-to-peer communications. End users can also use peer-to-peer applications and devices to improve robustness and remove single-points-of-weakness, and to provide a backup or supplement for primary communications technology.

2.2.2 Capabilities

2.2.2.1 Multi-Modal and Converged Services (Voice, Video, Data) and Data Transparency

NGN services will allow users (human and machines) to communicate with each other using different modes of communication: voice, text, image, and video. Whereas traditional networks have been focused on uni-modal services, such as voice services, the NGN will provide a multi-service architecture intended to support multimodal communication environments on top of a generic IP transport. In these environments, information can be communicated through various terminal devices, network access technologies, and underlying infrastructures.

Moreover, data transparency in an NGN means that the data content is not permanently altered in the transport network itself.

2.2.2.2 Information Presented Real-Time, Time-Shifted, and Transformed

Information traveling across the NGN may be presented in real-time (interactive voice) or time shifted (voice mail); and in its original format (analog speech) or transformed (file attachment). The information can be delivered by the network to a location, a device, a person, or broadcast to many, and may reflect personal preferences and mobility options.¹²

2.2.2.3 Greater Mobility and Ubiquity

The NGN is expected to approach near ubiquitous access, providing access and services anytime and anywhere where a wireless, wireline, or satellite signal can reach. The NGN will also improve mobility: open NGN interfaces will enable users to stop work at one location and resume at another. The NGN should also be able to provide continual connectivity while in motion.

2.3 Security on the NGN

Security mechanisms on open packet networks will differ from those of legacy telecommunications services in access control, control traffic protections, and trust accorded to other network elements. Legacy networks were circuit-oriented vertical networks, and so, much policy management was implied or “built into” the integrated service, and managed across all aspects of the network. Nevertheless, although security will need to be addressed differently on the NGN, it is likely that migration and convergence will create the opportunity for enhanced security features that will replace fundamental pre-NGN security capabilities. For instance, with NGN technologies, network architecture affords the opportunity to “build on” and improve policy management and service capabilities to aid emergencies.

Notably, on an open network such as the NGN, capabilities and responsibilities for providing security may reside at any level/layer or with any participant, making security an end-to-end challenge. The use of the NGN for NS/EP depends upon transport networks being highly available, reliable and tamper-free, even under stress. Applications must maintain high integrity, protect ownership rights of information, and protect against malicious attack.

3 NS/EP Communications and the NGN

The NGN can provide considerable benefits for NS/EP communications; however, to realize these benefits, and to speed and enhance the transition to NGN, we need solutions that address NS/EP functional requirements, especially for security and availability. This is an end-to-end problem; on a packet-based network such as the NGN, information will travel over a variety of networks and equipment, and a failure at any critical point, absent mitigation such as an alternative communications path, could impair communications. For the NGN to broadly meet essential NS/EP functional requirements in a consistent, continuous, and reliable end-to-end manner, a set of mechanisms must be promoted and adopted by those supplying network access, transport, and infrastructure services for this community, as well as NS/EP users.

In order to meet NS/EP requirements on the NGN, the NSTAC recommends that the President:

- ▶ **Identity Management.** Direct the Office of Management and Budget (OMB), the Department of Commerce (DOC), and Department of Homeland Security (DHS) to work with the private sector in partnership to build a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity “silos,” allows federation between the Government and commercial domains, and supports use of Government-issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including for priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.
- ▶ **Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services.** Direct the Office of Science and Technology (OSTP), with support

from the collective National Communication System (NCS) agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor programs that would foster NS/EP capabilities within the NGN, including initiatives concerning:

- A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user’s NS/EP authorization and required class of service; and
- NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into IPv6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IPSec for authentication and confidentiality.
- ▶ **Research and Development (R&D).** In support of the prior recommendation, direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, the National Institute of Standards and Technology (NIST), and the Department of Defense (DOD) to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/information technology and service providers.

- ▶ **Technology Lifecycle Assurance and Trusted Technology.** Direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of: (1) technology lifecycle assurance mechanisms and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.
- ▶ **Resilient Alternate Communications.** Direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure.
- ▶ **Agreements, Standards, Policy, and Regulations.** Direct DHS, the Department of State, and the Department of Commerce (including NIST and the National Telecommunications and Information Administration [NTIA]) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally distributed NGN environment.
- ▶ **Incident Management on the NGN.** Direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint

Coordination Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

- ▶ **International Policy.** Direct departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-U.S. companies in NS/EP incident response in the United States; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.
- ▶ **First Responders.** Direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

These recommendations are detailed in sections 5 through 13, respectively. Implementation of these recommendations would support the NGN's ability to meet NS/EP functional requirements, described below, while also providing greater capabilities to NS/EP users.

4 NS/EP Functional Requirements in an NGN Environment

4.1 "Legacy" Functional Requirements

The Federal Government has identified 14 functional requirements for NS/EP communications: enhanced priority treatment, secure networks, ubiquitous coverage, international connectivity, interoperable, scalable bandwidth, mobility, broadband service, reliability/availability, restorability,

survivability/endurability, non-traceability, affordability, and voice band service.¹³ Overall, these “legacy” requirements remain generally applicable to the NGN. However, the functional requirements themselves are insufficient to describe and define the needs of the Federal Government in an NGN environment. Concepts such as “secure networks” do not go far enough in describing what technologies, services, and applications will be needed to support the NS/EP mission in an NGN environment.

4.2 Key “New” Functional Requirements

The task force developed the following “new” functional requirements by examining five NS/EP scenarios (continuity of Government, critical Government networks, industry and critical infrastructure, public safety, and general users) as described in Appendix D. Not all functional requirements apply equally to every scenario. However, several requirements were common to all scenarios. These elements will be critical for NS/EP communications in an NGN environment:

- ▶ **Survivability.** Survivable networks can be made from imperfect components; alternatively, use of highly redundant elements does not guarantee a survivable network. To satisfy survivability requirements, numerous techniques could be combined, including but not limited to, hardware and software certifications, secure development processes for software that reduce vulnerabilities, diverse routing of local access and backbone transport, integration of wireless and wireline services, equipment redundancy, backup power technologies and restoration priorities, dynamic network restoration protocols, dedicated out-of-band management networks, and host and network-based intrusion detection. Highly survivable networks may also depend on technology that is not yet available that quickly and automatically restores end-to-end NS/EP services on the NGN.
- ▶ **Broad Platform Support and Interoperability.** This requirement entails supporting the widest possible variety of hardware platforms with their concomitant ranges of access speeds, transmission power, processor speed, software, and cost. Such requirements would span battery and solar-powered sensors in the short term to supercomputers and “smart dust” sensors that run custom micro-kernels on ambient energy absorbed from their environments in the very long-term.
- ▶ **Broad Application Support.** Broad support for a variety of applications that can be layered upon and be independent of the underlying transport would include both real-time and non-real-time communications, with the latter including store-and-forward, publish-and-subscribe, and archive models. For this requirement, multiple forms of audio, video, and data must be able to be sent using dedicated applications, as well as using umbrella applications such as web browsers that incorporate complex functionality. Familiar mechanisms such as dial, push-to-talk, fax, video conferencing, instant messaging, e-mail, and evolving peer-to-peer capabilities must all be considered. And, in addition to such point-to-point services, multicast service may increase the efficiency of delivering some applications.
- ▶ **Strong Usable Authentication.** NS/EP services must be reserved for authorized personnel. Violations or compromise could result in increased economic loss, widespread panic, loss of public confidence, or even loss of life. Strong authentication of users, devices, processes, and communications is a prerequisite for authorizing access level by role or responsibility. This includes authorization by link, device, and user, and a recognition that this capability should be platform independent, whenever possible.
- ▶ **Priority and Preemption Over Non-NS/EP Users.** Authorized NS/EP users should be given priority access to required network resources, including transmission capacity, servers, and operations personnel during crises when impairments or transient loads constrain available resources from satisfying both NS/EP and non-NS/EP demands. Priority must extend to the application level, i.e., emergency e-mails should take priority over all other messages even if transmission capacities and servers are operating normally. End-to-end prioritization may

be required beginning with the access link of the authorized, authenticated user, and such priority may need to be applied in those places where congestion can or may occur. Therefore, a wide variety of priority techniques will be needed along with methods to pass authorization among users, devices, communications, and network layers. Wireless end node link layers will have to fairly share or cede link capacity.

- ▶ **Mobility.** Mobility will require a combination of technologies used for strong authentication, along with wireless access methods including terrestrial, aerial, and satellite communication. The required solution also includes detailed radio technical requirements beyond the scope of this report, along with network layer techniques similar to ad hoc networking protocols.
- ▶ **Multilingual and Equal Access.** NS/EP communication among authorized users, as well as the general public, must accommodate users with a wide range of communication abilities. The NGN must facilitate support for multiple languages, and people with visual, auditory, cognitive, or other impairments.

In addition, while most scenarios demand or assume communications protection, it is expected this requirement will largely be met by end-to-end encryption provided by the communicating systems or applications. Of course, different NS/EP communities will require different levels of data confidentiality and integrity that must be met.

Other requirements are critical, but in some instances are at odds with the requirements of other scenarios. While these may also be critical, they are not common to all scenarios:

- ▶ **Relative Priority.** The scenarios highlighted varying requirements for priority within the NS/EP user community based on many factors, including situation-based, role-based, and application-based priority. Assigning data priority according to these factors is difficult. Should an acceptable, widely deployable solution be identified that can assign data priority, existing network elements and design

methods are adept at guaranteeing performance up to design load and isolating the effect of one traffic class on another.

- ▶ **Network-Based Location Estimation Versus Untraceability.** Use of location-based technologies continues to increase, both by the general public and within the NS/EP community. As these capabilities gain popularity, there are nonetheless instances where NS/EP users may not want location information or other information to be identifiable to others. Untraceable applications will also need to be available in the NGN environment.
- ▶ **Fail Safe Versus Fail Secure.** Some communications require systems to “fail secure;” if confidentiality, integrity, or other security services cannot be guaranteed, then no communication is to occur. In contrast, other uses require “fail safe” operation, preferring unencrypted communication to none at all. Either option will need to be available in the NGN environment.
- ▶ **Communities of Interest.** Applications and technology must be provided that will enable NS/EP users or other groups that support NS/EP to come together in a dynamic, authenticated manner over a multitude of platforms.
- ▶ **Content-Aware Security Services Versus Transparency.** Today, both active and passive content-aware security services are available. Some entities would prefer, as part of a layered defense-in-depth strategy, to depend on content-aware security services, for example, to block attacks before they reach systems. However, many entities do not require content awareness within the network or prefer to explicitly deny such capabilities. For example, logging of traffic or even statistics may reveal sensitive information. Therefore, such services should be available to NS/EP users on a per-connection or per-user basis,¹⁴ and user requests should not be overridden.
- ▶ **Emergency Alerts.** Emergency alert capabilities may leverage several existing technologies, including captive portals, broadcast and multicast capabilities,

and peer-to-peer networking. The NGN must be able to absorb and manage a large amount of alert message traffic, and new traffic management capabilities may need to be examined or understood, along with safeguards to prevent abuse.

5 Identity Management

Recommendation: The President should direct OMB, the Department of Commerce, and DHS to work with the private sector in partnership to develop a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity “silos,” allows federation between the Government and commercial domains, and supports use of Government issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including for priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.

5.1 Introduction

Identity management is a key underpinning of security for NS/EP communications on the NGN. The NGN provides open access to a broad array of communications, data, and services, and interconnects an increasing number of users, processes, and devices. This open access to an increased number of communicators introduces an enhanced set of vulnerabilities as compared to traditional voice and private line networks, where identity is generally directly linked to the service. Moreover, given the breadth of the NGN, interoperability among identity management mechanisms is critical; federation is essential. Government must leverage new and existing technologies in implementing its identity management processes.

Strong authentication of users, devices, processes, and communications is a prerequisite for authorizing access level by role or responsibility.¹⁵ This includes authorization by link, device, and user. Moreover, it is clear that this capability should be platform independent

whenever possible. Identity management systems must be independent of the underlying hardware platforms. In particular, they must support the broadest possible range of access speeds, transmission power, processor speed, memory, and operating system. Identity management systems must also be independent of the underlying application in order to enable any and all applications to use authenticated identity for access control and authorization when necessary. The authentication protocols used by the identity management system should also be, to the extent possible, independent of the underlying transport.

The President’s NSTAC has made recommendations in this area in earlier reports, notably with regard to the T1.276-2003 standard in the *Operations, Administration, Maintenance, and Provisioning (OAM&P) Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane Report*, issued on August 28, 2003. However, this section aims to elucidate specific identity management issues that relate to NS/EP communications in the NGN.

The Federal Government has also taken efforts to address the need for a common identification standard through the issuance of Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, the *Federal Information Processing Standard (FIPS) 201, Personal Identity Verification of Federal Employees and Contractors*, and *General Services Administration (GSA)’s Federal Identity Management Handbook*.¹⁶ FIPS 201 was developed to satisfy the requirements of HSPD-12 and provides procedures and specifications for improving the identification and authentication of Federal employees and contractors to allow for physical and logical access to Government resources. HSPD-12 and FIPS 201 focus on human authentication, personal identity verification (PIV) card management, and access control to physical and IT systems. Authorization decisions related to logical resources are not a part of the program and will remain at the enterprise level. The program’s current phase focuses on interface interoperability and the adoption of common assurance, biometric, and cryptographic standards. No efforts have yet been taken to explore how FIPS 201 might include common credentialing standards that could be used to support prioritized,

end-to-end NS/EP communications on the NGN. Although a common assurance taxonomy has been set forth, it has not been developed in partnership with the private sector to ensure federated interoperability between commercial and Government systems.

5.2 Identity Management Criticality

Identity management is a crucial underpinning of NS/EP communications over the NGN, which is likely to provide open access to a broad array of communications, data, and services, and interconnect an increasing number of users, processes, and devices. Without the ability to identify NS/EP users in the open NGN environment, NS/EP privileges cannot be properly assigned. Strong authentication for users, devices, processes, and communications is a prerequisite for authorizing access level by role or responsibility. If NS/EP services are not reserved for authorized personnel, Federal and private sector responses to natural disasters, terrorist attacks, or national security threats could be impeded. For example, without an effective identity management regime, NS/EP priority in a time of contention for access cannot be reliably and consistently granted. Furthermore, identity management is critical for NS/EP services such as information sharing among communities of interest. Accordingly, any identity management failures on the NGN could imperil access, connectivity, and delivery of critical NS/EP services.

5.3 Identity Management Mechanisms, Standards, and Taxonomy

Coordinated Federal agency efforts and public-private partnerships could dramatically improve identity management on the NGN. Federal department and agency support for the prompt development and use of identity management mechanisms, including strong authentication, could accelerate the implementation of more secure systems than currently exist on the PSTN. Coordinated agency efforts would greatly enhance secure access for both current Federal NS/EP users and those Federal officials who may become ad hoc NS/EP users in a crisis.

No cohesive effort to ensure that NS/EP requirements are addressed in identity management protocols and standards now exists. Given the need for interoperability between and within Government and commercial domains, a public-private partnership is essential to provide an appropriate forum for identifying requirements and leveraging existing and emerging protocols and standards. As executive agent for the NCS, DHS will be a critical participant in this effort. It will be important for the Manager of the NCS to engage with the appropriate senior officials and chief information officers in other agencies.

A public-private partnership could play an important role in developing and implementing a common assurance taxonomy that would be accepted within both Government and commercial domains. A broadly accepted taxonomy of identity assurance levels of operational requirements and levels of intensity is expected to contribute to pervasive interoperability of identity management mechanisms. Such taxonomies exist; for example, NIST Special Publication 800-63 Electronic Authentication Guideline defines a four-level assurance taxonomy for U.S. Government credentials. More recently, NIST issued FIPS 201, which Federal agencies are required to follow. FIPS 201 includes graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The graduated levels of a security access could potentially accommodate NS/EP users. However, neither the guidelines (Special Publication [SP] 800-63) nor the Federal standards (FIPS 201) reference any special NS/EP-related authentication requirements. Federal standards must recognize NS/EP requirements and define scalable assurance levels to address unique NS/EP assurance needs. Bodies chartered with the responsibility for ensuring the adequacy of authentication mechanisms on the NGN for NS/EP use need to communicate requirements to standards-making organizations. Finally, a common assurance taxonomy could also further the harmonization of protocols and standards.¹⁷

5.4 Resiliency of Identity Management

While networks can be built from imperfect components and still meet survivability requirements, identification mechanisms must be at least as survivable, standing alone or in combination with alternatives, as the NS/EP services that rely on them.

When Federal and critical infrastructures officials respond to NS/EP-related incidents, they need to rapidly establish their identity on any available network. A resilient identity management capability is critical for authenticating the NS/EP user so they can share important information and manage the crisis at hand.

5.5 Anonymity and Identification

Some NS/EP applications and services will be available only to identified objects or persons, who may or may not be regular NS/EP communicators. However, certain uses of the NGN, even for NS/EP communications, will likely remain anonymous, such as the reporting of public health information.

Given the increasing number of communicating users, processes, and devices, a user's identity on the NGN will be required more often, in a broader number and type of settings, and more frequently than today. Depending on the nature of the situation, ordinary users may need to receive NS/EP alerts, contact emergency services, or access other NS/EP services. In this context, identification for NS/EP purposes is not limited to the needs or activities of Government or other large organizations. The special vetting requirements for access to NS/EP services may compel the surrender of personal information by individuals, in order to obtain the necessary credentials for such access. That said, some NGN communications may or must be available to unidentified recipients (receiving alerts) or senders (emergency "911" communications, possibly), and "best efforts" transport services may well remain anonymous.

5.6 Federation, Interoperability, and Credentials

Government should ensure that its identity management mechanisms can be federated with the commercial sector, with international networks, and across the Federal Government; there should be no isolated "identity management silos" without

strong justification. While Government may choose to build "identity management silos," adopting its own authentication requirements, the end result is usually unsatisfactory. The resulting isolated systems often atrophy, and even Government employees and contractors begin to route around them. For example, agencies that failed to provide e-mail to employees sometimes found that employees would use personal e-mail accounts to communicate.

Even when NS/EP needs are at their greatest, such as for national security communications, silos tend to be reconnected because of operational needs to communicate. This can lead to higher costs and lower assurance. Government can and should mitigate against the risks of unplanned interconnection by planning for interoperability as systems are initially deployed.

Issuing Government (State or Federal) credentials that are capable of operating in a federated identity management environment could greatly improve identity management, especially in response to an incident. For example, priority could be afforded to appropriate persons or devices in an emergency on an ad-hoc basis (e.g., persons living near a weapon of mass destruction event). Federated identity management helps to resolve two challenges: (1) it is almost impossible to determine in advance who may need to send or receive NS/EP communications; and (2) one individual or entity may have multiple identities and need differing levels of access because of the roles they may perform in a given incident.¹⁸

Moreover, interoperability maximizes utility. Accordingly, interoperability or federation between sponsoring commercial and Government domains, voluntarily accepted by them, is essential to ensure the ability of users with credentials from diverse sources to communicate in times of crisis (e.g., a local first responder with an employee of the Department of Defense).

Government can greatly simplify implementation of an identity management system by relying upon and deploying existing and emerging interoperable protocols and standards for exchanging and storing security credentials, including mechanisms for revoking previously issued credentials. Consistent and

coordinated Government implementation would also encourage the development and implementation of existing and emerging standards for hardware interfaces and communication protocols for portable hardware cryptographic devices (e.g., smart cards, PDAs, cell phones) to enable flexible access to NGN services.

In sum, technical mechanisms (e.g., protocols) and policy mechanisms (e.g., a common taxonomy of assurance levels) support interoperability between and within commercial and Government domains, and should be accompanied by an enforcement capability, which could be distributed.

5.7 Commercial Technologies and Deployment

The Government could realize multiple benefits by encouraging the Federal use of more secure commercial existing and emerging identity management mechanisms for NS/EP. For example, Government use of commercial identity management technologies will create incentives for the further commercial development of such mechanisms and infrastructure to support them, leading to overall security improvement on the NGN. Commercial mechanisms are typically available at lower cost, provide greater capabilities, and are updated rapidly as technology improves. Deployment and use of mechanisms being deployed commercially will also support interoperability between commercial and Government domains (and support deployability of solutions). Therefore, preferences for Commercial-Off-the-Shelf (COTS) solutions should explicitly extend to identity management services and technologies.

To be effective for NS/EP communications, identity management solutions must be deployable—practicable, acceptable to the community using them, and scalable. Users will “route around” solutions of limited utility or that otherwise do not meet their needs, using alternative channels of communications, and NS/EP users will default to insecure methods of communication. Accordingly, Government efforts regarding identity management should, to the greatest extent possible, permit the market to determine and build the best mechanisms for meeting Government-specified NS/EP identification needs.

5.8 Trust/Social Concerns

Users should be required to reveal as little personal information as necessary to gain authorization, such information should be sufficiently protected, and entities must be accountable for the security of the information they collect. Technologically elegant solutions that are perceived to violate personal privacy will be criticized.

Care must be taken with issues of privacy and usability. To entice the voluntary, cooperative participation of individuals and organizations outside the sphere of Government activities, the “value proposition” must convincingly deliver a net benefit in the eyes of a potentially very large and diverse user population. The user experience must be simple, quick, satisfying, and highly resistant to abuse or error, because much of that population may have limited experience in the fundamental mechanisms underlying the identity management regime.

6 Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services

Recommendation: The President should direct OSTP, with support from the collective NCS agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor initiatives that would foster NS/EP capabilities within the NGN, including initiatives concerning:

- ▶ A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the

NGN, consistent with a user's NS/EP authorization and required class of service; and

- ▶ NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into IPv6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IPsec for authentication and confidentiality.

6.1 Unique NGN End-to-End Service Issues

Top-level elements and critical functional aspects for NGN end-to-end service include access, transport, and the availability of infrastructure and application-level services. If access, transport, and service availability can be assured for NS/EP functions, it is then possible to maintain the required state of readiness to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. However, the fundamental requirements of access, transport, and availability of services must be provided in a manner that assures that NS/EP communities receive the appropriate priority among potentially competing users.

Fulfilling any of the requirements above entails an ability to have packets within the NGN delivered with required performance, reliability, and priority end-to-end. To meet these needs, ensuring quality of service during normal periods of operation and during periods of network stress will be essential. Periods of network stress can result for any number of reasons, including physical, logical, malicious, unintentional, accidental, or other events that degrade the performance of a network or network service upon which a critical function relies.

End-to-end service connectivity considerations for NS/EP applications include, but are not limited to:

- ▶ Interior routing protocol(s) to exterior routing protocol(s) conversion,

- ▶ Translation or encapsulation of mixed network management traffic,
- ▶ Network topology hiding, protection, and isolation (Firewall) activities between connected networks,
- ▶ Design of data collectors for performance, fault, and accounting information,
- ▶ Dynamic network element configuration across an inter-connected environment,
- ▶ Definition, dissemination, and enforcement of end-to-end security policy, and
- ▶ Definition and dissemination of network management policies and standard operating procedures for use in defined NS/EP contingencies and scenarios.

6.2 Common Operational Criteria

For the foreseeable future, the NGN will be based on a set of interconnected individual networks. See Section 6.7. End-to-end service will be achieved through coordination of these multiple connected networks, linked both physically and logically via common operational criteria accepted and enforced among adjacent networks. Depending on the scope and severity of an NS/EP event, local network policy may need to be supplanted by a common operational criteria agreement. Policies for handling contention for resources and other critical issues on an individual network or across multiple networks in an NS/EP event require definition and enforcement of common operational criteria.

The common operational criteria should be defined for user authentication, network resource authorization, and precedence, permitting definition of multiple classes of service across constituent networks of an NGN, and ultimately should be a requirement for any network provider involved in NS/EP communications. User authentication and network resource authorization are two key criteria for access to network services whether or not contention is present. Precedence becomes a third key criterion when contention is present. Requests for classes of service, therefore, are based

on considering these three criteria—authentication, authorization, and precedence, in combination.¹⁹ Common operational criteria also would facilitate the transition from Internet Protocol version 4 (IPv4) to version 6 (IPv6), and would allow for more seamless peer-to-peer and meshed network communications.

The evolution of technology and communication services is triggering substantial changes in the makeup of the communications sector. The number of companies playing a significant role in providing the Nation's communication services is expanding dramatically, with an associated increase in complexity due to technology, services, and points of responsibility. Government coordination with the communications industry will need to be modified to account for these changes. Today, existing NS/EP programs such as the NCC and the priority services programs it oversees are built to support the small community of carriers that have traditionally supported the NS/EP role. The NCC's processes and approaches for coordination as they stand today will not support the increased number of NS/EP providers. Existing priority services programs rely on direct relationships with the individual wireline and wireless carriers providing the service. As complexity increases, new collaboration approaches must be developed for ensuring reliable NS/EP communications. To address the larger number of participants, technology, services, and points of responsibility, the common operational criteria should be developed using an inclusive joint industry-Government planning process. Because of the complexity and broad range of NGN operators and other stakeholders, it will be necessary to hold regular summits to foster the development of NGN criteria for NS/EP requirements. Annual or even more frequent reporting from this development framework would enhance coordination among Government and industry and tracking of progress by them.

The criteria should be agreed upon by participating networks in an NGN context, to provide a framework for supporting NS/EP activities that extend beyond a local network level. Network providers should demonstrate that they have the capability to support the criteria prior to an NS/EP event, including assignment of user priority and enforcement of NGN policy end-to-end.

NGN NS/EP common operational criteria must address and incorporate these essential elements:

- ▶ Identification, authorization, and authentication of the NS/EP user—namely, a person, communication device, or network—trying to access local telecommunications services.
- ▶ Priority access during times of contention and agreements on how priority transport of packets across multiple networks will be serviced consistent with a user's NS/EP authorizations and required class of service.
- ▶ Practices and controls to manage security to provide required operational integrity.
- ▶ Mechanisms and agreements for managing and coordinating incident response when events materially affect the normal servicing of NS/EP users.
- ▶ Best practices for participants, who are supporting and supplying services for NS/EP users of the NGN.
- ▶ Defined classes of service supported by all network participants within the NGN.

6.3 Local Access and Priority

In an NGN context, local access is defined as: (1) physical access and connectivity to communications, and (2) a local end point connection and the destination end point connection. Local access is critical to end-to-end service, connecting people and devices with network resources, and many issues with connectivity tend to occur at the access point.

Authentication should be required for a valid NS/EP user to gain access to limited NGN NS/EP resources, including approval of NS/EP priority requests at the local access and transport partitions. A network user can be an individual, a communications device, or another network, as all three may request network access and resources from one or more sub-networks within the NGN.

During an NS/EP event, many different types and levels of priority users may need to access the network. Priority management must be implemented uniformly across the NGN, based on user, device, or network authentication, network resources authorization, and class of service requested at the local access or transport partitions. Additionally, common operational criteria across the NGN could include a standard mechanism to ensure uniformity of priority definition and support end-to-end.

Establishing local access priority will require:

- ▶ Authentication of the user;
- ▶ Authorization of network resources;
- ▶ Identification of entities authorized (e.g., devices and human users);
- ▶ Establishment of information assurance and integrity; and
- ▶ Adherence to industry-accepted technical standards.

6.4 Scope and Relative Levels of Priority

As noted above, when extremes in load are present, NS/EP communications need appropriate prioritization. In this regard, priority must be provided on per-packet basis to “payload” or “content” as well as control traffic and other information used to set up a communication or gain access to an NS/EP service. Merely prioritizing packets that allow access to an NS/EP service could be insufficient in several circumstances, such as if the network loses some capacity, causing packets to be discarded even if appropriate bandwidth had been reserved or assigned. Accordingly, prioritization methods should protect the quality of an entire session and prevent packets from being discarded on the NGN.

The NGN should provide prioritization of command and control activities above all communications traffic including priority communication traffic so that the network control centers can appropriately manage and reconfigure the systems to respond to traffic conditions

(especially in times of congestion). Patch prioritization is an example of a command and control capability. When software flaws impair network conditions, distributing to and installing critical software patches on various NGN network components must be possible in order to take corrective action.

Finally, prioritization should extend to wireless communications on the NGN. In the circuit-switched network, Wireless Priority Service (WPS) is supported via a system whereby callers dialing a WPS feature code followed by a telephone number receive priority treatment (assuming they are subscribers to WPS) via radio queuing. In the NGN, a similar service should be supported. However, a vulnerability exists such that a flood of calls placed by a malicious attacker at the time of an emergency (some of which would likely be completed), or even repeated attempts from non-malicious users given the availability of automated access attempts, could clog the network and make it difficult for emergency responders to complete communications even with the use of WPS.

6.5 Internet Protocol version 6

IPv6 provides fundamental benefits over IPv4, including a vastly increased number of available IP addresses, more efficient routing infrastructure, better security implementation, and increased mobility while maintaining existing connections. One key benefit to NS/EP users may be the protocol's auto-configuration and neighbor discovery capabilities. These features would enable NS/EP devices to quickly locate other IPv6 devices for call routing and communications. Further, the simplified and extensible header in IPv6 also provides NS/EP planners an opportunity to request a certain quality of service.

The flexibility of IPv6 provides NS/EP users opportunities to logically control and manage their network communications over a shared or public infrastructure. This flexibility, combined with the ability to authenticate and encrypt end-to-end communications with IP security, provides new opportunities for providing temporary NS/EP services that can support incident management.

The transition to IPv6 is already under way in many networks. Such networks are, and can continue to be, inter-linked with legacy IPv4 networks using either protocol translation or tunneling mechanisms to route IPv6 data traffic within IPv4 packets. Network equipment interoperability and open standards-based compatibility are crucial in mixed IP protocol operational environments.

Seamless network-to-network trust relationships are essential among constituent networks comprising the NGN to ease access to network resources after initial user authentication and network authorization procedures have been successfully performed. Therefore, networks must accommodate a mixed protocol operational environment, supporting current and anticipated user requirements with either IPv4 or IPv6 network connectivity.

6.6 Peer-to-Peer Technology

Peer-to-peer (P2P) technology offers independence from centralized infrastructure, and is especially useful in times of crisis.

P2P communication techniques can be applied at the application level or at the network level. When used at the application level, two parties can communicate with each other as long as they have network connectivity with each other, without dependence on other infrastructure services. The network connectivity may be provided by centralized infrastructure through which messages are routed to the two peers.

Alternatively, the two peers may have network-level connectivity with each other that does not require or depend on centralized infrastructure. In such cases, the connectivity may be provided by a mesh or ad hoc network composed of devices connected using P2P communication techniques. For this reason, Common Operational Criteria among providers of constituent mesh and overlay networks should be established as an integral component of an overarching NGN security policy. See Section 6.7.

Network-level P2P communication frameworks have the advantage of being fully distributed, scalable, and cost-effective to deploy on either a short- or long-term basis.

Peer-to-peer networks, elements, and systems should play a key role in NGN end-to-end service for dedicated, mobile, and ad hoc users supporting NS/EP activities.

6.7 Meshed Network Environments and IP Security

In a typical NS/EP scenario, individual networks are integrated into a full or partial mesh of wire line, wireless, satellite, and private networks, including the Internet. An NS/EP contingency requires heterogeneous environments to quickly and effectively support high availability, resiliency, and security from an end-to-end services perspective. However, to support communications in these scenarios, a consolidation is required of myriad homogeneous (and often single-purpose) networks optimized for a dedicated user community.

Methods vary greatly for authenticating users, reserving network resources and bandwidth, assigning priority classes, enforcing end-to-end security policy, and determining optimal routes for data and management traffic among networks. In the NGN, interconnectivity is based on deployment of an overlay, peer, or hybrid architecture to support services end-to-end across multiple networks.

Meshed networks have the following advantages: (1) no single point of failure, which enhances resiliency; (2) a percentage of the network remains intact and usable even though large segments of the overall meshed architecture is rendered unusable; and (3) the incremental and distributed nature of a meshed network is more readily configured and builds incrementally in locations without preexisting infrastructure. Tradeoffs must be considered in implementation, however, such as possible instability in tightly meshed operational environments.

Using IPsec, a standard for providing security at the network layer by encrypting and/or authenticating all IP packets, to preserve confidentiality and authentication of communication increases in importance in a meshed

network environment, where the possible paths between two or more entities are more numerous. In such situations, it is difficult to establish and ensure a level of trust among connected devices. IPsec provides capabilities for user authentication, device authentication, integrity and authenticity of communications, and confidentiality of, communication, which can be used independently or in combination.

7 Research and Development

Recommendation: In support of the prior recommendation, the President should direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, NIST, and DOD to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria, and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/information technology and service providers.

Industry often pursues R&D in areas where it anticipates a clear financial return. Industry funding for basic research and for meeting non-market requirements, possibly including NS/EP communications, is less certain. Government-sponsored research is recommended to provide a forcing function for developing necessary end-to-end NS/EP capabilities. These efforts should focus on areas in which investments would not otherwise be made, that is, those that may not have a clear financial motivation but would further the cause of NS/EP communications. Funding of demonstrations, especially end-to-end focused efforts, will assist NS/EP communities in capitalizing on new technologies. Results must be shared with and be commercializable by industry.

Another area warranting research attention is the NGN architecture. In the current architecture, messages that control network elements are co-mingled with general payload. This presents the concern that network control messages could be accidentally or intentionally embedded within general payload traffic. The technical community is examining ways to increase security of network control messages

within various industry standards organizations. An investigation of methodologies that can protect the control plane and ensure that capabilities are not accessed inappropriately would be appropriate.

8 Technology Lifecycle Assurance and Trusted Technology

Recommendation: The President should direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of (1) technology lifecycle assurance mechanisms; and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.

Hardware and software flaws represent potential vulnerabilities that will likely be exploited to the detriment of NS/EP capabilities. Hardware (including programmed and programmable semiconductor “chips”) and software are pervasive in our society and will continue to be so in the NGN; flaws or even the deliberate introduction of vulnerabilities in this hardware and software, can occur across the entire technology lifecycle (design, development, and deployment). In addition, the current trend by vendors and service providers to leverage the advantages of outsourced and offshore mechanisms may present increased risk because there are few broadly-used standards, mechanisms, controls, or capabilities for lifecycle assurance. Further, during the deployment and sustaining phases of the technology lifecycle, there is a potential for incorrect installation, configuration, and maintenance errors to occur resulting in vulnerabilities exploitable by threat actors of varying capabilities and motivations.

Notably, as compared to the PSTN, the NGN depends to a much greater degree on widely distributed and powerful hardware and software components, raising the importance of the trustworthiness and security assurance of these components in order to protect security end-to-end on the NGN as part of a comprehensive risk management strategy. These components will also be produced by an

increasing number of entities, and NGN services will be delivered by an increasing number of providers (see Section 6.2); these producers and providers will have varying levels of competency and discipline.

As part of a comprehensive risk management strategy, the Government should address these risks by encouraging, by policy and incentive, research regarding, and implementation of, supply-chain processes and safeguards that provide trustworthy assurances for technology regardless of where or by whom technology is designed, developed, manufactured, or deployed. Use of technology lifecycle assurance mechanisms proven to increase the security of technology across the lifecycle (design, development, deployment, etc.) can thereby increase the security assurance of information and telecommunications systems used for NS/EP. These mechanisms may include advanced engineering disciplines, standards and certification regimes, and best comprehensive practices. For example, software development lifecycle mechanisms that incorporate secure development techniques, such as threat modeling, code reviews, and use of appropriate tools, can identify vulnerabilities, regardless of how they are introduced. The Government should encourage by policy and incentive techniques and processes that can be demonstrated to improve security and reduce vulnerabilities, and should support certification regimes that test implementation of such techniques. Infrastructure providers and NS/EP users, including Government agencies and enterprises, will bear more responsibility on the NGN because of the powerful hardware and software they possess that will affect the security of NS/EP communications. Effective certification regimes²⁰ will enable these users to make appropriate choices in order to protect NS/EP communications.

Moreover, further research and investment in technology lifecycle assurance mechanisms is needed in the public and private sectors as well as academia. Cooperation is needed among these entities in developing deployment and configuration standards, best practices, and guidance that will better manage and mitigate risks inherent in using the NGN for NS/EP.

Going forward, fundamental changes in technology can enhance the reliability of the NGN for NS/EP communications. The current state of technologies and architectures used in the Internet and NGN environment are wrought with long-known, recognized potential vulnerabilities.²¹ Many recent efforts have been focused on the mitigation and patching of these vulnerabilities and weaknesses. However, fundamental changes in technology, including new architectures not subject to the known vulnerabilities, offer the prospect of comprehensive change in system security. Investments must therefore be made in trusted technology research. Moreover, the “R&D cycle” itself should be conducted under a threat modeling and vulnerability analysis framework. If this were to be done, new technologies would have threats and vulnerabilities already mitigated, and be more trustworthy.

One example of this work is the trusted hardware root technologies.²² Software-only security solutions that attempt to protect sensitive data have systemic vulnerabilities.²³ Hardware-based solutions to security problems have advantages that complement software-based solutions, thus counteracting remaining vulnerabilities and providing defense in depth. This layered defense could allow such systems to be inherently more trustworthy by providing features such as secure boot as well as process and data signing and attestation.

9 Resilient Alternate Communications

Recommendation: The President should direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure.

Convergence of most communications to an IP-based backbone (the NGN) will result in more communications resilience. Most disruptions in the NGN will be relatively easy to repair or work around.²⁴ Regional service may be disrupted, but will be brought back online promptly in most cases. Unfortunately, NS/EP professionals and the public they serve cannot settle for communications that are up and running “in most cases.” As NS/EP depends more on NGN communications, damage or destruction to communications infrastructure can seriously impair NS/EP mission-critical response and recovery efforts; including those of Federal and localized first responders, non-governmental organizations (NGO), general public initiatives, and private-sector response and restoration. Because the point of access to the NGN is the point most likely to suffer congestion (with the most limited bandwidth, typically) or a single-point-of-failure, it is the point of greatest concern.

NS/EP responders already depend on alternate communications methods. They use cellular phones to provide communications redundancy, for example, where a cell-tower infrastructure is operating. Other examples include the use of a separate two-way radio system to provide primary system redundancy, and the provision of satellite capabilities. In the later case, satellite capabilities not only provide another preferred alternate access means, they also offer a nonterrestrial infrastructure base unaffected by most terrestrial disasters. Hand-carried devices can be designed to connect to an antenna or satellite system affixed to the exterior of a vehicle (or similar unit) or to other network “aware” devices that could extend service areas through interconnection and resulting geographic dispersion. And, the Federal Communications Commission (FCC) supports use of amateur radio organizations to provide alternate communications services. In short, the best resiliency is achieved by diverse communication methods.

Use of alternate communications for resiliency will become easier on the NGN given the capabilities of end-user devices. In the emerging NGN, many NS/EP-utilized communication devices will contain multiple access capabilities within the same form factor. Examples could include devices that access multiple commercial networks, satellite, and/or other private

systems, depending on availability, device functionality, and user authority. In this regard, private industry is developing devices with the innate ability to access multiple types of access networks (i.e., “on-ramps”) and infrastructure types (i.e., dynamic access/homing), which will be significant with regard to NGN NS/EP user capabilities, and strategic with regard to continuity of operations (COOP) planning. These devices should be adopted by NS/EP users.

Other techniques important for communications resiliency include having a resilient (robust) or alternate power supply, including devices and infrastructure components operated on available fixed electrical power systems, fuel-based fixed and portable electric generation, battery-based power, and other emerging energy sources such as solar power, depending on needs.²⁵ The combination of multiple WPS providers within an incident area can add overall capacity to an affected area and provide for alternate access methods. Priority can help provide resiliency of communications, and the coalescence/convergence of WPS and Government Emergency Telecommunications System (GETS) into a coordinated end-to-end NS/EP priority treatment service (see sections 6.3 and 6.4) will add resilient, reliable, and consistent capabilities for NS/EP communications users. NGN services such as ENUM (IP address/landline number and device mapping) and alternate contact routing, will enhance communications infrastructure reliability and enhanced capabilities. Finally, over-provisioning²⁶ of capacity by infrastructure providers can add resilience should network congestion or loss of network links occur.

Applying will further enhance the NGN for NS/EP services.²⁷ Diversity in routing critical links should be pursued, and steps taken to ensure true route diversity and not simply diversity of suppliers where the physical paths travel in the same cable sheaths or systems. Alternate communications access should also be provided at “sheltering” points. It is of paramount importance that Federal Emergency Management Agency (FEMA), National Guard, and local authorities have accessible alternate communications and resources for those who require them. For example, National Oceanic and Atmospheric Administration

(NOAA) and portable AM/FM capabilities are used for alternate communications, the overall NS/EP communication mission between NS/EP users, and as outreach to the general population.

Ensuring constant communications reliability during every high-level crisis is an infeasible goal. Accordingly, NS/EP users must consider the full spectrum of possible disruptions in their contingency planning and develop solutions based on their own unique requirements. Fortunately, the likely convergence of most communications into a robust IP backbone will create far more resilience than exists, and most disruptions will be relatively easy to repair or work around. (It is important that avoiding single-points-of-failure be a design consideration for the NGN.) Conversely, a greater dependence on communications over the NGN also has the potential to create a single point of failure from a local access perspective. With applications and services converging into a common infrastructure, those who could not gain access to the NGN in a crisis situation would have few viable alternatives.

Therefore, incident managers should implement alternate communications that will provide multiple access options for reaching the NGN backbone or for local and regional communications. Examples include satellite phones, line-of-sight optical systems, digital broadcast satellite (DBS), devices with multi-access capabilities, mesh networks, metropolitan wide-area networks, such as IEEE 802.11(b) Wi-Fi (Wireless Fidelity) and IEEE 802.16 Wi-MAX (Worldwide Interoperability for Microwave Access) networks, and many others. Currently, the NCC and other agencies use the SHARED RESOURCES (SHARES) High Frequency (HF) Emergency Radio program, which provides a single interagency emergency message handling system for the transmission of NS/EP information. The SHARES program brings together existing HF radio resources of Federal, State, and industry organizations when normal communications are destroyed, disrupted, or unavailable due to natural or manmade disasters.

OMB and DHS have significant oversight and planning requirements for ensuring resilient communications. Under the Federal Information Security Management Act of 2002 (FISMA), OMB must annually approve

agency IT security programs. As part of this process, OMB could base approval of such programs on a focused plan for resilience. Further, OMB's FISMA reporting process could monitor agency progress in this area annually. OMB has already issued a memorandum directing each agency to review its telecommunications capabilities in the context of planning for contingencies and COOP situations;²⁸ such reviews should consider not only physical route diversity but also alternate communications mechanisms that could operate should a loss of access infrastructure occur. Finally, DHS's Federal Emergency Management Agency is updating Federal Policy Circular 65 (FPC65), which establishes IT communications requirements for COOP communications and could build NGN-specific requirements into the overall planning effort.

10 Agreements, Standards, Policy, and Regulations

Recommendation: The President should direct DHS, the Department of State, and DOC (including NIST and NTIA) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally-distributed NGN environment.

Arrangements and expected behaviors between entities are one of the basic building blocks of the communications infrastructure.²⁹ These include mutual agreements/Service Level Agreements (SLA), industry standards, accepted policies and Government regulations (collectively, ASPR). Whether between two entities or among hundreds, and whether among companies, Governments, or both, ASPRs have an essential role in ensuring NS/EP communications. Unlike the NS/EP capabilities of legacy networks,

which were built on an existing framework, the NS/EP capabilities of the NGN will be developed as the NGN itself is being developed. This requires meticulous care in the establishment of supportive ASPR. To this end, one of the critical goals of the recommendation above, to establish a Common Operational Criteria development framework, is to foster the creation of effective ASPR.

The intrinsic vulnerabilities of ASPR include:³⁰

- ▶ Lack of ASPR;
- ▶ Conflicting ASPR;
- ▶ Outdated ASPR;
- ▶ Unimplemented ASPR (complete or partial);
- ▶ Interpretation of ASPR (mis- or multi-);
- ▶ Inability to implement ASPR;
- ▶ Enforcement limitations;
- ▶ Boundary limitations;
- ▶ Pace of development;
- ▶ Information leakage from ASPR processes;
- ▶ Inflexible regulation;
- ▶ Excessive regulation;
- ▶ Predictable behavior due to ASPR;
- ▶ ASPR dependence on misinformed guidance;
- ▶ ASPR ability to stress vulnerabilities;
- ▶ ASPR ability to infuse vulnerabilities; and Inappropriate interest influence in ASPR.

The intentional or unintentional exercise of any of these vulnerabilities by a threat can significantly impair NS/EP communications. For example, agreed upon standards that are not implemented fail to provide the defined capabilities. Similarly, information leakage through policy development processes and predictable behavior from known regulations can provide tactical advantages to an adversary.

Of course, implementation of this recommendation faces significant challenges. First, ASPR development lifecycles are often very time-consuming. Second, ASPR processes are often complex, require considerable technical, regulatory, and other expertise. Third, ASPR development often involves a large number of stakeholders and associated interests—including the broad international community. The Common Operational Criteria development framework must be designed to address the vulnerabilities presented by ASPR and the challenges associated with them.

Multiple international standards bodies and industry forums are developing NGN ASPR.³¹ Regarding standards, industry vendors and operators are actively developing the requirements, architecture, and detailed protocols. However, Government involvement in these NGN activities is limited. With convergence, and the enhanced NS/EP services that the NGN will provide, an increasing number of standards will be of critical importance. Accordingly, the NGNTF previously recommended that:

- ▶ The President should direct his departments and agencies to participate more broadly and actively in the NGN standards process in partnership with the private sector in areas such as web services, directory services, data security, network security/management, and control systems, all of which will become increasingly important to NS/EP communications platforms.³²

The Government must monitor development of standards that will affect NS/EP communications on the NGN; it must also actively participate and contribute in appropriate for a to influence the development process so that NS/EP needs are better met and new NGN capabilities are available for NS/EP communications.

Additionally, the appropriate Government agencies and regulatory bodies must be active in defining NGN NS/EP requirements. Vendors and operators make the best effort possible to represent the governmental and regulatory positions. However, sometimes these positions are interpretations by the various companies of the Government wishes and mandates. It would be beneficial for the NGN standards process if Government representatives could be present during the development of the NS/EP NGN services and capabilities requirements to clarify the Government requirements and mandates.

This work includes such critical areas as resilient communications (see above) and first responder communications³³ needs, critical to support and enhance the end-to-end NS/EP mission. This work should be supported via appropriate private industry and Government resources and technical contributions.

Moreover, leadership in many areas of NGN standards, including some associated with NS/EP communications, resides in international and foreign regional bodies. See Appendix I. Some of these bodies have organizational rules that prevent the participation of companies from various regions of the world. For example, the European Telecommunications Standards Institute (ETSI)³⁴ TISPAN (Telecommunications and Internet Protocol Harmonization over Networks [TIPHON] and (Services and Protocols for Advanced Networks) [SPAN]) project is developing sets of NGN-related standards that will probably be attempted to be applied globally. However, the current organizational rules require TISPAN meeting participants to be ETSI members. To be an ETSI member, the associated companies of the participants must have business offices or operating business divisions in Europe. Based on these organizational rules, many of the United States-based companies, including the largest wireless operator in the United States, are prevented from being active participants in the TISPAN activities and are prevented from having access to the members-only area of the TISPAN project that contains detailed contributions and discussion papers.³⁵ The United States' NS/EP interests could be adversely

affected if the ability of its companies and Government to participate in standards development is impaired, and United States NS/EP requirements are not adequately represented.

11 Incident Management on the NGN

Recommendation: The President should direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the NCC, for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

11.1 Introduction

NS/EP communications incident management has traditionally existed in the realm of the physical event, and a process is in place to manage those events, including how they affect wireline and wireless communications. The NCC has historically assisted in the NS/EP incident management function for communications providers.

However, the NGN environment includes numerous new technologies and new industry players who control key network elements but may not have relationships in place with industry and Government incident managers. Most new communications providers are not members of the NCC, and therefore, they are not as easily accessible during an incident, nor do they reap the benefits of membership, including building trusted relationships with industry and Government. Additionally, the network itself is becoming increasingly complex and global in nature, pushing incident management out beyond the realm of the territorial United States.

As new providers and technologies continue to enter the communications arena, management of cyber incidents and blended physical/cyber incidents has proven more improvisational. Unlike management of physical incidents, management of cyber incidents is associated with limited common terminology, few standard processes, and few established guidelines on how the situation should be handled. Federally funded cyber exercises have been conducted to pinpoint gaps, yet they have not reached the level of sophistication and standardization required. Future cyber exercises should approach the degree of professionalism attained by military exercises in the areas of planning, organization and evaluation, and must include a feedback loop for discussion and implementation of lessons learned.

Meanwhile, communications providers are transforming their networks by branching out heavily into IP-based wireless and packet-switched communications. These architectures and the host of new providers and technologies create significant challenges for incident management in the NGN.

11.2 Unique NGN Incident Response Issues

The transition period to the NGN presents challenges for ensuring the security and availability of NS/EP communications, including in the broad areas of first responder communications, control systems, such as Supervisory Control and Data Acquisition (SCADA) systems, network gateway protection, Continuity of Operations (COOP), Continuity of Government (COG), and financial services transactions. In addition, new threats and vulnerabilities create complex risk scenarios for NS/EP communications in an NGN environment. A further challenge is the NGN's global nature, which will require that methods for managing incidents of national significance address international cooperation.

The time available to respond to or thwart a cyber attack on converging networks continues to decrease, making it more difficult for human mitigation of the attack. In the near future, automated mitigation efforts will be needed to effectively manage an incident, which only increases the complexity of the NGN environment and effectively removes incident control

from human hands. With the reduced response time, incident managers have even less time to thwart cyber attacks and must focus their efforts on response and mitigation.

The open, layered architecture or nature of the NGN facilitates the offering of new services and services from new providers. Many new providers are unfamiliar with NS/EP incident response. Corporate "attitudes" may differ between the two entities on incident management priorities—for instance, NS/EP incident management often requires more information sharing and collaboration with Government entities than is normal for nontraditional providers. New providers existing in an unregulated environment are more hesitant to develop relationships with Government entities. The providers have created informal incident response networks that have been sufficient to respond to customer needs, and yet they may not be formal enough to ensure NS/EP communications will remain secure and available during an incident of national significance. Companies will need to develop a mutual understanding on how to meet customer expectations for service on the NGN while continuing to ensure that NS/EP capabilities, including priority treatment of communications, are available to the Government and other incident managers at appropriate times.

With increasing complexity, interdependencies (known and unknown) and the distributed nature of the network, management plans will need to remain flexible to account for numerous attack methods, recognizing the limitations of a one-size-fits-all approach. The key to NGN incident management will be to maintain the level of service expected today by consumers while balancing new threats.

11.3 Industry Involvement Throughout the Planning Process

Incident response must be a joint effort between industry and Government. As such, industry and Government must work jointly on strategic policy for incident management from its earliest stage of development. This would be a change from the current process in which Government produces a formal plan

and industry is asked to comment in the plan's final stages. The private sector should be more active during planning and response, but as part of a collaborative process as an equal partner with Government.

DHS has published a variety of high-level plans, including the National Response Plan (NRP) and the National Incident Management System (NIMS). For the most part, these plans exist at a very high level, and are derived from a background of physical rather than cyber events. From an incident management perspective, the plans do not go into detailed processes for incident management and recovery; they are geared more toward offering high-level organizational principles for desired results. NIMS, for instance, is aimed at a very broad audience and is considered a "framework" for responders at all levels to use in working together. These plans, constructed by the Government with little input from industry, provide very little guidance for real-world mechanisms and processes for incident management in an NGN environment. For example, had industry been involved in the detail of the Homeland Security Operations Center (HSOC) approach, industry would likely have been more engaged in the Center's early activities.

11.4 Joint Coordination Center

A joint coordination center for industry and Government should be established. 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. Such a center would improve communications between industry and Government as well as among industry members, and would incorporate and be modeled on the NCC.

The center should be a Government-funded, appropriately equipped facility, manned jointly by experts from all key sectors. In a fully converged NGN environment, everything will be interconnected and interdependent to a greater degree, and thus means of coordinating among all key sectors must exist. Physically collocated, joint manning is vital to achieve the high level of interpersonal trust needed for sharing sensitive specific information and to achieve the level of mutual credibility required in a fast-paced

decision-oriented environment.³⁶ It should provide the full set of planning, collaboration, and decision-making tools for those experts to work, whether together as a whole or in focused subgroups.

Industry is at times hesitant to share information with the Government because it is unsure of how the information will be used, and Government-to-industry information sharing should also be improved.³⁷ DHS has a vision for how HSOC will function to improve information sharing; however, the HSOC's current operational interface to the private sector is nascent and needs further development. An environment of trust must be established. A joint operations center could play a key role in fostering that environment and in enhancing HSOC operations. In addition, appropriately cleared industry experts collocated in a joint coordination center with their Government counterparts could assist the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the DHS intelligence analysis arm, in performing its analytical and reporting functions, helping to ensure that HITRAC products are more complete, credible and useful.

11.5 Exchange Program

Incident response, including planning for response, requires a joint industry/Government effort, and each group must better understand the other's role. To this end, an exchange program should be instituted to foster understanding between industry and Government practitioners in network operations, security operations, and crisis management. The groundwork for this initiative has already been laid; an IT Exchange Program³⁸ (ITEP) has been established by the Office of Personnel Management but has not been implemented in the executive branch or at the Federal department or agency level.

11.6 Federal Incident Management Training Academy

A Federal training academy for incident managers should be established. NGN incident management operations would be improved if cross-sector industry training is available. Accordingly, the Government should set up an all-hazards intensive training center with specific attention played to NGN and cyber issues.

Experienced incident managers have repeatedly stated that having employees with the capability, knowledge, and authority to respond during an incident is far more important than having a detailed written plan. A training academy could immerse students from industry and Government in realistic and intense scenarios over a set period of time, such as a one-week session of round-the-clock incident management immersion.³⁹ This would also foster strong relationships among NGN incident responders in industry and Government, laying the groundwork for more effective communications during an actual incident.

11.7 Exercise Program

To further the capability, knowledge, and authority of incident managers, a formal exercise program for NS/EP communications incident response on the NGN should also be established. This program should be collaboratively developed, broadly participatory, and regularly evaluated. It could be developed in tandem with the training academy, and would be designed to fit into national strategic plans such as the NRP. The exercises themselves should be modeled on the level of detail and professionalism demonstrated by military programs. The key to the success of this program will be the implementation of lessons learned into future activities. Industry must be involved early on in the process and should be involved in the creation of the objectives for the exercise.

11.8 Increased Research and Development Funding

As historic methods for responding to incidents become outmoded, R&D funding related to incident management should increase. This investment could fund incident management research toward developing advanced monitoring, detection, decision making, and response capabilities. A concerted effort should be made to research human factors in incident management.

12 International Policy

Recommendation: The President should direct his departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental

cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-U.S. companies in NS/EP incident response in the United States; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.

Protecting and promoting NS/EP communications requires international action. The NGN will be used globally. NGN communications will transit international borders. Finally, NS/EP services will be provisioned internationally (such as Domain Name System [DNS] services). It is simply not tenable to treat NS/EP communications as a domestic issue only.

Both private industry and Government have made progress in the pursuit of international cooperation and coordination. Industry is inherently international—many if not all NSTAC member companies have international operations—and must work with other international companies and Governments on key issues affecting NS/EP communications. Moreover, formal and informal industry coordination mechanisms operate internationally, and standards development organization have international membership.⁴⁰

The State Department effectively represents the Government in international discussions regarding critical infrastructure protection. Those discussions have recently included the requirements for NS/EP communications. As the highly connected NGN reduces the effect of national borders on our networks, NS/EP communications will increasingly involve international issues. Accordingly, it is critical that upcoming international discussions on critical infrastructure protection include an NS/EP element.

Many issues, however, remain, including how to handle incident response in a converged environment. See Section 11, above. In short, we have a good understanding of how to handle NS/EP incident response on the existing PSTN, but converged networks are far more likely to involve international players, with incidents first noticed abroad, participants affected abroad, services provided from abroad, or components

(hardware/software) provided from abroad. The Federal Government will face difficult issues in deciding whether and how to involve international participants in a national security communications incident when those participants are outside of the United States. Similarly, international companies may have much to contribute to U.S. watch, warning, and incident response capabilities, including the Telecommunications and Information Technology Information Sharing and Analysis Centers (ISACs); however, it is unclear whether participation of international companies in these fora would adversely affect their partnership with the United States. The Federal Government should develop and communicate to industry a rational policy that balances the need for including the most critical companies with protecting the national security of the United States.

Outside the realm of incident response, it is possible that different governments could take contrary approaches to protecting NS/EP communications on the NGN. With widespread international interdependence, such conflicts could undercut the effectiveness of solutions inside and outside of the United States. Accordingly, in the international discussions referenced above, and in other international fora, the Federal Government should seek compatible approaches to NS/EP communications, consistent with the recommendations in this report.

13 First Responders

Recommendation: The President should direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

When mature, the NGN will provide first responder and public safety organizations with much greater capabilities, such as transmission of data real-time along with voice. The NGN will also aid interoperability in cases where “operability” of first responder and public safety networks and the NGN itself are present. The connection or bridging of disparate networks to

the NGN will allow communication between them via the underlying protocols of the NGN. See Figure 2. As noted in the NGNTF’s Near Term Recommendations Report:

- ▶ The timely migration to newer digital, interoperable, and standardized solutions, backed by appropriate policy use for such systems, will help ensure that America’s first responders are properly prepared, equipped, and able to coordinate their response to all-hazards and emergency situations.⁴¹

However, significant challenges also surround end-to-end NGN services for first responder and public safety organizations. First responder and public safety networks may be among the last to be upgraded to the NGN due to security and availability concerns arising from interconnection and because of the difficulty, particularly in terms of resources, to upgrade legacy systems. With regard to the former, this Report recommends critical steps to make the NGN an NS/EP-capable network. And with regard to the latter, the Federal Government can play a critical role in supporting the transition of first responders and public safety organizations to the NGN. As stated in the Near Term Report:

- ▶ Government agencies, such as [DHS Office of Interoperability and Compatibility],⁴² should continue to enhance the capabilities of first responders via the following: providing needed levels of funding for digital equipment; supporting standards and policy development; allocating spectrum appropriately and in an expedited manner; broadening the deployment of WPS; and upgrading Public Safety Answering Points.⁴³

14 Conclusion

The NGN can provide considerable benefits for NS/EP communications; however, to realize these benefits and speed the transition to the NGN, solutions that address NS/EP functional requirements are required, especially for security and availability. This is an end-to-end problem; on a packet-based network such as the NGN, information will travel over various networks and equipment, and a failure at a critical point absent

mitigation, such as an alternate communications path, could impair the communication. For the NGN to broadly meet the essential NS/EP functional requirements in a consistent, continuous, and reliable end-to-end manner, a set of mechanisms needs to be promoted and adopted by those supplying network access, transport, and infrastructure services for this community, as well as NS/EP users. Accordingly, industry and the U.S. Government should enhance their partnership to achieve an elevated level of cooperation to implement these mechanisms, developing: organizational solutions for incident management and the partnership itself; cooperative frameworks supporting identification and end-to-end NS/EP communications; technical solutions that support the next generation of NS/EP-supporting technology on the NGN; and policy solutions that address the increasing diversity, complexity, rapidity of change, and international nature of the NGN itself. There is no silver bullet. Government and industry need to work cooperatively to implement a set of solutions that support NS/EP on the NGN.

Footnotes

1 Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003; Rauscher, Karl. F., Protecting Communications Infrastructure, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.

2 “Next generation networks will take communications beyond vertical silos of function and capability to one packet-based network delivering multiple services that are accessible by multiple types of devices.” ATIS Press Release, Dec. 6, 2004. See also: “IP [the Internet Protocol] is the common thread of a whole host of new and emerging multimedia applications that blend video, voice and data capabilities.” TIA Press Release, Feb. 9, 2005. (http://www.tiaonline.org/media/press_releases/index.cfm?parelease=05-04).

3 Thus, the NGN may be said to be service oriented, as it is focused on delivery of services that are agnostic of the network or terminal type. The U.S. Department of Defense calls this concept Net Centricity: that “Anyone, anywhere can get to any data source and exploit the information they are authorized to access.”

4 Office of Science and Technology Policy (OSTP) and National Security Council (NSC) policies define NS/EP telecommunication services as: “[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 CFR 201.2[g]). Furthermore, the term telecommunications is defined by the OSTP and the NSC policies as: “[A]ny transmission, emission, or reception of signs, signals, writing, images, graphics, and sounds or intelligence of any nature by wire, radio, optical or other electronic means” (47 CFR 201.2[k]). The extent to which these and other Government NS/EP policies apply to new communications mechanisms remains under discussion.

5 Interoperability” is the “ability of software and hardware on different machines to communicate with each other.” Computer User High Technology Dictionary, <http://www.computeruser.com/resources/dictionary/dictionary.html> (hereinafter “Computer User High Technology Dictionary”).

6 “Packet Switching: A technology for sending packets of information over a network. Data is broken up into packets for transmission. Each packet has a header containing its source and destination, a block of data content, and an error-checking code. All the data packets related to a message may not take the same route to get to their destination; they are reassembled once they have arrived.” Computer User High Technology Dictionary.

7 Circuit Switching. A communications method which establishes a dedicated channel for the duration of the transmission, allowing data to be transmitted in real time. The telephone network is a circuit-switched network.” Computer User High Technology Dictionary.

8 For example, the U.S. Department of Defense next generation capability, the Global Information Grid (GIG), involves the concept of Network Centric Enterprise Services (NCES), which includes nine basic next generation services: information assurance (IA); user assistant; messaging; applications; ESM; mediation; discovery; storage; and collaboration.

9 Because services are virtually independent of transport, and there are multiple transport options for a given service, this architecture may be said to be “componentized.”

10 An open standard is a document either developed or ratified by standards organization that operates by consensus or agreement and whose membership is generally open to those impacted by the standards.

11 “New applications can be invented and provided over the NGN via software installed at each endpoint without requiring modification to the [Next Generation Service Provider’s] network or services.” ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture, Issue 1.0, November 2004, at p. 19 (“ATIS Framework”), available on the net at: <http://www.atis.org/topsc/Docs/ATIS-NGN-Framework-Part1-Issue1.pdf>.

12 See ATIS Framework at 8.

13 National Security Telecommunications Advisory Committee, Convergence Task Force Report, 2001.

14 Control mechanisms should not rely on inspection of data content to perform control functions (although they may use such inspection as an optimization), as data may be compressed, encrypted, or otherwise transformed either end-to-end or in-transit.

15 Identity management, while critical, does not replace the need for encrypting information during its transmission (e.g., encryption of the payload of packets) on the NGN to avoid eavesdropping. See Section 4.2 above.

16 The FIPS 201 standard can be accessed from the NIST web site at <http://csrc.nist.gov/piv-project/index.html>. The Federal Identity Management Handbook is available at <http://www.cio.gov/ficc/documents/FederalIdentityManagementHandbook.pdf>.

17 In addition, the E-Authentication E-Gov initiative has developed the components of a federated identity management architecture across the Federal Government, intended to allow citizens, businesses, and State and local government to use a credential of their choice to access e-Government services.

18 The identity management strategy should recognize that an individual might have separate identities (persona) that cannot be associated with each other except by the individual. This would happen where an individual participates in noninteroperable identity-management systems, and could occur within a single identity-management system if the individual needs unrelated identities. These multiple identities are different from the multiple roles that an individual might have associated with a single identity.

19 Common operational criteria define classes of service available or supported based upon accepted definitions of these three criteria for an individual network, or multiple networks in the NGN.

20 One relevant regime is the “Common Criteria for Information Technology Security Evaluation” (CCITSE), referred to as the “Common Criteria” and adopted as an international standard: ISO/IEC 15408. The Common Criteria, at commercially-used evaluation levels, focuses on the correctness of security features as opposed to vulnerabilities in the non-security features of software.

21 For example, there are inherent weaknesses of Von Neumann architectures versus Harvard architectures in processor technology. Attacks against software have been known for some time, and attacks against hardware are now being published. See *SemilInvasive Attacks A New Approach to Hardware Security Analysis*; Sergei P. Skorobogatov, University of Cambridge, April 2005.

22 The Trusted Platform Module (TPM) (specification and other information can be found at <https://www.trustedcomputinggroup.org/groups/tpm>) is one example of a hardware/firmware-based solution that helps security system hardware and software designers and builders work cooperatively to address these issues.

23 See Appendix G, Systematic Assessment of NGN Vulnerabilities. The vulnerabilities may also be addressed substantially by special purpose systems that are not widely deployed, perhaps due to the cost or reduced functionality of such systems.

- 24** As noted above, the NGN will increase network robustness and resiliency through the nature of its mesh architecture, offering many possible routes for traffic and redundancy of equipment and servers. This addresses the familiar single-point-of-failure challenge for reliability. However, the NGN could experience broad disruptions as a result of single modes of failure, such as those associated with a logical protocol error or widespread logical software coding error. See Appendix G, Systematic Assessment of NGN Vulnerabilities. Other recommendations of the Task Force, such as providing priority to command and control communications, are intended to address the single mode of failure concern. This “Resilient Alternate Communications” recommendation specifically addresses the concern of a single point of failure at the access point.
- 25** Another NSTAC Task Force, the Telecommunications and Electric Power Interdependency Task Force is examining interdependencies between these two sectors.
- 26** “Over-provisioning involves providing communications links the bandwidth of which “exceeds the expected traffic load by a certain margin, which is selected to ensure that the link can absorb both expected and unexpected traffic fluctuations.” See Y. Huang and R. Guerin, “Does Over-Provisioning Become More or Less Efficient as Networks Grow Larger?[,]” http://csr.bu.edu/icnp2005/Papers/20_yhuang-Overprovision.pdf.
- 27** See e.g., Network Reliability and Interoperability Council best practices found at www.nric.org. Additional information on these best practices can be found at <http://www.bell-labs.com/user/krauscher/nric/>.
- 28** OMB Memorandum M-05-16, Memorandum for the Heads of Departments and Agencies, June 30, 2005, issued pursuant to Section 414 of Treasury, Transportation, Independent Agencies, and General Government Appropriation Act, 2005 (Division H of P.L. 108-447).
- 29** See Appendix G—Systematic Assessment of NGN Vulnerabilities.
- 30** Ibid.
- 31** See Appendix I, NGN and NS/EP ASPR Ecosystem
- 32** NGNTF Near Term Recommendations Working Group Report, March 2005.
- 33** These standards activities include ITU-R WP8A, Project MESA, and TIA TR-8.8, Broadband Data Systems.
- 34** ETSI has received repeated complaints about this organizational rule and is considering potential rule changes that would allow U.S.-based companies to participate. No specific changes have been incorporated yet.
- 35** One method to overcome this challenge is through the use of a trusted third party that meets the ETSI criteria to represent U.S. NS/EP interests. In addition, industry and standards development organizations are working to ensure U.S. requirements are addressed by groups like ETSI.
- 36** “If the partnership between the federal government and private sector is to be successful, another key requirement is establishing a permanent physical location or forum so that critical and non-critical sectors can interface with one another and their federal counterparts. This is essential to developing and maintaining long-term collaborative relationships.” A Review of the Top Officials 3 Exercise, DHS OIG Report OIG-06-07, p. 24 (Nov. 2005).
- 37** Both these observations were confirmed at the August 2005 NGN Incident Response Subject Matter Experts meetings. See Appendix D.
- 38** See <http://www.opm.gov/fedregis/2004/69-011504-2311-a.htm>.
- 39** Of interest, a bill has been introduced to establish a “National Homeland Security Academy” which would provide both coursework and hands-on training exercises. S. 2158, introduced Dec. 21, 2005.
- 40** Government participation in international standards development is addressed in Section 10.0.
- 41** NGNTF Near Term Recommendations Working Group Report, March 2005.

42 DHS' Office for Interoperability and Compatibility oversees the SAFECOM program, which "is a communications program that provides research, development, testing and evaluation, guidance and assistance for local, tribal, state, and federal public safety agencies working to improve public safety response through more effective and efficient interoperable wireless communications."

43 NGNTF Near Term Recommendations Working Group Report, March 2005.

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE



**NSTAC Report to the President on
Next Generation Networks**

Appendices

March 28, 2006

Table of Contents

A	Task Force Members, Other Participants, and Government Personnel	A-1
B	Acronym List	B-1
C	NGN Definitions	C-1
D	Summary of Analysis Framework	D-1
	D.1 Working Group Processes	D-3
	D.2 Subject Matter Expert Meetings	D-4
	D.3 Scenarios	D-4
E	Federal Functional Requirements	E-1
F	End-to-End Services Issues	F-1
	F.1 Background	F-3
	F.1.1 End-to-End Services	F-3
	F.1.2 The NGN: A Work in Progress	F-3
	F.1.3 The NGN: A Highly Complex Service Environment	F-3
	F.1.4 The NGN is Composed of Multiple, Interconnected Networks	F-4
	F.1.5 Gaining Consensus for a Uniform NGN Logical and Physical Design Is a Critical Success Factor	F-4
	F.1.6 Fundamental NGN Services Availability Issues	F-5
	F.2 Key and Unique NGN NS/EP Issues	F-6
	F.2.1 Local Access Requirement	F-6
	F.2.2 Establishing Priority Among Networks	F-7
	F.2.3 Contention for Resources	F-8
	F.2.4 Common Operational Criteria Framework	F-10
	F.2.5 NS/EP Capability Assurance	F-10
	F.3 Important Technologies	F-11
	F.3.1 Implications of the Internet Protocol	F-11
	F.3.2 Key Benefits of IPv6 Compared with IPv4	F-11
	F.3.2.1 Expanded Addressing Space	F-11
	F.3.2.2 Highly Efficient Routing Infrastructure	F-11
	F.3.2.3 Enhanced Security	F-12
	F.3.2.4 Mobility Support	F-12
	F.3.2.5 Other IPv6 Capabilities	F-12
	F.3.2.6 IPv4 to IPv6 Transition Considerations	F-13
	F.3.3 Peer-to-Peer Networking	F-13
	F.3.4 Meshed Network Environments	F-14
	F.3.5 Role of IPsec	F-15
	F.3.6 Combined Use of Technologies	F-15
	F.3.7 Transition and Interaction of Directory Services	F-15
	F.4 Conclusion	F-16

G	Systematic Assessment of NGN Vulnerabilities	G-1
	G.1 Background	G-3
	G.2 Systematic Assessment	G-3
	G.2.1 Power	G-4
	G.2.2 Environment	G-5
	G.2.3 Hardware	G-6
	G.2.4 Software	G-7
	G.2.5 Payload	G-9
	G.2.6 Networks	G-10
	G.2.7 Human	G-11
	G.2.8 Policy	G-12
H	NGN Threat Analysis	H-1
	H.1 Background	H-3
	H.2 Threat Analysis	H-3
	H.2.1 Widespread Susceptibility	H-3
	H.2.2 Threat Actor Convergence	H-3
	H.2.3 Network Convergence Threat Impacts	H-3
I	NGN and National Security and Emergency Preparedness Agreements, Standards, Policies, and Recommendations Ecosystem	I-1

Appendix A

Task Force Members,
Other Participants, and
Government Personnel

Task Force Members

Microsoft Corporation

Mr. Philip Reitingger, Chair

BellSouth Corporation

Mr. David Barron, Vice Chair

AT&T, Inc.

Ms. Rosemary Leffler

Bank of America Corporation

Mr. Roger Callahan

BellSouth Corporation

Ms. Cristin Flynn Goodwin

The Boeing Company

Mr. Robert Steele

Cingular Wireless LLC

Mr. Brian Daly

Computer Sciences Corporation

Mr. Guy Copeland

Lockheed Martin Corporation

Dr. Allen Dayton

Lucent Technologies (Bell Labs)

Mr. Karl Rauscher

Motorola, Inc.

Mr. Michael Alagna

Nortel

Dr. John S. Edwards

Northrop Grumman Corporation

Mr. Dennis McCallam

**Qwest Communications
International, Inc.**

Mr. Jon Lofstedt

Raytheon Company

Mr. Frank Newell

**Science Applications International
Corporation**

Mr. Henry Kluepfel

Sprint Nextel Corporation

Mr. John Stogoski

Telcordia Technologies, Inc.

Ms. Louise Tucker

Unisys Corporation

Mr. J. Michael Gibbons

United States Telecom Association

Mr. Thomas Soroka

VeriSign, Inc.

Mr. Michael Aisenberg

Verizon Communications, Inc.

Mr. James Bean

Other Participants

ATIS

Mr. Timothy Jeffries

BellSouth Corporation

Mr. Bryan Garrett

Ms. Pamela Gurule

Cingular Wireless LLC

Mr. Brian Daly

Mr. Peter Musgrove

Mr. DeWayne Sennett

Cisco Systems, Inc.

Ms. Robin Roberts

Mr. Chip Sharp

COMTek Communications Technologies, Inc.

Mr. Lew Morrison

Cox Communications, Inc.

Mr. Mark Adams

Mr. Larry Dexter

Mr. Craig Howell

Mr. Scott Smith

George Washington University

Dr. Jack Oslund

Global Crossing

Mr. David Cooper

Hewlett-Packard Company

Mr. Joseph Connor

Mr. Stephen Squires

Intel Corporation

Mr. Ryan Ware

Juniper Networks, Inc.

Mr. Ron Bonica

Lockheed Martin Corporation

Dr. Kate Cherry

Mr. Joseph Cramer

Mr. Chris Nolan

Lucent Technologies

Mr. Tom Anderson

Ms. Cheryl Blum

Mr. Glenn Evans

Mr. Brenton Greene

Mr. Robert Thornberry

Dr. Zhibi Wang

Lucent Technologies (Bell Labs)

Mr. Stuart Goldman

Mr. Eric Grosse

Dr. Alan Jeffrey

Mr. Rick Krock

Mr. Theodore Lach

Dr. Anil Macwan

Mr. James Runyon

Mr. David Shinberg

Mr. Rao Vasireddy

Microsoft Corporation

Mr. Khaja Ahmed

Mr. Jerry Cochran

Mr. Shawn Hernan

Mr. Ted Tanner

Mr. Paul Nicholas

Mr. Henry Sanders

Mr. Sanjay Kaniyar

Motorola, Inc.

Mr. Michael Berta

Mr. Tom Gaynor

Mr. James Goldstein

Mr. Don Dautel

Mr. Benjamin LaPointe

Mr. Chip Wood

Pennsylvania State University

Dr. Thomas La Porta

PriceWaterhouseCoopers

Mr. James Craft

Qwest Communications International, Inc.

Mr. Curtis Ashton

Raytheon Company

Mr. Sean Anderson

Rutgers University

Dr. Michael Tortorella

Spectrasite

Mr. Ted Abrams

Sprint Nextel Corporation

Mr. Chase Cotton

Ms. Allison Growney

Mr. Keecheon Kim

Telcordia Technologies, Inc.

Mr. Arun Handa

Mr. Robert Lesnewich

Telecommunication Industry Association

Mr. David Thompson

United Telecommunications Council

Ms. Prudence Parks

University of California at Berkeley

Dr. Shannon Lake

VeriSign, Inc.

Mr. Anthony Rutkowski

Verizon Communications, Inc.

Mr. Timothy Beard

Mr. Bruce Fleming

Mr. Stuart Jacobs

Government Personnel

Department of Defense

Mr. Scott Swartz

Federal Reserve Board

Mr. Chuck Madine

Department of Homeland Security

Mr. Daniel Ahr

Mr. Gary Amato

Mr. Steve Carty

Mr. David Delaney

Mr. Thomas Falvey

Mr. Alan Gallagher

Ms. Mai Tai Galloway

Mr. John Graves

Mr. Rick Lichtenfels

Ms. DeJuan Price

Ms. Carol-Lyn Taylor

Capt. Eric Koenig

Mr. Dan Zink

General Services Administration

Mr. Doug Covert

Appendix B

Acronym List

Acronym List

ASPR	Agreements, Standards, Policies and Recommendations	OASIS	Organization for the Advancement of Structured Information Standards
ATIS	Alliance for Telecommunications Industry Solutions	OIC	Office of Interoperability and Compatibility
BGP	Border Gateway Protocol	OSTP	Office of Science and Technology Policy
COP	Committee of Principals	PCS	Process Control System
CRISP	Cross Registry Information Service Protocol	PKI	Public Key Infrastructure
DCS	Digital Control Systems	PSTN	Public Switched Telephone Network
DHS	Department of Homeland Security	RFC	Request for Comment
DISA	Defense Information Systems Agency	SCADA	Supervisory Control and Data Acquisition
DNS	Domain Name System	SCTP	Stream Control Transmission Protocol
DOD	Department of Defense	SIP	Session Initiation Protocol
DOS	Denial of Service	SOAP	Simple Object Access Protocol
ETS	Emergency Telecommunications Service	SSH	Secure Shell
FCC	Federal Communications Commission	SSL	Secure Sockets Layer
FICC	Federal Identity Credentialing Committee	TCP	Transmission Control Protocol
GETS	Government Emergency Telecommunications Service	TIA	Telecommunications Industry Association
GIG	Global Information Grid	TLS	Transaction Layer Security
GSA	General Services Administration	VPN	Virtual Private Network
IAIP	Information Analysis and Infrastructure Protection	VTMWG	Vulnerabilities and Threat Modeling Working Group
IDS	Intrusion Detection System	WPS	Wireless Priority Service
IES	Industry Executive Subcommittee	XML	Extensible Mark-Up Language
IETF	Internet Engineering Task Force		
INEEL	Idaho National Laboratory		
IP	Internet Protocol		
IPS	Intrusion Prevention System		
IPSec	Internet Protocol Security		
IPv4	Internet Protocol Version 4		
IPv6	Internet Protocol Version 6		
IRIS	Internet Registry Information Service		
ISP	Internet Service Provider		
IT	Information Technology		
NCS	National Communications System		
NDAC	Network Design and Analysis Center		
NGN	Next Generation Networks		
NGNTF	Next Generation Networks Task Force		
NIST	National Institute of Standards and Technology		
NRIC	Network Reliability and Interoperability Council		
NSC	National Security Council		
NS/EP	National Security and Emergency Preparedness		
NSTAC	National Security Telecommunications Advisory Committee		
NTRWG	Near Term Recommendations Working Group		

Appendix C

NGN Definitions

NGN Definitions

As used in this paper:

Applications: Software or hardware entities that provide specific, valuable functions or services to users.¹

Services: Functions provided by software or hardware entities built on top of the transport networks to deliver user-visible services such as fixed telephone services, mobile telephone services, and Internet services.²

Transport Networks: Facilities that carry user information and network management/control information between different endpoints.

Appendix D

Summary of Analysis
Framework

Summary of Analysis Framework

D.1 Working Group Processes

At the President's National Security Telecommunications Advisory Committee (NSTAC) XXVII Meeting held on May 19, 2004, the NSTAC Principals requested that a task force be created to address how the Government can continue to best meet national security and emergency preparedness (NS/EP) telecommunications requirements and address emerging threats in the evolving NGN environment. Subsequently, the Next Generation Networks Task Force (NGNTF) was created to:

- 1) Agree upon a high-level description of the NGN's expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely;
- 2) Identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and accountability among network participants and network layers will work; and
- 3) Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements.

As a first step, the NGNTF assembled a group of subject matter experts (SME) and Government stakeholders to discuss NGN issues in August 2004. As a result of the meeting, working groups were created to address the following five areas: (1) a description of the NGN; (2) NGN service scenarios and user requirements; (3) end-to-end services provisioning; (4) NGN threats and vulnerabilities; and (5) incident management on the NGN. A sixth working group was formed to address actions that could be taken immediately to preserve or enhance NS/EP communications for the future.

The Near-Term Recommendations Working Group (NTRWG): The NTRWG examined near-term opportunities for which existing technology could be leveraged to improve the security and availability of NS/EP

communications on converging networks. The NTRWG also investigated areas where Government involvement was needed in the near term due to the immediacy of events—such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs. Based on the NTRWG's analysis of near-term challenges and opportunities, the NSTAC made several recommendations to the President in March 2005.

The NGN Description Working Group: This group was formed to provide a high-level description of the NGN. The description reflects the vision of different communities and addresses what is known, what is unknown, and what the market may determine regarding the network.

The Scenarios and User Requirements Working Group (SURWG): The SURWG examined existing descriptions of NS/EP functional requirements to develop recommendations for Government stakeholders regarding how these functional requirements should be amended or supplemented based on the scenarios. To accomplish its analysis, the working group developed scenarios in five areas: Continuity of Government, critical Government networks, industry and critical infrastructure, public safety, and general users. After identifying NS/EP user requirements that apply within an NGN environment for each scenario class, the working group then considered how these requirements will differ from those of traditional communications networks and what this will mean for network users.

The work of the SURWG served as the foundation for the work of the NGNTF's End-to-End Services Working Group and the Vulnerabilities and Threat Modeling Working Group. Together their work provided key insights into how next generation NS/EP services can be more resilient and maintain high quality, on-demand, seamless accessibility.

The End-to-End Services Working Group (ESWG): The ESWG examined the end-to-end services aspects of the evolving NGN and the implications to those performing NS/EP functions. The working group tasks included describing how end-to-end services would be provisioned and explaining how the interfaces

and accountability among network participants and network layers would work. Building upon the work of the SURWG, the ESWG identified specific areas that Government, industry, and user community stakeholders and decision-makers must address, which will impact availability of those end-to-end services that the NS/EP communities require at times of crisis.

The Vulnerabilities and Threat Modeling Working Group (VTMWG): The VTMWG examined relevant threats and vulnerabilities from an NS/EP perspective, using the SURWG scenarios among others. The VTMWG examined vulnerabilities of NGNs from an NS/EP perspective; examined relevant threats associated with the SURWG scenarios from an NS/EP perspective; and identified how responsibilities for responding to or mitigating these threats have shifted. Emphasis was placed on confidentiality, integrity, availability, and authentication of communications.

The Incident Management Working Group (IMWG): The IMWG was formed to respond to NGN incident management issues raised at the August 2004 SME Meeting, including response time needed to thwart cyber attacks, the increase of nontraditional service providers in the NGN environment, and a need for improved information-sharing incentives, among other issues. In August 2005, the IMWG hosted a SME Meeting on Incident Management in the NGN, which was attended by about 100 incident managers from the communications and information technology industry as well as the Federal Government. The 2005 SME Meeting Proceedings are published separately.

D.2 Subject Matter Expert Meetings

August 4-5, 2004: The NGNTF held its first SME Meeting on August 4-5, 2004, at Computer Sciences Corporation (CSC) in Falls Church, Virginia. The primary objectives of the meeting was to facilitate a better understanding of the key technical and policy issues surrounding the evolution of the current telecommunications network to NGNs and to develop the NGNTF's work plan for addressing the issue. The NGNTF used the input from this meeting to develop its key objectives for the task force, including an effort to develop near term recommendations. The SME meeting focused on several critical areas including: Priority and Alternatives

for NS/EP Communications; Cyber Security; End-to-End Services; and Wireless and Incident Management. The NGNTF's working groups—Description, Scenarios and User Requirements, End-to-End Services, Vulnerabilities and Threat Modeling, and Incident Management—were formed as a result of the findings from the meeting.

August 30, 2005: The NGNTF held a second SME Meeting with the National Coordinating Center (NCC) Task Force (NCCTF) on August 30, 2005, also at CSC in Falls Church, Virginia. The purpose of the meeting, "Incident Management in Next Generation Networks," was to further explore the findings from the Incident Management breakout group at the first NGNTF SME Meeting and to receive feedback on potential incident management recommendations for the NGNTF final report. A further objective of the meeting was to validate findings from three of the NGNTF subgroups: the SURWG, the ESWG, and the VTMWG.

D.3 Scenarios

The NGNTF created and charged the SURWG to develop scenarios for NS/EP communications on the NGN. The SURWG examined existing descriptions of NS/EP functional requirements to develop recommendations for Government stakeholders on amendments or supplements to these functional requirements based on the scenarios. To accomplish their analysis, the working group developed five scenarios:

- ▶ **Continuity of Government.** Focused on the needs and functional requirements for maintaining the systems and networks critical to the ongoing functioning of Government during incidents of national significance.
- ▶ **Critical Government Networks.** Focused on the needs and functional requirements of a network key to the continuity of the U.S. economy, Fedwire.
- ▶ **Industry and Critical Infrastructure.** Focused on the needs and requirements for maintaining the functionality of Supervisory Control and Data Acquisition (SCADA) systems supporting U.S. critical infrastructures.

- **Public Safety.** Focused on the needs and functional requirements of first responders and other public safety organizations, such as hospitals, during an NS/EP event.

- **General Users.** Focused on the needs and functional requirements of the general civilian user during incidents of national significance and how these might compete, or in some cases interfere, with NS/EP communications needs. A further emphasis is on the NS/EP user that must access NS/EP communications services from a general civilian device or location (e.g., home Voice over Internet Protocol [VoIP] service; Internet access over a wireless handheld from a public hotspot).

After identifying NS/EP user requirements for each scenario class that apply within an NGN environment, the working group then considered how these requirements would differ from those of traditional communications networks and what this would mean for network users. The work of the SURWG served as the foundation for the work of the NGNTF's ESWG and the VTMWG.

Appendix E

Federal Functional
Requirements

Federal Functional Requirements

The President's National Security Telecommunications Advisory Committee's Convergence Task Force Report, 2001, determined that the following functions were necessary for the Federal Government to effectively make use of Next Generation Networks (NGN). Concepts such as "scalability" or "secure networks" do not go far enough in describing what technologies, services, and applications will be needed to support the Government's national security and emergency preparedness (NS/EP) mission going forward. As will be discussed in greater detail below, and throughout the scenarios to follow, the functional requirements are not applicable to all networks, systems, and users. However, Federal agencies may pick and choose the NGN NS/EP services needed to support a mission, based on the particular environment.

The fourteen Federal functional requirements are as follows:

- Enhanced Priority Treatment
- Secure Networks
- Ubiquitous Coverage
- International Connectivity
- Interoperable
- Scalable Bandwidth
- Mobility
- Broadband Service
- Reliability/Availability
- Restorability
- Survivability/Endurability

- Non-traceability
- Affordability
- Voice-Band Service

Appendix F

End-to-End
Services Issues

End-to-End Services Issues

F.1 Background

This Appendix provides additional background (developed by the End-to-End Services Working Group) on end-to-end services relevant to the conclusions and recommendations of the Next Generation Networks Task Force (NGNTF), which are contained in the main body of the Report.

F.1.1 End-to-End Services

A variety of new feature-rich services, extending beyond those available today, will emerge as the NGN develops. New expanded and highly integrated services, including video, geo-location and navigation aids, peer-to-peer communications and a plethora of other new and “smart” multimedia, interactive programming and data-intensive information services will become commonplace and ubiquitous. The strong emergence of standards-based technology for web services within service-oriented architectures (SOAs) will increase information technology adaptability and efficiency for a broad range of user and network applications. Greater wireless-based capabilities will allow access to information and services without the familiar wire tethers of our legacy telecommunications world. Nomadic capabilities will also blur the line between a location-based telephone and a mobile terminal, and location or numbering constraints.

Individuals with national security and emergency preparedness (NS/EP) roles and mission functions have a critical need to understand how the NGN service environment impacts their ability to execute those functions, and how their needs for assured services and availability will be satisfied by the NGN under a range of operational conditions; namely, routine day-to-day activities all the way to highly stressful crisis conditions.

It is critical for user communities to understand how to plan, implement, and accomplish their NS/EP missions through effective use of the evolving NGN environment. A question repeatedly asked by members of these communities: “what NS/EP required functions will be provided inherently by the NGN and what functions will NS/EP users need to provide?”

The NGN infrastructure will integrate a number of common network and information services, including messaging, discovery, collaboration, storage, numbering, and security. A plethora of custom application-oriented services for various affinity groups will also exist. For the various NS/EP communities of users, it is most important that those NGN capabilities and services used for critical mission functions be well-defined, understood, available and reliable.

Over time, it is anticipated that market force mechanisms will satisfy those NS/EP community requirements that have broad application within the NGN. As they are today and have historically existed, the most critical and often more narrowly required NS/EP community’s needs may have to be addressed through alternative support mechanisms. Recent events and disasters have highlighted the importance of this community, including first responders, be given the support they need.

In order for the NGN to broadly meet essential NS/EP community requirements in a consistent, continuous and reliable manner from end to end, a ‘common operational criteria’ must be defined and adopted by entities supplying network access, transport and infrastructure services for this community.

F.1.2 The NGN: A Work in Progress

A fully capable NGN, as envisioned by both infrastructure and service-oriented professionals, readily supports current and forecast user requirements with highly available and robust connectivity. As the NGN itself is in an early implementation stage, actual access, transport, and service availability today may not fully support anticipated NS/EP user requirements. In addition, as the NGN is a local, regional, national, and global service environment, uniform and consistent support of broad NS/EP user requirements across extended geographical distances is a most challenging design goal.

F.1.3 The NGN: A Highly Complex Service Environment

Complex enterprise service environments, such as the NGN, are composed of multiple disparate networks, network management systems and data operations centers, integrated both logically and physically to support myriad applications for a diverse user community of interest. In an NS/EP context, daily

operational complexity is significantly increased as a result of the emergence of often unforeseen and highly variable challenges, including real-time bandwidth allocation to support routine and surge data traffic, rapid user authentication and resource prioritization, transparent control of inter-network data and signaling information, and seamless management of critical and real-time end-to-end services, all supported within a compliant heterogeneous operational framework.

Although heterogeneous by design, the NGN shares common logical and physical components, such as:

- ▶ Routing and switching network elements,
- ▶ Network element operating systems,
- ▶ Network management platforms,
- ▶ Basic application services present on each network,
- ▶ Desktops and/or workstations in a distributed architecture, and
- ▶ Internal and external network routing protocols.

F.1.4 The NGN is Composed of Multiple, Interconnected Networks

NS/EP service availability in a dedicated, ad hoc, and/or geographically dispersed environment is enabled through dynamic, adaptive and resilient management of data traffic transported across interconnected user, management and control planes. Inter-network service connectivity considerations for NS/EP applications include, but are not limited to:

- ▶ Interior routing protocol(s) to exterior routing protocol(s) conversion
- ▶ Translation or encapsulation of mixed network management traffic
- ▶ Network topology hiding, protection and isolation (Firewall) activities between connected networks

- ▶ Design of data collectors for performance, fault, and accounting information
- ▶ Dynamic network element configuration across an interconnected environment
- ▶ Definition, dissemination and enforcement of end-to-end security policy, and
- ▶ Definition and dissemination of network management policies and standard operating procedures for use in defined NS/EP contingencies and scenarios.

Figure F-1, shown below, illustrates a notional depiction of the NGN. Note that public safety networks may be markedly different from this more commercially-oriented NGN diagram, however many of the basic concepts and NS/EP needs are the same, or even more demanding given the user class.

F.1.5 Gaining Consensus for a Uniform NGN Logical and Physical Design Is a Critical Success Factor

The NGN is designed to support NS/EP scenarios in a localized, metropolitan, regional, national and international context. Success of the NGN, from an architectural and services perspective, is based on stakeholder understanding and acceptance of its capabilities to support well-defined user requirements. Therefore, implementation of the NGN requires designing and developing a scalable, high-availability network architecture capable of supporting current and anticipated user requirements, with realistic levels of service defined. Development of this network architecture includes identifying and resolving issues in the current operational environment that impede achieving that end-state goal. Such issues include optimization of network management capabilities; development, acceptance and the dissemination of operational procedures and practices; and, effective end-to-end mechanisms to rapidly isolate and resolve any network instabilities that impact availability and performance across the NGN.

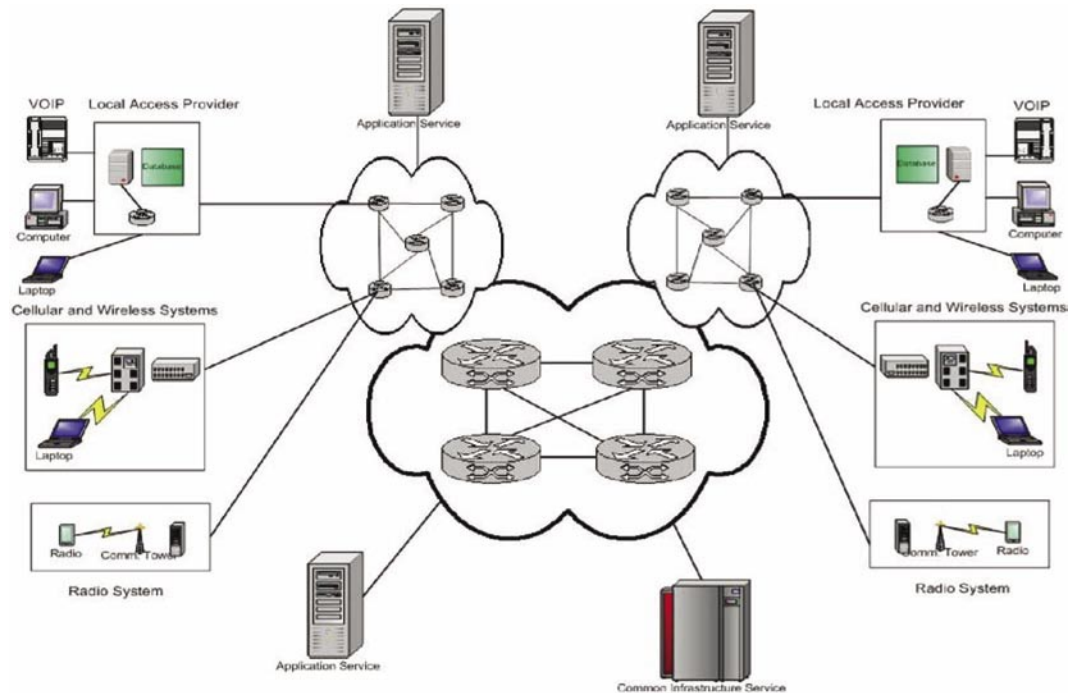


Figure F-1 Notional Depiction of a Commercially Oriented NGN

The NGN NS/EP common operational criteria must address and incorporate these essential elements:

- Identification, authorization and authentication of the NS/EP user—namely, a person, communication device or network—trying to access local telecommunications services
- Priority access during times of contention and agreements on how priority transport of packets across multiple networks will be serviced consistent with a user’s NS/EP authorizations and required class of service
- Practices and controls to manage security to provide required operational integrity.
- Mechanisms and agreements for managing and coordinating incident response when events are materially affecting the normal servicing of NS/EP users
- Best practices for participants, who are supporting and supplying services for NS/EP users of the NGN

► Defined classes of service that are supported by all network participants within the NGN.

Addressing these needs will be a challenge of extraordinary significance and will require unprecedented leadership and collaboration among the public and private sectors.

F.1.6 Fundamental NGN Services Availability Issues

An NGN designed to support NS/EP applications and services for commercial, civil, and Government organizations, focuses on enabling a high-availability, secure and interoperable environment for local, regional and national user connectivity. Based on a logical framework, the NGN emphasizes high availability in a resilient, high bandwidth transport backbone as a principal characteristic. From a security perspective, the NGN is concerned with authentication of users attempting to access the network, uniform enforcement of security policy through user tracking and auditing, and network resources authorization. Interoperability of diverse network elements, protocols and operating systems in a geographically dispersed operational

environment is a significant issue; therefore, managing it effectively is critical to the viability and resiliency of ongoing NS/EP applications and services support in the future.

F.2 Key and Unique NGN NS/EP Issues

NS/EP requirements on the NGN (see Report, Section 4) can be described in terms of three toplevel fundamental and critical functional requirements: (1) access to the NGN; (2) transport of information within the NGN; and (3) availability of infrastructure and application-level services. Assurance of access, transport and services availability for NS/EP functions enable the required state of readiness and ability to respond to and manage any local, national, or international event or crisis that causes injury or harm to the general population, damage to or loss of property, or degradation of the NS/EP operational posture anywhere within the United States. However, the fundamental requirements of access, transport, and availability of services must be provided in a manner that assures NS/EP communities receive an appropriate level of service priority among potentially competing users and activities.

F.2.1 Local Access Requirement

In an NGN context, local access is defined as:

- ▶ Physical access and connectivity to communications, and
- ▶ A local end point connection and the destination end point connection (for human or machine network users as physical and logical entities).

Local access, transport and user services are the three constituent partitions of any network environment. Depending upon context, any of these three may be physical, logical or both concurrently. Local access is the partition that connects people and communications devices, identified as machines, with network resources. Networks connect together at the transport partition, and also use network resources. Therefore, a user community includes

people, communications devices, and other networks. People and communications devices are connected locally and remotely to a network at local access, while networks connect at the transport partition.

Within the NGN it is essential that:

- 1) A network user is defined as an individual, a communications device (machine), or another network, as all three may request network access and resources from one or more sub-networks within the NGN.
- 2) Mandatory authentication is required for a valid user and authorization for resources in appropriate cases such as where the user could affect the NGN itself, and for all user requests at the local access partition and transport partition.

Establishing local access priority requires:

- ▶ Authentication of the user,
- ▶ Authorization of network resources,
- ▶ Identification of entities authorized (e.g., devices and human users),
- ▶ Establishment of information assurance and integrity, and
- ▶ Adherence to industry-accepted technical standards.

Priority is not an issue when all authenticated users have unrestricted access to network resources. Additionally, priority is typically not an issue in the transport partition, especially in the network backbone. However, priority is potentially an issue at local access due to contention for finite network resources available. Resources may be physical and logical, including physical switch ports, logical circuits, bandwidth, connection time limits, and end-to-end resource reservation constraints. Priority access, therefore, is based on the presence of contention for physical and logical resources within a network.

For the foreseeable future, NGN evolution will be as an overlay—composed of multiple physical networks bound together logically by common operational criteria and an overarching security policy. Each individual network's internal operational policy is based on supporting its own user community of interest first, and then supporting directly connected adjacent networks. However, common operational criteria, agreed upon by networks bound by cooperation in an NGN context; provide a framework for supporting NS/EP activities that extend beyond a local network level. In an NGN supporting NS/EP activities, common operational criteria for adjacent networks may supplant local network policy.

Priority resource requests for individuals or communications devices received from external networks are serviced in accordance with the common operational criteria for connected networks in an NS/EP context. When there is sufficient bandwidth and network connectivity to support all requests, there is no contention and priority is not considered. However, when contention for network resources occurs, networks will address resource requests either on a priority or first-come, first-served basis.

In a first-come, first-served context, all resource requests are of equal priority. New requests for network resources are denied in favor of maintaining already established connections once congestion or connectivity thresholds are met. When priority is considered, networks will actively arbitrate resource requests through enforcement of connection time limits; or by clearing lower priority connections randomly (informal call clearing); or via a weighted queue mechanism (formal call clearing) to accommodate higher priority requests. Determination of priority may be based on type of authenticated user, device or network, network resources requested, and type of service indicated in network protocol headers or end-to-end flow labels.

Within the NGN it is essential that:

- 1) A common operational criteria is defined and agreed upon by participating networks in an NGN context, to provide a framework for supporting NS/EP activities that extend beyond

a single local network. Criteria focuses on authentication, authorization, contention, and priority issues across constituent networks in an NGN framework.

- 2) Priority management is implemented uniformly across the NGN, based on user, device or network authentication, network resources authorization, and class of service requested at the local access or transport partitions.
- 3) Priority is defined here as contention for network access, resources and services, but not for access to applications.

F.2.2 Establishing Priority Among Networks

Within an evolving NGN, multiple discrete networks are integrated as required to support NS/EP activities. Communication between two parties may originate in a network of a certain type and go through one or more different networks. Priority is defined and enforced differently by individual entities within the NGN, thus end-to-end priority determination is based on a concatenation of multiple local network policies that respond differently to NS/EP events. The mechanism for evaluating and handling priority of the packet/message/circuit may be different than the one used in the network of origin. Defining and enforcing end-to-end priority is a challenge for network designers and operations personnel alike due to the dynamic nature of the NGN, and the scope, severity and duration of potential NS/EP events. Defining common operational criteria across the NGN is a preferred mechanism to ensure uniformity of priority definition and support end-to-end. This will eventually necessitate agreements at both a business and policy level as well as at the technical levels. This will require definitions of equivalencies and shared semantics for various levels of priority between different types of networks. An appropriately articulated minimal acceptable service threshold of metrics or capabilities by the U.S. Government would benefit those with NS/EP requirements as developers engineer capabilities within the NGN. Further, suitable standard bodies will need to develop the protocols for translating required priority mappings.

Network-to-network connectivity typically occurs at the transport partition. However, under conditions of contention at either the local access or transport partition, user priority becomes the key criterion for permitting access to network resources after successful authentication and authorization occurs. In an NGN, end-to-end contention is a measure of the availability of resources across multiple constituent networks. Common operational criteria define and enforce priority uniformly for any and all users requesting network resources at either the local access or transport partitions. Participating networks in an NGN are required to successfully demonstrate the capability to support specified common operational criteria, such as assigning user priority and policy enforcement. This proof of performance and enforcement is normally defined and demonstrated prior to any actual NS/EP event.

Within the NGN it is essential that:

- 1) A common operational criteria across the NGN is defined as a standard mechanism to ensure uniformity of priority definition and support end-to-end.
- 2) Mutual service level guarantees are developed that encode a set of common operating rules that all registered networks agree to follow;
- 3) The capability to support common operational criteria is demonstrated, such as assignment of user priority and enforcement of NGN policy end-to-end, prior to an actual NS/EP event; recognizing that processes should be in place for ad-hoc or unanticipated support.

F.2.3 Contention for Resources

This issue is critical and highly complex, incorporating a number of intangible concepts such as contention/congestion, the “value” of users and resources, and decision-making in response to all types of NS/EP scenarios. Therefore, clarification is written in detail to propose a tangible approach to assessing and managing the interaction of contention, arbitration and precedence—which clearly complement or oppose each other, based upon event specifics.

For the foreseeable future, the NGN will be based on an overlay of individually connected networks, brought together physically and logically to support a myriad of NS/EP activities. Policies for handling contention for resources on an individual network or across multiple networks require definition and enforcement of common operational criteria. Such criteria provide a uniform mechanism for dealing with arbitration, priority treatment/pre-emption and precedence within a single network or across an expansive NGN.

User authentication and network resource authorization are two key criteria for access to network services whether or not contention is present. Precedence becomes a third key criterion when contention is present. Requests for classes of service, therefore, are based on considering these three criteria—authentication, authorization, and precedence, in combination. Common operational criteria define classes of service available or supported based upon accepted definitions of the three key criteria for an individual network, or multiple networks in the NGN.

An example representative framework supporting common operational criteria is presented below in Figure F-2. The critical elements of this framework: a) user authentication types, b) network service authorization levels, and c) resource precedence states, are combined to define specific classes of service (CoS) offered. Traffic management schemes employing traditional network queuing techniques can support these classes of service by ensuring equitable access and arbitration, or priority, as appropriate.

User authentication types, identifying essential and non-essential entities requesting access to the network at either the local access or transport partition, include:

- ▶ **Support:** Non-critical, sustaining, and administrative individual or network entity
- ▶ **Essential:** First responders, and key personnel or network entity

User Authentication Types	Network Service		Classes of Service (CoS)	Traffic Management Schemes
	Authorization Levels	Resource Precedence States		
Support	Routine	No Precedence to No Precedence Default	Best Effort	FIFO
Support	Imminent	Precedence to Precedence Default	Priority	PQ Med & Low
Support	Sustaining	Precedence to Precedence Default	High Priority	PQ Normal, Med & Low
Essential	Response	High Precedence to High Precedence Default	Critical	WFQ
Essential	Response	High Precedence	Pre-Emptive	CBQ
User Authentication + Service Authorization + Precedence = Class of Service → Queuing Method				

Figure F-2 Common Operational Criteria Representative Framework

Network service authorization levels, based on criticality or potential impact of NS/EP events and scenarios, include:

- **Routine:** Priority/pre-emptive and planning preparations for an anticipated NS/EP event, such as an approaching hurricane or forest wildfire
- **Imminent:** Near-term preparations for an anticipated NS/EP event
- **Response:** Initial critical response to an NS/EP event that has occurred
- **Sustaining:** Ongoing response to, and support for, an NS/EP event after initial response activities are completed

Resource precedence states, based on the presence or lack of contention, include:

- **No Precedence:** No contention present or detected, requested network resource parameters (e.g., bandwidth, connection time) are available to all authenticated and authorized users
- **No Precedence, Default:** Threshold of minimal contention detected, default network resource parameters (i.e., standard operational profile, but no special requests) are available to all authenticated and authorized users
- **Precedence:** Above threshold of minimal contention detected, requested network resource parameters (e.g., bandwidth, connection time) are available to all authenticated and authorized users with any precedence level greater than none

► **Precedence, Default:** Above threshold of minimal contention detected, default network resource parameters are available to all authenticated and authorized users with any precedence level greater than none

► **High Precedence:** Above threshold of minimal contention detected, requested network resource parameters (e.g., bandwidth, connection time) are available to all authenticated and authorized users with any precedence level greater than Precedence

► **High Precedence, Default:** Above threshold of minimal contention detected, default network resource parameters are available to all authenticated and authorized users assigned with any precedence level greater than Precedence

Classes of service (CoS), derived as combinations of user authentication types, network service authorization levels, and resource precedence states, include:

- Best Effort
- Priority
- High Priority
- Critical
- Pre-Emptive

Traffic management schemes correspond to specified classes of service via queuing methods listed below, and are actively employed by operations personnel to manage, arbitrate or preempt access to network resources:

- ▶ First-in, first-out (FIFO) queuing with finite connection time limits supports Best Effort CoS
- ▶ Priority queuing (PQ) with Medium and Low queue weighting supports both Priority and Best Effort CoS
- ▶ PQ with Normal, Medium and Low queue weighting supports High Priority, Priority and Best Effort CoS
- ▶ Weighted fair queuing (WFQ) with Critical, Normal, Medium and Low queue weighting supports Critical, High Priority, Priority and Best Effort CoS
- ▶ Class-based queuing (CBQ) supports Pre-Emptive, Critical, High Priority, Priority and Best Effort CoS

F.2.4 Common Operational Criteria Framework

Support for the Pre-Emptive service class requires the network to assign resources on a virtually unrestricted basis in support of highly critical essential users. The preferred traffic management queuing method is class-based, which permits network operations and management personnel to manually clear existing connections in favor of highly critical incoming requests or allow the network to manage access and resources through autonomous flow-based criteria. In all classes of service, network connectivity ensures access to network applications. Therefore, access to applications occurs as a result of authorization to use the network resources needed to establish connectivity with any hosts, databases and servers. A pre-emptive CoS involves policy decisions and authorization.

Within the NGN it is essential that:

- 1) A common operational criteria is defined for user authentication, network resource authorization, and precedence that permit definition of multiple classes of service for networks participating in the NGN.
- 2) Traffic management schemes are implemented supporting fair access, arbitration and priority treatment/pre-emption of network resources end-to-end.

F.2.5 NS/EP Capability Assurance

A planning, design and response criteria for the NGN is based on the summation of criteria successfully implemented by individual constituent networks. Therefore, a “global” NGN is a confederation of networks, cooperatively merged in response to common NS/EP events, which benefits from a cohesive end-to-end integration of best practices learned and implemented at a local network level. NGN planners and implementers focus on two issues concurrently: designing a resilient network that meets and exceeds user requirements at a local, regional, national and international level; and, maintaining local user and services priorities across an extensive NGN network environment.

The purpose of the NGN is to provide highly available and resilient network access, transport and services on a local and national basis, in support of myriad NS/EP scenarios. Availability and resiliency of the NGN will be enhanced over time as the evolution from an overlaid and inter-working network environment into a seamless and functional NGN environment is completed. Success of this migration, including peer-to-peer capabilities, depends on the ability of planners and implementers to continually support user requirements and expectations of service on a geographically dynamic basis.

Networks integrated into the NGN to support NS/EP activities are designed to satisfy user requirements for local network services, directly connected (adjacent neighbor) networks, and other networks as required. Agreed-upon common operational criteria are developed, disseminated and enforced both locally and between adjacent neighboring networks. Common operational criteria focuses on acceptable methods of user authentication, network resource authorization, and precedence, based upon the scope and severity of any NS/EP event at a local, regional national or international level; and successfully bind multiple networks together, as required, into a flexible and highly responsive NGN. End-to-end network availability and service support is achieved a priori by coordination of multiple connected networks, linked together both physically and logically via common operational criteria accepted and enforced among adjacent networks.

Maintaining end-to-end service priority across the NGN is based on supporting homogeneous CoS at a local, regional and national level. Enablement and support of multiple user and services priorities is part of the common operational criteria between connected networks within the NGN. Depending upon the scope and severity of an NS/EP event, local network policy may be supplanted by a common operational criteria agreement to provide connectivity, bandwidth and resource priority to external network users in times of emergency.

Within the NGN it is essential that:

- 1) The NGN meet or exceed user requirements at a local, regional, national and international level, and ensure consistency and continuity of user and services priorities throughout the NGN.
- 2) CoS are defined, based on common operational criteria, and are supported by all applicable network participants within the NGN.

F.3 Important Technologies

The requirements of the various NS/EP user scenarios on NGN will require a variety of technologies—some existent and some emergent. The technologies, protocols and methodologies recommended here are well understood, offering clear benefits that make their use in the NGN highly conceivable and perhaps inevitable.

F.3.1 Implications of the Internet Protocol

The current Internet Protocol Version 4 (IPv4) has served as the underlying protocol for the Internet for almost 30 years. Its robustness, scalability, and range of features are now being challenged by the growing need for new and abundant IP addresses, spurred in large part by the rapid growth of new network-aware terminals and appliances, and IP-based multimedia services, such as online or peer-to-peer interactions and Voice over Internet Protocol (VoIP). Internet Protocol Version 6 (IPv6) is a critical technology that ensures that the Internet can support a continually expanding user community worldwide. This technology will accelerate global broadband deployment, and promote proliferation of IP-connected capabilities

and devices. IPv6 focuses on a number of prominent issues encountered in today's Internet. While the greatly increased addressing capability is a primary benefit, the most important difference between the two protocols lies in with the utility of the expanded address space available in IPv6. By incorporating critical capabilities, such as hierarchical addressing structure, flexible security mechanisms, and user mobility, IPv6 supports new computing and communication models that are difficult to support using the IPv4 protocol. Two features of particular importance to NS/EP users may be the auto-configuration and neighbor discovery capabilities of IPv6, which would enable NS/EP devices to quickly locate other IPv6 devices for call routing and communications. Further the simplified and extensible header in IPv6 also provides NS/EP planners an opportunity to request a certain quality of service. With IPv6, applications and services can be readily developed and deployed, and will function effortlessly, without requiring complex network configurations and routing schemas, cumbersome management supervision, or special server deployments.

F.3.2 Key Benefits of IPv6 Compared with IPv4

F.3.2.1 Expanded Addressing Space

When the IPv4 protocol's address space was first designed in the late 1970s, its exhaustion was regarded as inconceivable. However, due to advances in technology and address allocation practices that did not anticipate a virtual explosion of devices connected to the Internet, the IPv4 address space was rapidly consumed. By 1992, it became apparent that a replacement protocol should be designed. The address space in the IPv6 protocol is 128 bits, supporting 340,282,366,920,938,463,463,374, 607,431,768,211,456 (3.4x10³⁸) possible IP addresses. The IPv4 address space is comparatively small at 32 bits.

F.3.2.2 Highly Efficient Routing Infrastructure

Global addresses used on IPv6 segments of the Internet are designed to create an efficient, hierarchical, and easily summarized topology and routing hierarchy that is based on the common occurrence of multiple Internet service provider levels. On the IPv6 portions of the Internet, backbone routers have smaller routing tables, which correspond with routing formats of the

global Internet service providers (ISPs). Developments in multi-homing show promise for future innovations such as redundancy, load balancing, and network congestion detection and management. A site is considered to be multi-homed when it connects to more than one service provider.

F.3.2.3 Enhanced Security

Private communications over a public medium, including the Internet, require secure services that appropriately protect digital information from being monitored or modified while in transit. Although an IPv4-based standard, known as Internet Protocol security (IPsec), provides security for data packets, use of this standard is optional. As a result, proprietary solutions are prevalent. In IPv6, IPsec support is a requirement of the protocol, providing standards-based network security for devices, applications, and services, while promoting interoperability among differing IPv6 implementations. IPv6 resolves additional security issues that cannot be solved using IPv4.

F.3.2.4 Mobility Support

IPv6 allows network nodes to be highly mobile, permitting arbitrary changes in location on an IPv6 network while maintaining existing connectivity. When a node connected by either IPv4 or IPv6 changes its location in the network, it typically changes its IP address as well. Without mobility support, which is not easily achievable in IPv4, loss of connectivity with peers results. With mobile IPv6 in use, the mobile node is always reachable through one permanent address. A connection is established with a specific permanent address assigned to the mobile node; and remains connected no matter how often the mobile node changes locations or acquire temporary-use addresses. Packets may be routed to the mobile or nomadic node using its permanent address regardless of the node's current point of attachment (i.e., location) to the service network or the Internet. The node (mobile or nomadic) continues to communicate with other nodes, either stationary or mobile, after transferring on to a new link. The movement of a mobile or nomadic node away from its home link, therefore, is transparent to a transport protocol, any higher-layer protocols, and/or applications. The Mobile IPv6 protocol is suitable for mobility across both homogeneous media and heterogeneous media.

For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another, as well as node movement from an Ethernet segment to a wireless LAN cell. The mobile node's IP address remains unchanged regardless of movement. Another example could involve movement and recognition of a device from a home to a mobile environment, or some other nomadic capability the NGN and IPv6 may enable.

Mobile IPv6 protocol addresses network-layer mobility management issues as well. Some mobility management applications, such as handoff among wireless transceivers, which cover only a very small geographic area, are solved using link-layer techniques. For example, in many current wireless LAN products, link-layer mobility mechanisms support handoff of a mobile node from one cell to another, dynamically re-establishing link-layer connectivity to the node in each new location.

F.3.2.5 Other IPv6 Capabilities

Other representative capabilities in IPv6 that support NS/EP requirements are listed below:

- ▶ Multiple IP addresses that disconnect identities and their IP addresses.
- ▶ Improved confidentiality through temporary IP addresses used by key individuals (POTUS) to reduce the likelihood of profiling or tracking their communications.
- ▶ Multiple IP addresses that connect identities, devices and their IP addresses; especially useful for Public Safety NGN capabilities and effective peer-to-peer interactions.
- ▶ Automatic self-configuration and self-healing, permitting a network to be established or re-established rapidly in response to an NS/EP contingency.
- ▶ Mobile IP feature in IPv6 enabled devices to move around the Network, or even into other networks, without losing connectivity (described above).

F.3.2.6 IPv4 to IPv6 Transition Considerations

A transition from IPv4 to IPv6 is not a trivial migration, but is a complex transformation, or evolution, from one network protocol to another. Initial interest in IPv6 in the 1990s was based on a perceived shortage of addressing space and lack of security features available with the IPv4 protocol. Renewed interest in IPv6 today is based on a number of factors, including: leveraging an extensive address space for emerging network applications, enhancing user mobility across multiple networks, and supporting granular quality of service (QoS) capabilities throughout a geographically distributed network, such as the NGN. Transformation planning from IPv4 to IPv6 focuses on supporting both networking protocols concurrently, and today is an essential success factor of NGN implementations. IPv6 is an increasingly significant capability for enterprise networks requiring international connectivity.

Protocol translation and encapsulation, known as tunneling, are two key techniques used to support a mixed protocol (IPv4 and IPv6) operational environment. Therefore, networking equipment in the NGN is required to be dual-stacked, capable of operating as either IPv4 or IPv6 compliant. Emerging IPv6 networks are, and can continue to be, inter-linked with legacy IPv4 networks using either protocol translation or tunneling mechanisms to route IPv6 traffic in IPv4 packets. Network equipment interoperability and open standards-based compatibility are crucial in mixed IP protocol operational environments

Maintaining consistency and continuity of common operational criteria in a mixed protocol environment is a complex challenge, requiring deliberate coordination and management of authentication, authorization, priority and service class credentials among networks using either the IPv4 or IPv6 protocol. Seamless network-to-network trust relationships, based on the use of centralized registration databases or distributed user credentials, are essential among constituent networks comprising the NGN to facilitate unimpeded access to network resources, once initial user authentication and network authorization transactions are successfully performed.

NS/EP service requirements for the NGN are readily supported by migrating to an IPv6 transport backbone and IPv6-enabled applications. As noted above, IPv6 provides enhanced network security via IPsec and additional integrated features of the protocol. The dynamic mobility capabilities of IPv6 support ad hoc networking applications and are readily adaptable to resilient peer-to-peer network designs. Additional security applications and software can be applied to trusted users via network edge or device to further enhance security measures.

Within the NGN it is essential that:

- 1) The NGN be planned, designed and implemented as a mixed protocol operational environment, capable of supporting current and anticipated user requirements with either IPv4 or IPv6 network connectivity.
- 2) Trust relationships to maintain and preserve the consistency and continuity of common operational criteria, including authentication, authorization, priority and service class definitions, throughout the NGN, are developed and implemented seamlessly from end to end.

F.3.3 Peer-to-Peer Networking

Peer-to-peer (P2P) networking offers a distributed alternative to legacy centralized network structures, and offers value during times of network stress or compromise to infrastructures or services. Characteristic features of P2P networking include:

- Applications are available when the network path between peers is available. No other supporting infrastructure is required to enable this connectivity. This allows a specific group of NS/EP users to fully utilize P2P-based applications even though this user community may be isolated from the greater NGN. For example, emergency workers, using mobile devices in a devastated area, are readily able to send and receive text and images between themselves on an isolated network.
- Instant messages (IM) using conventional messaging service require establishment of two

sessions, with one between the sender and the messenger cloud and a second between the recipient and the messenger cloud. By use of peer-to-peer networking, bandwidth use is highly efficient, in that the IM session message traffic passes only between the connected peers.

- ▶ Communication between two entities, without connectivity to intermediaries, increases overall confidentiality. As an example, two NS/EP users on wireless VoIP phones are able to converse directly without requiring any additional support infrastructure. Another benefit of this scenario is lower latency between local and remote users due to the shorter distances required to connect them as peers. Note that P2P application may involve policy and management decisions of command entity due to resource allocation and traceability/dispatch needs. This is a typical case for Public Safety jurisdictional networks and incident command.

P2P communication techniques can be applied at the application level or at the network level. When used at the application level, two parties can communicate with each other as long as they have network connectivity with each other, without dependence on other infrastructure services. The network connectivity may be provided by centralized infrastructure through which messages are routed to the two peers.

Alternatively, the two peers may have network level connectivity with each other that does not require or depend on centralized infrastructure. In such cases the connectivity may be provided by a mesh or ad hoc network composed of devices connected using P2P communication techniques. For this reason, Common Operational Criteria among providers of constituent mesh and overlay networks should be established, as an integral component of an overarching NGN security policy. (See Report, Section 6.7.)

Network level P2P communication frameworks have the advantage of being fully distributed, scalable, and cost-effective to deploy on either a short- or long-term basis.

Peer-to-peer networks, elements and systems should play a key role in NGN end-to-end service for dedicated, mobile, and ad hoc users supporting NS/EP activities.

Within the NGN it is essential that:

- 1) Peer-to-peer networks, elements and systems are integrated into the NGN long-term system design and standardization strategy to ensure effective connectivity for dedicated, mobile and ad hoc users supporting NS/EP activities.
- 2) Common operational criteria among constituent peer-to-peer and overlay networks supporting NS/EP activities be established, disseminated and enforced, as an integral component of an overarching NGN security policy.

F.3.4 Meshed Network Environments

Already recognized as an important component of the NGN, it is important to consider that P2P and IPv6 are easily optimized in mesh networking environments.

Advantages of mesh networks include:

- ▶ No single point of failure, which enhances resiliency; A percentage of the network remains intact and usable even though large segments of the overall meshed architecture is rendered unusable; and
- ▶ Easily configured, in that the incremental and distributed nature of a mesh network is more readily configured and built-up incrementally, especially in locations without preexisting infrastructure.

In a typical NS/EP scenario, individual networks are integrated into a de facto full or partial “mesh” of wireline, wireless, satellite, private networks and worldwide Internet elements, as applicable and appropriate to mission. An NS/EP contingency requires heterogeneous environments to quickly and effectively support high availability, resiliency and security from an end-to-end services perspective. However, to support communications in these scenarios, a consolidation of myriad homogeneous (and often single-purpose) networks optimized for a dedicated user community is

required. Methods for authenticating users, reserving network resources and bandwidth, assigning priority classes, enforcing end-to-end security policy, and determining optimal routes for data and management traffic among networks vary greatly. In the NGN, interconnectivity is based on deployment of an overlay, peer or hybrid architecture to support services end-to-end across multiple networks.

Current national and international standardization activity is examining the potential importance of mesh networking, especially for first responders.

F.3.5 Role of IPsec

The evolution of the NGN is based predominantly on the use of common elements like Internet Protocol (IP). IPsec is a security mechanism designed specifically for enhancing the security of the IP. It provides increased security capabilities in support of NS/EP event scenarios. IPsec isolates and protects user services and applications on the NGN, ensures authenticated access to services, ensures the authenticity of communication, preserves the integrity of messages and supports communications confidentiality.

The following capabilities of IPsec are available singly or in combination:

- User authentication;
- Device authentication;
- Integrity and authenticity of communication; and
- Confidentiality of communication.

F.3.6 Combined Use of Technologies

The technologies described above are individually useful but become much more so when used in combination. An example includes a set of users entering an area without infrastructure. Their user devices will auto-configure themselves and discover each other (e.g., a specific IPv6 characteristic) and can begin to communicate using P2P or other applicable connections. Similarly, the use of IPsec to preserve confidentiality and authentication of communication becomes more important in a meshed network environment, for example, where the possible

paths between two or more entities are numerous. In such situations, it is difficult to establish and ensure a level of trust among many connected devices. Support by the Federal Government Science and Technology community of full scale demonstrations of how these technologies can be used to enhance NS/EP capabilities within the NGN is vital to rapid progress and establishment of best practices for those with NS/EP requirements.

F.3.7 Transition and Interaction of Directory Services

Further as the telecommunications world evolves another critical requirement will be the capability to enable communications between the “legacy” and the NGN environments. VOIP subscribers connecting with tradition “plain old telephone systems” (POTS) users is a current example of an application that operates end-to-end and crosses both environments. The directory services associated with routing and electronic numbering are developing between these environments and the interoperability challenge is depicted in the following diagram.³

Another recent example of a critical public safety service of the POTS environment that will need to be available in the NGN environment is enhanced 911 (E911) emergency services.⁴ This is a precedence setting example of how critical existing services that we rely upon for public safety will need to be developed for the NGN environment. Additionally, in 2003, the FCC recognizing the need to speed full implementation of E911 and greater coordination among all stakeholders, undertook a “Coordination Initiatives” to complement current efforts by involved parties to speed and rationalize the E911 deployment process, and to ensure that the all parties and the public have clear expectations about the roles of the respective parties and deployment plans. This further provides insight on scope of coordination efforts that will be required for assuring the NGN can meet NS/EP community needs.

Such coordination will be required to establish electronic numbering (ENUM), or telephone number mapping, either at carriers, infrastructure level or both, to meet the public/end user needs within the NGN for integrated services and mapping to the legacy public switched telephone network (PSTN) environment, as PSTN

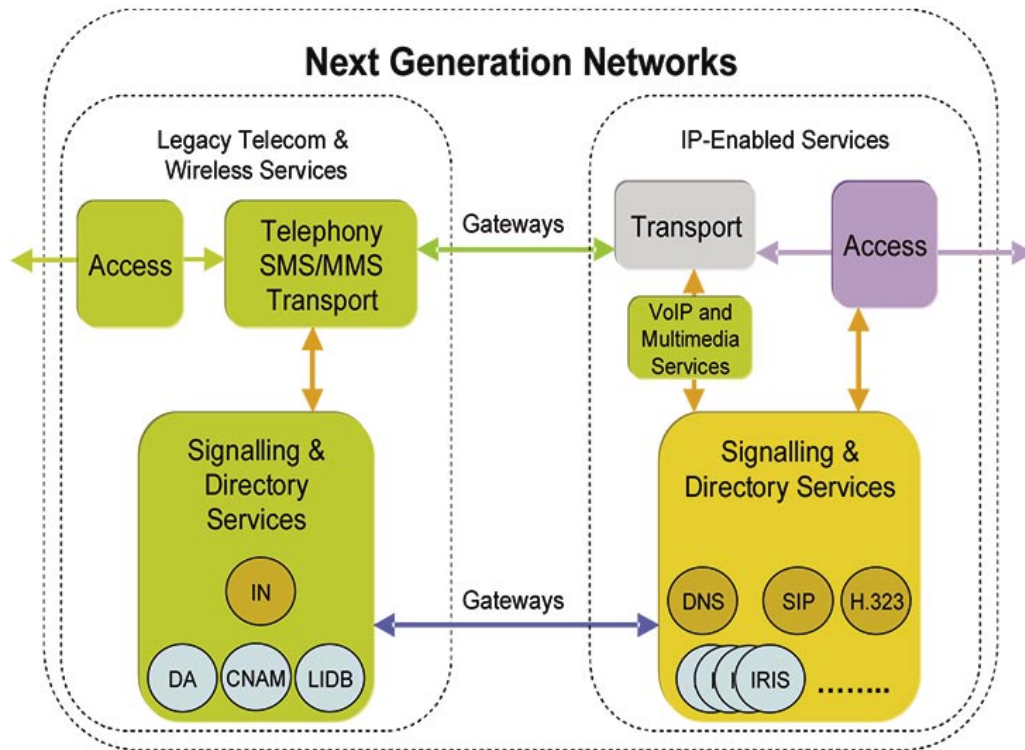


Figure F-3 Interoperability: Signaling & Directory Considerations

inter-working will be required for a long time. Facilitation activities and coordination among stakeholders will be required to achieve such integrated solutions for the NGN, along with necessary standards.

F.4 Conclusion

As the NGN is in an early implementation stage, actual access, transport, and service availability today may not fully support anticipated NS/EP user requirements. It is a responsibility of the Federal Government to ensure that NS/EP requirements are articulated and coordinated among its users, standard bodies and the broad range

of service providers. In order for the NGN to broadly meet essential NS/EP community requirements in a consistent, continuous and reliable manner on an end-to-end basis, common operational criteria must be defined and adopted by entities supplying network access, transport and infrastructure services for this community.

Appendix G

Systematic Assessment
of NGN Vulnerabilities

Systematic Assessment of NGN Vulnerabilities

G.1 Background

This Appendix provides additional background [developed by the Vulnerabilities and Threat Modeling Working Group (VTMWG)] on NGN vulnerabilities relevant to the conclusions and recommendations of the Next Generation Networks Task Force (NGNTF), which are contained in the main body of the Report.

G.2 Systematic Assessment

The vulnerabilities of the NGN were studied systematically⁹ to determine the vulnerabilities of the NGN; the analysis included:

- ▶ A suitable framework for vulnerability assessment.
- ▶ A comprehensive list of intrinsic vulnerabilities of the NGN ingredients.
- ▶ Relevant trends that affect the exposure of the vulnerabilities.
- ▶ Evaluation of significance of each vulnerability in the NGN.

The framework selected to study NGN vulnerabilities was one already regularly used in several industry-government-academic fora.⁶ The framework consists of the eight ingredients with which the communications infrastructure is built. This framework is comprehensive in the sense that all the things needed for the full operation of a communications network are included. As shown in Figure G-1, below, it also recognizes the role of other infrastructures.

Figure G-2, below, is provided for explanatory purposes. It is an example table of the vulnerabilities lists that are provided in the following pages for each of the eight ingredients. The first column provides a comprehensive list of the vulnerabilities for that ingredient. Vulnerabilities are defined as “a characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.”⁸ The second column indicates the exposure of each vulnerability in the NGN relative to legacy networks. The third column indicates the impact of significant trends, which are listed below each table.

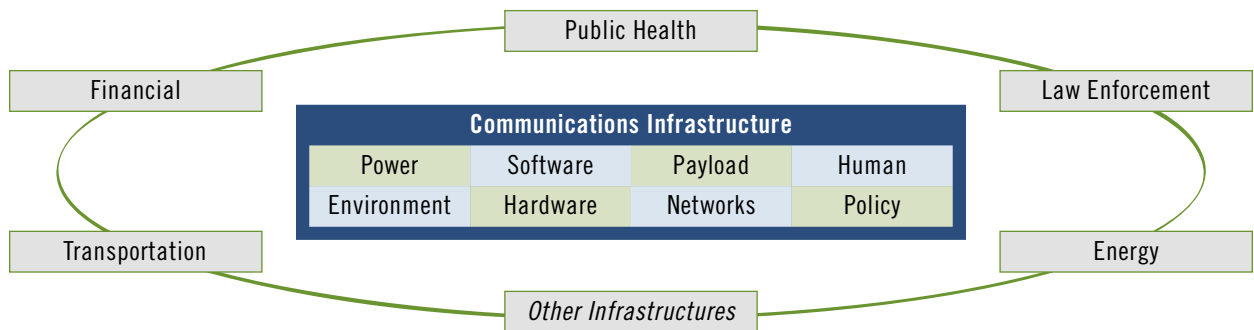


Figure G-1 Communications Infrastructure Ingredients and Dependencies⁷

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
attribute i	-	a
attribute ii	=	a, b
attribute iii	+	n/a

* Trends from the NGNTF VTMWG

Figure G-2 Example Ingredient Vulnerability List

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
uncontrolled fuel combustion	=	
fuel contamination	=	
fuel dependency	=	
battery combustion	=	12
battery limitations	=	6
battery duration	=	1
maintenance dependency	=	1, 4, 5, 7
require manual operation	=	4
power limitations	=	5, 8
frequency limitations	=	2
susceptibility to spikes	=	
physical destruction	=	7

* Trends from the NGNTF VTMWG

G.2.1 Power

The Power ingredient includes the internal power infrastructure, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.

Significant Trends Related to NGN Power Vulnerabilities

- 1) Network access devices are no longer powered by network elements (many devices do not have back-up power).
- 2) Increased reliance on A/C, which has more components.
- 3) Higher voltage UPS systems have more cells in series.
- 4) Higher voltage increases safety and training attention.
- 5) Increased dependence on back-up power for cooling.
- 6) A/C UPS back-up systems are currently not highly reliable.
- 7) Increased regulation from local codes (e.g., sprinklers, battery disconnect switches) decreases reliability.
- 8) Increased use of 208/240 V power systems because of higher density in data centers.
- 9) Decreasing size of many locations suggests lower engineering level of back up power.
- 10) Increased use of embedded systems (“boxes” used as commodities).
- 11) Decreased power consumption.
- 12) Battery combustion concern is decreasing do to better battery design and technology.
- 13) Increasing use of public and remote sites.
- 14) Increasing use of network-based, software-controlled, power management systems.

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
accessible	=	3, 6
exposed to elements	=	2, 6
dependence on other infrastrucures	=	2, 4, 6
contaminate-able	=	6
subject to surveillance	=	2, 3, 6
continuously being altered	=	5, 6
identifiable	=	1, 2, 3
remotely managed	=	2, 3, 4
non-compliance with established protocols and procedures	=	4, 6

* Trends from the NGNTF VTMWG

G.2.2 Environment

The Environment ingredient includes buildings, trenches where cables are buried, space where satellites orbit, locations of microwave towers and cell sites, and the ocean where submarine cables reside.

Significant Trends Related to NGN Environment Vulnerabilities

- 1) Some environments may be less significant with broad mesh distribution of functionality.
- 2) Increasingly mobile.
- 3) Increasingly be virtual.
- 4) Increasingly have cooling challenges.
- 5) Increasingly may not have a back-up.
- 6) Increasing reliance by some on “hot spots”—more public and less under control.

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
chemical (corrosive gas, humidity, temperature, contamination)	=	11
electric (conductive microfiber particles – carbon bombs)	=	
radiological contamination	=	
physical (shock, vibration, strains, torque)	=	6
electromagnetic energy (EMI, EMC, ESD, RF, EMP, HEMP, IR)	+	12
environment (temperature, humidity, dust, sunlight, flooding)	=	3
life cycle (sparing, equipment replacement, ability to repair, aging)	=	7
logical (design error, access to, self test, self shut off)	+	4, 6, 9, 10, 15, 16

* Trends from the NGNTF VTMWG

G.2.3 Hardware

The Hardware ingredient includes the hardware frames, electronic circuit packs and cards, and metallic and fiber optic transmission cables and semiconductor chips.

Significant Trends Related to NGN Hardware Vulnerabilities

- 1) More portable hardware introduces more dependencies on various power capabilities.
- 2) Widespread impact of a single mode of failure more likely with increasing use of common hardware across vendors.
- 3) Increasing density of logic generates more heat.
- 4) Sabotage or malicious design insertion may be more likely due to increasing trend of offshore outsourcing.
- 5) Increasing capacity of transmission facilities.
- 6) Increasing capacity of single devices increases their value and importance.
- 7) More rapid technology turnover (decades to years).
- 8) Increasing storage of sensitive information on hardware.
- 9) May be more common for hardware to include tamper detection and tamper response.
- 10) Increasing ability to access and control remotely (in-band control considerations).
- 11) Increasing use of non-NEBS compliant devices.
- 12) Increasingly smaller footprint results in smaller gaps between components on circuit cards greater challenge for short circuits and physical integrity.
- 13) Fewer large, centralized systems being replaced with more, smaller distributed systems.
- 14) End user equipment is becoming much more sophisticated.
- 15) Increasing complexity of devices.
- 16) Increasing availability of capability to do firmware and microcode updates.

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
ability to control (render a system in an undesirable state, e.g., confused, busy)	+	5, 18, 22, 23
accessibility during development (including unsegregated networks)	+	8, 11
accessible distribution channels (interception)	+	5, 8, 18, 23
accessibility of rootkit to control kernel/core	+	5
developer loyalties	+	11, 18
errors in coding logic	+	11, 13, 14
complexity of programs	=	13, 14, 18
discoverability of intelligence (reverse engineer, exploitable code disclosure)	+	5, 6, 29
mutability of deployed code (patches)	+	8, 19, 21, 23, 24
incompatibility (with hardware, with other software)	+	15, 17 to 20, 26

* Trends from the NGNTF VTMWG

G.2.4 Software

The Software ingredient includes the physical storage of software releases, development and test loads, version control and management, and chain of control deliver.

Significant Trends Related to NGN Software Vulnerabilities

- 1) Increased risk of over-the-air exploitation (re-keying of encryption for end user radios, gain access or intercepting upgrades, change user profile/identity).
- 2) Increasing use of wireless-installed software.
- 3) Increased use of artificial intelligence (rules-based expert systems).
- 4) Increased risk of widespread logical single point of failure.
- 5) More use of embedded operating systems (can be altered with in-band control).
- 6) Prevalence of worms and viruses common to PCs will increasingly be used as an attack vector for public networks.
- 7) More authentication occurring at the application layer.
- 8) More use of open source systems (tampering more of a concern)—move away from propriety code.
- 9) Increasing risk of confidentiality failure (leak of information...who called whom).
- 10) Increasing availability of malware.
- 11) Increasing exposure through offshore development.
- 12) Increasing concern of mis-authorization elevating someone's privileges.
- 13) Comprehensive inspections continue to be impractical—potential impact is getting worse.
- 14) Software testing tools are improving.
- 15) Continued need to support legacy code (transition issue).
- 16) New releases increasingly have ability to fall back on previous version.
- 17) Increasing exposure of legacy code to new unconstrained environment.

- 18) Shift toward service-oriented architectures (control given to many new parties, complexity of possible permutations of software component assembly is too large).
- 19) Patch management has a bigger impact because more of the network is based on software—more far reaching impact, more failure mode effects analysis needed.
- 20) Configurability of software maybe more difficult.
- 21) Network is a system of systems—patching can have large cascading effects.
- 22) Increasing role of traffic restrictions—software will control what is and is not supposed to be there (priority services).
- 23) Increasing need for prioritized patch messages (fix a collapsed network using in-band management).
- 24) Anticipated increased use of software-controlled radios.
- 25) More capable end-user devices.
- 26) Increasing complexity of interfaces between systems More incentive for people to learn the open protocols.

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
unpredictable variation	+	1, 6, 8, 10
extremes in load	+	1, 2
corruption	=	5, 7, 8, 10
interception	=	2, 3, 4, 7
emulation	+	2, 3, 4, 7
encapsulation of malicious content	+	2, 7, 8
authentication (mis-authentication)	+	2, 3
insufficient inventory of critical components	=	1, 2
encryption (prevents observability)	+	12

* Trends from the NGTF VTMWG

G.2.5 Payload

The Payload ingredient includes: the information transported across the infrastructure; traffic patterns and statistics; information interception; and, information corruption. It includes both normal and signaling and control traffic.

Significant Trends Related to NGN Payload Vulnerabilities

- 1) Includes many types of services (voice, data, video).
- 2) Increasing sophistication regarding prioritization.
- 3) IP address tracking allows identity in header.
- 4) Increased spoofing concerns.
- 5) Increased concern for NS/EP needs to get a message through with “one shot”.
- 6) New capabilities to control and provision bandwidth dynamically.
- 7) Co-mingled traffic and control messages.
- 8) Session persistence permits session hijacking.
- 9) New challenges for AJ/LPI/ LBD (anti-jamming, low probability of intercept, laser beam detection) effects on NS/EP communications.
- 10) More variation in Quality of Service.
- 11) Increased concern of channel hijacking.
- 12) Increasing challenge for preventing a negative impact from concealed messages in encrypted or otherwise hidden content.
- 13) Service providers may give out information that can be used against its own networks and there is much data to be mined.

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
capacity limits	+	4, 9, 12, 14
points or modes of failure	=	2, 3, 6, 7, 14
points of concentration (congestion)	-	3, 5, 6, 14
complexity	+	1, 2, 5, 6, 7, 9
dependence on synchronization	=	2, 7, 20
interconnection (interoperability, interdependence, conflict)	+	2, 8, 10, 13, 14
uniqueness of mated pairs	-	13
need for upgrades and new technology	+	5, 12, 14, 15, 19
automated control (*via software)	+	1, 5, 6, 11
accessibility (air, space or metallic or fiber)	+	4, 8, 12
border crossing exposures	=	4, 8

* Trends from the NGNTF VTMWG

G.2.6 Networks

The Network ingredient includes: the configuration of nodes and their interconnection; network topologies and architectures; various types of networks, technology, synchronization, redundancy, and physical and logical diversity; and network design, operation and maintenance.

Significant Trends Related to NGN Network Vulnerabilities

- 1) Shift from reliance on silicon to software.
- 2) Departure from deterministic to non-deterministic path control.
- 3) Shift from circuit to packet entails losing a dedicated path.
- 4) Increasing presence of wireless increases exposure to blocking and sniffing.
- 5) New capabilities to control and provision bandwidth dynamically.
- 6) New real-time reconfiguration of network resources.
- 7) Increased diversity of network practices of interconnected networks.
- 8) Increased sensitivity of AJ/LPI/ LBD (blocking, interception) effects on NS/EP communications.
- 9) More variation in Quality of Service.
- 10) De-segregated traffic and control messages in payload.
- 11) Increased use of artificial intelligence.
- 12) More diverse modes of access.
- 13) Non-homogeneous distribution of vulnerabilities.
- 14) High bandwidth and powerful computing capabilities are increasingly common.
- 15) Increasing sophistication of PSAP communications.
- 16) Increasing concern over channel hijacking.
- 17) Emergence of IPv6.
- 18) Increasing use of grid and peer to peer networking (versus client-server architecture).
- 19) More security exploits require more software patching.
- 20) Increasing concern over being used for harm (GPS, end user device detonation triggers).

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
physical (limitations, fatigue)	=	1, 6
cognitive (distractibility, forgetfulness, ability to deceive, confusion)	=	1, 3, 4, 7
ethical (divided loyalties, greed, malicious intent)	=	2, 5, 6
user environment (user interface, job function, corporate culture)	=	1, 5, 6
human-user environment interaction	=	2, 3, 6

* Trends from the NGNTF VTMWG

G.2.7 Human

The Human ingredient includes: human involvement throughout the entire lifecycle of activities related to the communications infrastructure (design, implementation, operation, maintenance and de-commissioning); intentional and unintentional behaviors; limitations; education and training; human-machine interfaces; and, ethics and values.

Significant Trends Related to NGN Human Vulnerabilities

- 1) Competitive challenges result in increasing work overloads.
- 2) Increased use of biometrics (can introduce higher rejection or false positive rates).
- 3) Complexity takes longer time to progress along learning curve.

- 4) Deployment of technology increasing outpaces availability of accurate and complete documentation.
- 5) Increasing use of wireless connectivity increases dependence on authentication and authorization.
- 6) Increased frequency of virtual and remote teams weakens social cohesion (emergency response teams, trusted environments).
- 7) Training and procedures remain key to familiarity.

Vulnerability	Presence in NGN vs Legacy	Affected by Trend*
Lack of ASPR (agreements, standards, policies, regulations)	+	1, 4, 5, 7, 9, 15
Conflicting ASPR	+	3, 4, 5, 7, 13, 15
Outdated ASPR	+	1, 4, 5, 7, 8, 15
Unimplemented ASPR (complete or partial)	+	6, 8, 9, 10, 11, 13
Interpretation of ASPR (mis- or multi-)	+	9, 13, 15
Inability to implement ASPR	+	3, 6, 9, 10
Enforcement limitations	+	2, 3, 15
Boundary limitations	+	2, 3, 6, 15
Pace of development	+	1, 4, 5, 8, 12, 13
Information leakage from ASPR processes	=	2, 14
Inflexible regulation	=	2, 7, 8, 11, 15
Excessive regulation	-	2, 8, 10, 15
Predictable behavior due to ASPR	=	7, 14
ASPR dependence on misinformed guidance	=	8, 9, 13
ASPR ability to stress vulnerabilities	+	4, 7, 13
ASPR ability to infuse vulnerabilities	+	3, 4, 13
Inappropriate interest influence in ASPR	=	2, 9

* Trends from the NGNTF VTMWG

G.2.8 Policy

The policy ingredient includes: behaviors between entities, namely agreements, standards, policies and regulations (ASPR); national and international scopes, as well as Federal, State and local levels; other legal issues; and any other arrangement between entities, including industry cooperation and other interfaces.

Significant Trends Related to NGN Policy Vulnerabilities

- 1) Increasing need to redefine prioritization criteria (e.g., other infrastructures that support NS/EP).
- 2) Goal of protecting U.S. network is harder to distinguish with global interconnectivity of NGNs.
- 3) Attribution and retribution framework is missing.
- 4) Loss of functionality when inter-working between NGN and legacy networks.
- 5) Need for mapping the multiple NGN priority levels to the one level in the legacy networks and vice versa.
- 6) Lack of an agreement to carry an NS/EP call (wireless roaming).
- 7) Priority handling of 911 calls could drown NS/EP calls.
- 8) Migration from Time Division Multiplexing (TDM) to IP networks.
- 9) More and smaller service provider and network operators.
- 10) Decreasing capital investment availability.
- 11) Multiple modalities (video, data, voice).
- 12) Rapid deployment of IP replacing TDM, without ASPR.
- 13) Rapidly increasing complexity of technical solutions.
- 14) More ASPR work published on the Internet.
- 15) Diverging views globally on the level of regulation needed for NGNs/ the Internet.
- 16) Increasing use of wireless spectrum.

Appendix H

NGN Threat Analysis

NGN Threat Analysis

H.1 Background

This Appendix provides additional background on threats to the NGN relevant to the conclusions and recommendations of the Next Generation Networks Task Force (NGNTF), which are contained in the main body of the Report.

H.2 Threat Analysis

Threats to the NGN were studied using NGN-specific threat modeling⁹ approach focusing on both NGN and national security and emergency preparedness (NS/EP) communications with a focus on cyber attacks, but which also examined blended cyber and physical attacks on the NGN. To conduct a threat analysis for the NGN environment, the NGN scenarios described above were taken and broken down into an appropriate collection of user classes that could be analyzed in a more granular fashion. These user classes represented unique user types and requirements¹⁰ within each NGN scenario context.

Next, four levels of threat classes were identified based on motivations and capabilities, ranging from Class A, a nation-state or agency with extensive resources, to Class D, an individual with limited resources. These threat classes were evaluated not just based on resources but also on their motivations and their anticipated and developed cyber and kinetic capabilities (e.g., computer network attack, electronic warfare, psychological operations, military deception, kinetic).

As a final step is the threat modeling exercise, the NGN scenarios, user classes, and requirements were combined with the threat landscape and an analysis of susceptibility a particular user class (in the context of an NGN scenario) to the various threat actor classes was performed. The result was enumeration of the threat types to which each user class was likely to be susceptible. The analysis addressed threats to the confidentiality, integrity, and availability of information or services in an NGN environment. The threat types were based on the STRIDE classification method proposed by Howard and LeBlanc.¹¹ STRIDE denotes Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Escalation of Privilege. The threat analysis for the

NGN environment and scenarios was primarily focused on cyber and/or blended cyber/kinetic attacks. The result of this exercise was a matrix detailing the anticipated and likely threats for each user class within the context of an NGN NS/EP scenario. In this analysis, several threat trends surfaced.

H.2.1 Widespread Susceptibility

Most user classes were susceptible to significant threat types from virtually every threat actor class. For example, in the Continuity of Government scenario, information disclosure and denial President's National Security Telecommunications Advisory Committee of service are significant threats to all user classes including the National Command Authority (NCA). In addition, the most secure NCA mechanisms (e.g., nuclear launch) may be very unlikely to be threatened but other operational functions, such as emergency response authority, may be highly susceptible to a wide range of threat types.

H.2.2 Threat Actor Convergence

Due to the complex web of relationships between threat actors, the threat landscape has become converged leaving old methods of threat analysis potentially obsolete. For example, the growing financial motivation for cyber crimes has overshadowed motivations around personal fame and reputation for individual hackers. The likelihood of collaboration across threat classes is extremely high. For example, a nation-state, foreign intelligence service, terrorist group, or organized crime group could employ an individual hacker who is motivated by financial gain but does not necessarily share his employer's motivations and/or ideological views. Conversely, an individual hacker with no affiliation to a nation state or terrorist group might be sympathetic to the political or ideological cause and become a voluntary agent in the furtherance of that cause. Finally, the insider threat is not a standalone threat class but one that crosses all threat classes —there can be insiders in every scenario that are employed by any threat actor.

H.2.3 Network Convergence Threat Impacts

Convergence in the NGN environment will create an inherently more complex environment where various "planes" (i.e. control, data, user, etc.) are merged. Convergence creates a scenario where the threats and

adversaries of the individual converged systems are inherited by the entire converged system. For example, a threat scenario unique to and perhaps well known to the public switched telephone network (PSTN) and not present for the Internet, would now be faced by all in the converged environment. In addition, traditional PSTN network security focus is only put on the network elements. In a converged network, the threat to data integrity/validity must also be examined in addition to threats to network elements. Convergence will present a greater threat to control systems as

control and management networks via wireless, PSTN, and the Internet are converged. Finally convergence, legacy network interoperability requirements, the infancy of converged network management tools, and other factors in the NGN environment have made network management in the NGN environment increasingly difficult.¹²

The NGN Scenario Threat Profile Matrix, shown below, details anticipated threats for each user class within the context of an NGN NS/EP scenario.

NGN Scenario: Continuity of Government

Threat Classes	Motivations	Capabilities
A - Nation State/Agency (\$1012)	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B - Ideological/NGO (\$109)	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (\$106)	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (\$103)	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
National Command Authority	Survivability Interoperability Broad Application Support Authentication Priority over Non-NS/EP Mobility NLA and/or Non-traceability Fail-secure only Content-aware security Emergency Alerts	Information Disclosure Denial of Service	Information Disclosure Denial of Service	Information Disclosure Denial of Service	None
Departmental-Level (e.g. DoD, DoS, DHS)	Survivability Interoperability Broad Application Support Authentication Priority over Non-NS/EP Mobility NLA and/or Non-traceability Fail-Safe and/or Fail-secure Communities of Interest Content-aware security Emergency Alerts	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service	Denial of Service
Regional, State & Local	Broad Application Support Interoperability Authentication Priority over Non-NS/EP Mobility Fail Safe (defaults to available) Communities of Interest Content-aware Security Emergency Alerts	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service

NGN Scenario: Continuity of Government – *continued*

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
CI Provider (Private or Public sector)	Survivability Interoperability Authentication Internal priority over Non-NS/EP Mobility Fail Safe and Fail Secure Content Aware Security	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service
General Public	Multi-lingual/Accessibility Broad platform support Broad Authentication Support Mobility Fail Safe Only Emergency Alerts	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

NGN Scenario: Critical Government Networks

Threat Classes	Motivations	Capabilities
A - Nation State/Agency (\$1012)	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B - Ideological/NGO (\$109)	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (\$106)	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (\$103)	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Financial Transaction Networks (e.g. FedWire)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Mobility Fail secure Content-aware security Services Restorability Secure networks International connectivity Interoperable Scalable bandwidth Reliability/Availability Network Location Awareness Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service

NGN Scenario: Critical Government Networks – *continued*

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Government Operations Command and Control (e.g. FAA Air Traffic Control)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Fail safe Content-aware security Services Emergency alerts Scalable bandwidth Reliability/Availability Restorability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service
Intelligence Networks (SIPR, JWICS, etc.)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Mobility Network-based location Awareness and/or nontraceability Fail secure Communities of interest Content-aware security Services Restorability International connectivity Scalable bandwidth Reliability/Availability Affordability Secure Networks	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service	None	None
Information Sharing Networks (HSIN, HSIN-Secret, CWIN, etc.)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Mobility Multi-lingual/Accessibility Fail secure Communities of interest Content-aware security services Emergency alerts Restorability Enhanced priority treatment Secure networks International connectivity Scalable bandwidth Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service

NGN Scenario: Critical Infrastructure – Control Systems (e.g., Supervisory Control and Data Acquisition, Process Control Systems, Digital Control Systems)

Threat Classes	Motivations	Capabilities
A - Nation State/Agency (\$10 ¹²)	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B - Ideological/NGO (\$10 ⁹)	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (\$10 ⁶)	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (\$10 ³)	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Control Systems Management Entity (e.g., data historian server, application server, human machine interface, energy management system, operations support systems)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Fail safe Emergency alerts Restorability Secure networks Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service
Control Systems Network	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Fail safe Restorability Secure networks Ubiquitous coverage Scalable bandwidth Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service
Control Systems Endpoint (e.g., program logic controller, remote terminal unit, sensor, switch/relay)	Survivability Broad platform support and interoperability Strong, usable network authentication Priority over non-NS/EP Fail safe Emergency Alerts Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service

NGN Scenario: Public Safety

Threat Classes	Motivations	Capabilities
A - Nation State/Agency (\$10 ¹²)	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B - Ideological/NGO (\$10 ⁹)	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (\$10 ⁶)	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (\$10 ³)	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Emergency Responder (e.g., Police, Fire, EMS, hospitals)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Mobility Network-based location awareness Fail safe Communities of interest Content-aware security services and/or transparency Emergency alerts Restorability Ubiquitous coverage International connectivity Scalable bandwidth Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Repudiation Information Disclosure Denial of Service
Government Public Safety Leadership (e.g., elected officials and staff)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Mobility Fail safe Communities of interest Content-aware security services Emergency alerts Restorability Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Information Disclosure Denial of Service	Information Disclosure Denial of Service

NGN Scenario: Public Safety – *continued*

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Media (e.g., TV, radio, print)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Mobility Multi-lingual/accessibility Relative priority Fail safe Communities of interest Emergency alerts Restorability Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service
Emergency Communication Networks (e.g., E-911, PSAP, WPS, SHARES)	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Mobility Multi-lingual/Accessibility Network-based location estimation Fail safe Emergency alerts Ubiquitous coverage International connectivity Scalable bandwidth Broadband service Reliability/Availability Restorability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege
General Public	Broad platform support and interoperability Broad application and datatype support Mobility Multi-lingual/Accessibility Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

NGN Scenario: General Public/Home User

Threat Classes	Motivations	Capabilities
A - Nation State/Agency (\$10 ¹²)	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B - Ideological/NGO (\$10 ⁹)	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (\$10 ⁶)	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (\$10 ³)	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Roaming/Nomadic (e.g., hotspot, wireless)	Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Mobility Multi-lingual/Accessibility Network-based location estimation Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege
Home-based	Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Mobility Multi-lingual/Accessibility Network-based location estimation Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

NGN Scenario: General Public/Home Use – *continued*

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Home-based	Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Mobility Multi-lingual/Accessibility Network-based location estimation Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege
Privileged NS/EP User Outside of COG/CGN Scenario	Survivability Broad platform support and interoperability Broad application and datatype support Strong, usable network authentication Priority over non-NS/EP Mobility Fail Safe and/or fail secure Communities of interest Content-aware security Emergency alerts Secure networks Ubiquitous coverage International connectivity Scalable bandwidth Broadband service Reliability/Availability Non-traceability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service	Information Disclosure Denial of Service

Notes

1. Threat Classes
 - a. Threat classes are denoted based on their intentions/motivations and capabilities. In addition, a descriptive resource classification is used referring to the dollar value potential for a given class (e.g. \$1012 for a nation-state).
 - b. A certain degree of overlap in threat classes is understood and accepted as part of the analysis.
2. Threat Capabilities Definitions
 - a. CNO - Computer/Network Operations (includes computer/network attack – CNA, computer/network exploitation – CNE, and computer/network defense – CND)
 - b. EW - Electronic Warfare (including directed and non-directed energy weapons)
 - c. PO - Psychological Operations (including social engineering, extortion, etc.)
 - d. MILDEP - Military Deception (i.e. counter intelligence, counter-counter intelligence, etc.)
 - e. Kinetic (Physical attack, damage, degradation, destruction, etc.)
3. Threat Type/Classification
 - a. Threats to Confidentiality, Integrity, and Availability of information or service
 - b. STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Escalation of Privilege
 - c. Threat analysis is primarily focused on cyber and/or blended cyber/kinetic attacks.
4. Requirements
 - a. Requirements used are derived from the following two sources and several overlaps exist between the two taxonomies.
 - i. NSTAC NGNTF Scenario and User Requirements Working Group (SURWG)
 - ii. Federal Enterprise Architecture Functional Requirements
5. Threat Applicability to Requirements
 - a. For a given threat type (STRIDE) there may or not be applicability to a specific requirement. Further analysis would be required to specify which of the requirements for a given user class would be impact by a given threat.

Appendix I

NGN and National Security
and Emergency Preparedness
Agreements, Standards,
Policies, and Recommendations
Ecosystem

NGN National Security and Emergency Preparedness Agreements, Standards, Policies, and Recommendations Ecosystem

Type of ASPR	Body	Working Party	Work Description
International NGN Technology Standards	ITU-T	SG 2, 13, 16 and 19	<ul style="list-style-type: none"> ▶ Emergency Communications ▶ SG 2 is developing the International Emergency Preparedness Scheme (IEPS) requirement
		SG 11	▶ International Emergency Call Priority
	ITU-R	SG 8 (WP8F)	<ul style="list-style-type: none"> ▶ Emergency Calling and Priority Treatment ▶ Geographic Location/Privacy for IMT-2000-ADVANCED
	GSC	GTSC/GRSC	<ul style="list-style-type: none"> ▶ Emergency Communications for Public Protection and Disaster Relief ▶ Crash Notification and PSAP/Public Communication
	ETSI/TIA	MESA	▶ Broadband Public Safety Partnership Project for User Requirements and Service/Feature Specifications
	ISO	TC 204 (WG 16)	▶ Emergency Communications over Intelligent Transport Systems (ITS)
Global Internal Protocol (IP) Telephony & Internet Standards	IETF	WG geopriv	▶ Emergency Calling Geographic Location/Privacy
		WG ecrit	<ul style="list-style-type: none"> ▶ Routing Emergency Calls to PSAPs ▶ Security Threats to Emergency Calling
		WG ieprep	<ul style="list-style-type: none"> ▶ Emergency Telecommunications Service ▶ Priority Services
		BOF GIG	<ul style="list-style-type: none"> ▶ Global Communications for Disaster Recovery ▶ Global Information Grid (GIG)
European NGN Technology Standards	ETSI	EMTEL	<ul style="list-style-type: none"> ▶ Emergency Communications Network Resiliency ▶ Emergency Communications between Authorities ▶ Emergency Communications from Authorities to Citizens ▶ Emergency Communications between Citizens ▶ Emergency Messaging
North American NGN Technology Standards	ATIS	PTSC / WG SAC	<ul style="list-style-type: none"> ▶ Emergency Telecommunications in IP Networks ▶ Packet Priority and Call Priority
		PRQC / WG SEC	▶ Emergency Telecommunications Services
		ESIF	<ul style="list-style-type: none"> ▶ Interconnection of E9-1-1/Emergency Services ▶ PSAP Network Interfaces and Protocol for NGN (TaskForce 34) ▶ Wireless E9-1-1 Readiness Implementation Plan ▶ Federal Telecommunications Service Propriety PSAPs
	TIA	TR-8	▶ Broadband Public Safety Communications
		TR-30	▶ Textphone Accessibility to Emergency Services in IP Environments
		TR-34	▶ Emergency Capabilities for IP over Satellite (IPoS) Communications
		TR-41	<ul style="list-style-type: none"> ▶ IP Terminal and Enterprise Network Support for Emergency Calling Service ▶ Enterprise Location Information Server Interfaces
		TR-45	<ul style="list-style-type: none"> ▶ Wireless Emergency Calling and Priority Services for cdma2000® ▶ Location Identification/Determination Services ▶ Broadband Data Capabilities for Enhanced Public Safety Services

Figure I-1 Selected NGN NS/EP ASPR Activities

Figure I-1 provides a brief description of selected work efforts underway in various agreements, standards, policies and recommendations (ASPR) bodies that are

related to national security emergency preparedness (NS/EP) communications (excluding lawful intercept).

Figure I-1 Selected NGN NS/EP ASPR Activities – *continued*

Type of ASPR	Body	Working Party	Work Description
IMS-3G Specifications	3GPP	WG SA1	▶ Priority Services
	3GPP2	WG1	▶ Services and Systems Requirements
NGN Service Control Interface / Service Enabler Specifications	Parlay Group		▶ Emergency Telecom Services
North American Service Provider Specifications	NENA		▶ Next Generation E9-1-1 Services
	Telcordia		▶ E9-1-1 Service Requirements
	Network Reliability and Interoperability Council	various	▶ Voluntary Best Practices on physical security, cyber security, network reliability, infrastructure protection, interoperability, public safety, emergency preparedness

NGN Standards Ecosystem

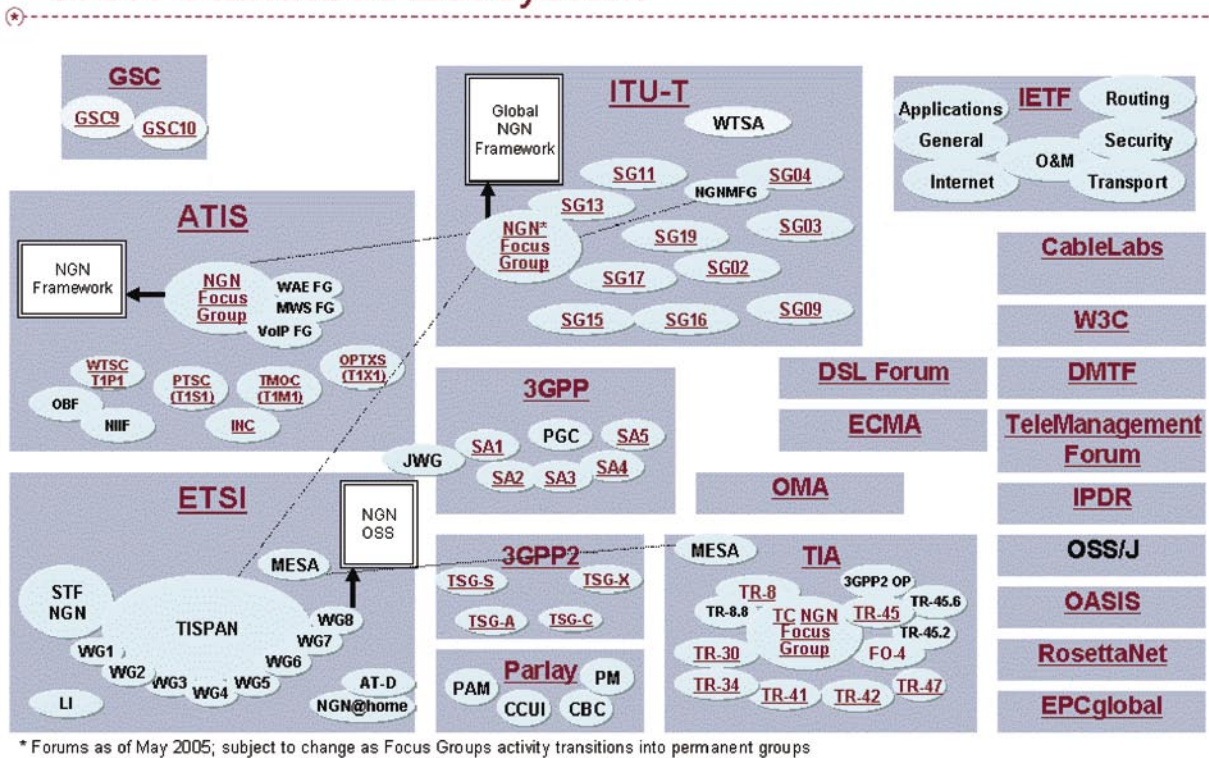


Figure I-2 The NGN Standards Ecosystem

Figure I-2 reflects the complexity of the NGN standards ecosystem.



Footnotes

- 1** See Computer User High Technology Dictionary (defining “Application” as “[a] program that helps the user accomplish a specific task; for example, a word processing program, a spreadsheet program, or an File Transfer Protocol (FTP) client. Application programs should be distinguished from system programs, which control the computer and run those application programs, and utilities, which are small assistance programs.”)
- 2** ATIS divides services into Transport Services, involving the transport of packets, and Application Services, which include remote delivery of functions by applications to users (e.g., network storage). ATIS Next Generation Network Framework, Part I: NGN Definitions, Requirements, and Architecture, p. 19-20 (Nov. 2004) (hereinafter ATIS NGN Paper Part I). Some might add Infrastructure Services, which provide the platform for transport and applications, to this list.
- 3** International Telecommunication Union, Study Group 2 – Delayed Contribution 49, December 6-15, 2005
- 4** See “First Report and Order and Notice of Proposed Rulemaking (FCC 05-116),” May 19, 2005, that it would require interconnected VoIP providers to provide E911 service. In its announcement the FCC noted; “The IP-enabled services marketplace is the latest new frontier of our nation’s communications landscape, and the Commission is committed to allowing IP-enabled services to evolve without undue regulation. But E911 service is critical to our nation’s ability to respond to a host of crises. The Commission hopes to minimize the likelihood of situations like recent incidents in which users of interconnected VoIP dialed 911 but were not able to reach emergency operators. Today’s Order represents a balanced approach that takes into consideration the expectations of consumers, the need to strengthen Americans’ ability to access public safety in times of crisis, and the needs of entities offering these innovative services.”
- 5** Over one hundred subject matter experts were included in this analysis, representing knowledge and operational experience from each of the eight ingredients that make up the framework.
- 6** Rauscher, Karl. F., Protecting Communications Infrastructure, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004; Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop, www.comsoc.org/~cqr; Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003, NRIC VII Wireless Network Reliability Focus Group Final Report, Issue 3, October 2005, NRIC VII Public Data Network Reliability Focus Group, Issue 3, October 2005 (www.nric.org), and the ATIS Network Reliability Steering Committee (NRSC) 2002 Annual Report (www.atis.org/nrsc).
- 7** Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003; Rauscher, Karl. F., Protecting Communications Infrastructure, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.
- 8** Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003, page 39.
- 9** As one example, see Microsoft’s Threat Modeling methodology as published by Swiderski and Snyder, ISBN: 0735619913.
- 10** See Section 4 of this Report.
- 11** See NGN Scenario Threat Profile matrix below for more information on STRIDE. Also see Howard and LeBlanc, STRIDE Classification for Threat Modeling.
- 12** See the NSIE 2005 Assessment of Risks to the Security of the Public Network prepared by NSTAC/NCS.

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-i
1 Introduction and Charge	1
1.1 Background on the NCC	1
1.1.1 History of NSTAC Studies on the NCC	2
1.1.2 NCC Membership	2
1.1.3 NCC Value Statement	4
1.2 Charge of the NCCTF	4
1.3 Scope of Study	4
1.4 Approach	5
2 NCC Findings	6
2.1 Authorities Guiding Mission	6
2.2 NCC Mission Statement	7
2.3 NCC Functions	7
2.4 NCC Membership and Operating Structure	8
2.4.1 Sector Coordinating Council Framework	9
2.4.2 NCC Membership Expectations	9
3 NCC Roadmap for the Future	10
3.1 One-Year and Ongoing Roadmap Actions	10
3.1.1 Organizational Structure	10
3.1.2 Information Sharing and Analysis	11
3.1.3 Who's in Charge?	13
3.1.4 Incident Management/Emergency Response	15
3.1.5 Policy	18
3.2 Three-Year Roadmap Actions	19
3.2.1 The New Value Proposition	19
3.2.2 IT and Communications	19
3.2.3 Industry Analysis	21
3.3 Five-Year Roadmap Actions	21
3.3.1 Incident Management/Emergency Response	21
3.3.2 International	22
3.4 Potential Roadblocks	23
3.5 Conclusion	24
4 Recommendations to the President	24

Appendices

A Task Force Members, Other Participants, and Government Personnel A-1

B NCCTF Interim Report B-1

C NCC Roadmap for the Future Recommended Actions List C-1

D Member Expectations of the National Communications System and the National Coordinating Center. D-1

E NCS Directive 3-4: National Telecommunications Management Structure. E-1

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 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 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.

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.

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

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.

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)
- ▶ 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 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.

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.

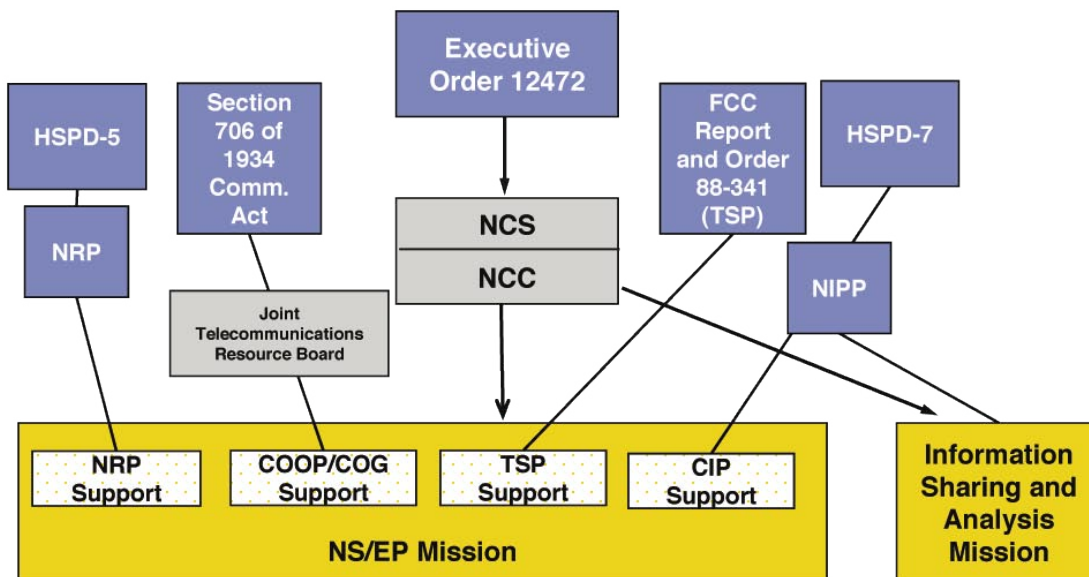


Figure 2.1 NCC Authorities and Missions

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.

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 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 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 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.
- ▶ 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 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.

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/regulated 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.

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

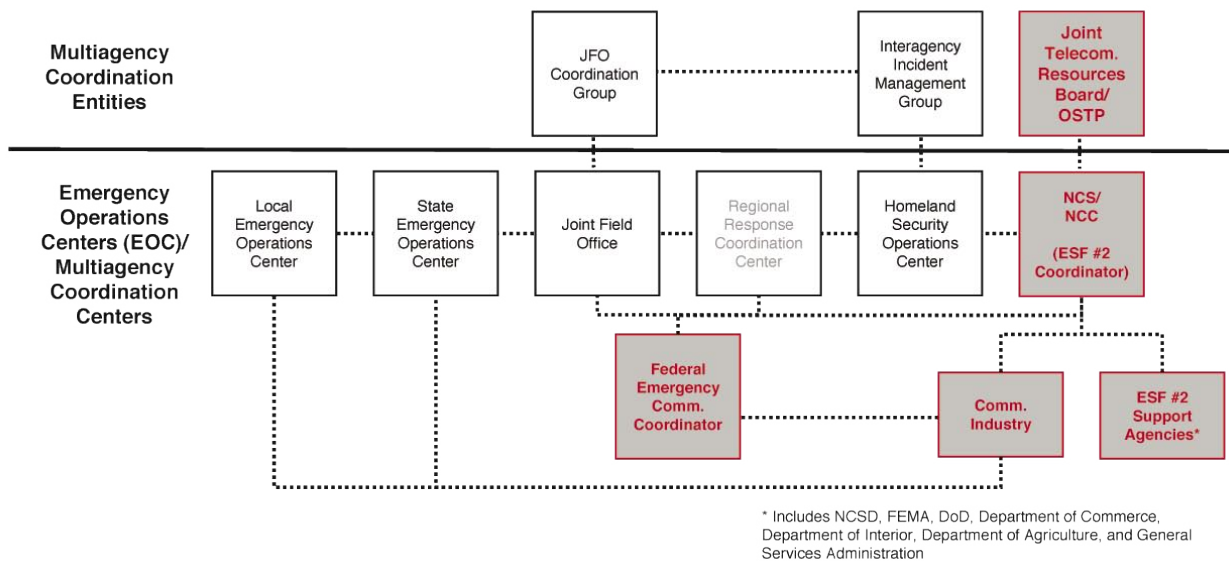


Figure 3.1 ESF#2 Alignment with NIMS Framework

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.

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 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.

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 (NCSD) 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.**
- ▶ **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 NCS, 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 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.**
- ▶ **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 NCS 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 Operations²⁷ 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.

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 NCSA 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 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—

- ▶ **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.

Footnotes

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

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.}

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

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.

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.

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.

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

11 NSTAC Satellite Task Force, March 2004.

- 12** HSPD-7 (“Critical Infrastructure Identification, Prioritization, and Protection”), issued in December 2003, superseded PDD/NSC-63 of May 22, 1998 (“Protecting Americas Critical Infrastructures”).
- 13** For clarity, the NCCTF refers to the sector as “communications” instead of “telecommunications” in this report.
- 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.
- 17** DHS. “LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process.” December 2005.
- 18** E.O. 12472, Section 1(b)(2).
- 19** E.O. 12472, Section 1(d)(1).
- 20** National Response Plan. December 2004. pg. 4.
- 21** GAO-06-365R Preliminary Observations on Hurricane Response, February 1, 2006.
- 22** The task force assumes that this 1992 directive is currently in force. See Appendix E for the text of the directive.
- 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.”
- 24** See Appendix F for more information on the IT ISAC.
- 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>.
- 26** NSTACs Next Generation Networks Task Force Report, March 2006.
- 27** <http://www.reliefweb.int/telecoms/tampere/index.html>.
- 28** Recommendations 1 and 2 in The Federal Response to Hurricane Katrina Lessons Learned.
- 29** Incorporation of IT ISAC.
- 30** HAS, Title II, and bill nos. of House and Senate original information sharing acts.
- 31** ISA website.
- 32** HSA sector table.
- 33** HSPD-7.
- 34** HSPD-12.
- 35** PCII Interim Regulations.
- 36** IT ISAC comment on draft PCII regulations.

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.

Ms. Rosemary Leffler

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. Christopher Guttman-McCabe

Lockheed Martin Corporation

Dr. Allen Dayton

Lucent Technologies (Bell Labs)

Mr. Richard Krock

Microsoft Corporation

Mr. Philip Reitinge

Nortel

Dr. John S. Edwards

Qwest Communications

International, Inc.

Mr. Thomas Snee

Raytheon Company

Mr. Frank Newell

Science Applications International Corporation

Mr. Henry Kluepfel

The Boeing Company

Mr. Robert Steele

United States Telecom Association

Mr. David Kanupke

VeriSign, Inc.

Mr. Michael Aisenberg

Verizon Communications, Inc.

Mr. Roger Higgins

Other Participants

BellSouth Corporation

Mr. David Barron

Cingular Wireless LLC

Mr. James Bugel

Microsoft Corporation

Mr. Paul Nicholas

Qwest Communications

International, Inc.

Mr. Jon Lofstedt

Sprint Nextel Corporation

Ms. Allison Gowney

Telecommunications Industry Association

Mr. Daniel Bart

Mr. David Thompson

George Washington University

Dr. Jack Oslund

Verizon Communications, Inc.

Ms. Ernie Gormsen

Government Personnel

Department of Defense

Ms. Hillary Morgan

Department of Energy

Mr. John Greenhill

Department of Homeland Security

Mr. Thomas Falvey

Mr. Jeffrey Glick

Mr. Charles Lancaster

Mr. Michael Lombard

Mr. John O'Connor

Mr. Don Smith

Ms. Christina Watson

CAPT Thomas Wetherald

Federal Reserve Board

Mr. Charles Madine

General Services Administration

Mr. John Migliaccio

Mr. Thomas Sellers

Office of Management and Budget

Ms. Kim Johnson

**Office of Science and
Technology Policy**

Ms. Linda Haller Sloan

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

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					
	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					

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years
	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	█				
	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	█	█	█	█	

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years
	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					
	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 NCSA 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					

Responsible Entity	Action Item	1 Year	2 Years	3 Years	4 Years	5 Years
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 and the National
Coordinating Center

Member Expectations of the National Communications System and the National Coordinating Center

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 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



COMMAND, CONTROL,
COMMUNICATIONS
AND INTELLIGENCE

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

313A	
DEFENSE	
FDA	
04 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 (NCSD) 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. NCSD 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 NCSD 3-4. For additional information on the implementation of NCSD 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, 1982

NCS 3-4

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

NCS DIRECTIVE 3-4

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

HCSD 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 REMT CPG/RCC is the REMT 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 REMT CPG/RCC is also capable of serving as an alternate NCC.

b. 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 REMT CPG/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 CPG, REMT CPG/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

NCSD 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 OMNCS.

(2) Will assist the OMNCS 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 OMNCS 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 CFG and REMT CFG/RCC operational matters in coordination with OSTP.

May 4, 1992

NCSD 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 OMNCS with NTMS implementation and planning in support of the NEMT and RENT CFG/RCCs.

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

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

e. General Services Administration:

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

May 4, 1992

NCSB 3-4

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 CONOPS

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 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 Act,³² HSPD 7³³ and HSPD 12,³⁴ 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) program,³⁵ 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 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

NSTAC XXIX

Correspondence
to the President



NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

April 12, 2006

The Honorable George W. Bush
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

The unprecedented communications challenges posed by Hurricanes Katrina and Rita highlighted that some existing communications systems still lack sufficient levels of operability and interoperability among the multiple response and recovery entities including the Departments of Homeland Security and Defense, the National Guard, State and Local Governments, critical infrastructure sectors, and other non-Governmental organizations. Your February 2006 report, *The Federal Response to Hurricane Katrina: Lessons Learned*, recommends development of a National Emergency Communications Strategy that supports communications operability and interoperability, and advises that the strategy consider the direction of the telecommunications industry and supporting recommendations of your National Security Telecommunications Advisory Committee (NSTAC). The NSTAC Principals fully endorse the creation of an overarching National Emergency Communications Strategy and offer our strong commitment to assist in its development.

The NSTAC has identified immediate actions that will significantly improve the Nation's emergency communications capabilities prior to the upcoming 2006 hurricane season while recognizing that some elements may already have begun. Without prompt action, effective coordination and response to National incidents will remain severely hampered this summer and beyond. The NSTAC recommends that you direct the Department of Homeland Security and other appropriate agencies to accelerate their efforts and adequately resource actions to assure completion, prior to the summer of 2006, of the recommended initiatives listed below:

1. Establish a uniform protocol working with Federal, State, and Local Government organizations that can dynamically identify their emergency management coordinators' contact information, especially during times when regular contact information is changed due to event situations, and have a capability to share that information with DHS (e.g., via websites). This capability should be administered by the National Communications System (NCS) in concert with the National Coordinating Center (NCC) to assist in its execution of Emergency Support Function #2 for communications. The capability will enable rapid contact and coordination with response entities pursuant to Recommendation #35 of the *Lessons Learned Report*.
2. Create a deployable communications capability for the Gulf Coast region in accordance with Recommendation #37 of the *Lessons Learned Report*. This capability must focus on rapidly deployable, interoperable mobile communications solutions that will provide reliable communications to emergency responders at all levels of Government in a disaster-affected region. We anticipate that this capability will be a prototype that can be quickly established throughout the Nation for use as a gap-filler when communications infrastructure has been damaged by natural or man-made disasters. NSTAC companies are prepared to actively provide expertise and support for this capability.

3. Formally integrate the NCS national security and emergency preparedness priority programs (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) into the National Emergency Communications Strategy pursuant to Recommendation #34 of the *Lessons Learned Report*. These priority programs have demonstrably enhanced communications operability and interoperability and could further complement State and Local first responder communications in support of public health, safety and law enforcement requirements.
4. Additionally, the NSTAC recommends that you direct the National Telecommunications and Information Administration to work in conjunction with the Federal Communications Commission to streamline the authorization process for use of Federal incident response (IR) frequencies by the larger non-Federal Government emergency response community. Removing barriers to responsively authorize use of Federal IR frequencies will facilitate interoperability between Federal and non-Federal emergency responders.

In addition to these immediately applicable recommendations, your NSTAC has recently provided other recommendations addressing specific critical communications concerns as a result of its ongoing review of the Hurricane Katrina response. Our previous correspondence has addressed a broad range of issues such as ensuring access and suitable credentialing for telecommunications infrastructure provider response personnel, formally designating such personnel as "Emergency Responders" to enable provision of non-monetary Federal assistance under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)*, and improving industry-Government incident response coordination via the NCC. These recommendations also deserve consideration for incorporation into the overall National Emergency Communications Strategy.

Thank you for this opportunity to make these recommendations to further strengthen our Nation's emergency responder communications. Adoption of these critical recommendations will help ensure that short-term interoperability solutions are implemented prior to the upcoming hurricane season. On behalf of the NSTAC Principals, I thank you for your support and we look forward to continuing our work with you and your staff.

Sincerely,



F. Duane Ackerman
NSTAC Chair

Copy to:
The Vice President
Secretary of State
Secretary of Defense
The Attorney General
Secretary of Transportation
Secretary of Energy

Director, Office of Management and Budget
Assistant to the President for National Security Affairs
Assistant to the President for Homeland Security
Director, Office of Science and Technology Policy
Chairman, Federal Communications Commission
Secretary of Commerce
Assistant Secretary of Commerce for Communications and Information
Secretary of Homeland Security
Under Secretary for Preparedness, Department of Homeland Security
Assistant Secretary for Cyber and Telecommunications/Director, National Communications System
Assistant Secretary for Infrastructure Protection, Department of Homeland Security
Director of Chemical and Nuclear Preparedness and Protection Division, Department of Homeland Security
Director of State and Local Government Coordination, Department of Homeland Security
Director of Federal Emergency Management Agency, Department of Homeland Security
Assistant Secretary for Congressional and Intergovernmental Affairs, Department of Homeland Security
NSTAC Principals and Industry Executive Subcommittee Members



NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

April 12, 2006

The Honorable George W. Bush
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500

Dear Mr. President:

As your industry advisor on national security and emergency preparedness (NS/EP) communications matters, the National Security Telecommunications Advisory Committee (NSTAC) would like to bring to your attention certain issues that are impacting the ability of the communications sector and the National Coordinating Center (NCC) to plan for and respond to major disasters at a regional level. The following recommendations are based both on the findings of a comprehensive review of the NCC initiated in early 2005 that extended into the time period following Hurricane Katrina, and on the more recent White House report on Hurricane Katrina.

One of the challenges during major disaster response efforts has been a lack of effective coordination between industry and government at the regional level. Industry's emergency planning efforts have begun to respond to this need. Likewise, the National Communications Systems (NCS), part of the Department of Homeland Security (DHS), is developing an Emergency Support Function (ESF) #2 – Communications Federal Operations Plan to provide supplemental detail to the *National Response Plan* (NRP).

Mr. President, we believe this effort requires your personal support by directing all ESF#2 support agencies, including the Federal Emergency Management Agency, General Services Administration, Department of Defense, the Federal Communications Commission, and others to give their full attention to this matter and, when completed, to comply with the Plan. In particular, the Federal Emergency Communications Coordinator (FECC) must be acknowledged by all Federal entities as the lead of ESF #2 in the region. Further, the FECC should coordinate and the Joint Field Office (JFO) should accommodate, as necessary, 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. The NSTAC believes that regional communications and information technology coordination led by the FECC, within or as a virtual capability of the JFO, would significantly improve the ability of government and the private sector to respond to major incidents. This requirement for communications industry presence must be taken into consideration as the site for the JFO is being selected.

The plans and preparations outlined above are essential steps to be taken to be better prepared for the hurricane season of 2006. However, as we both know, Hurricane Katrina was unprecedented by nearly every measure, including the extent of devastation in the impact area, the scope of the evacuation both prior to and after the event, the scale of government and private sector response required, and the security concerns for our personnel as they responded to the event. Even with the steps outlined above, we could still be overwhelmed by another event of this magnitude, particularly as recovery activities continue from last year.

To augment the activities already underway, NSTAC plans to ask the Communications and Information Technology Sector Coordinating Councils (SCCs) to conduct a short-term industry-led task force with the

primary goal of planning for a regional coordinating capability in the Gulf Coast and Southeastern regions prior to the 2006 hurricane season. This task force will be asked to determine the best short and long-term regional communications and information technology coordinating capabilities that could be established external to the JFO. This capability is aimed at coordinating the capabilities of many industry segments in disaster response efforts at the regional level. We ask you to support this effort by directing DHS, the Office of Science and Technology Policy, and the Homeland Security Council to support us in this effort, as requested by the industry councils.

We will ask these two coordinating councils to address the following issues: (1) how industry should coordinate regional response; (2) what funding sources may be necessary for this regional capability; (3) whether the capability should be virtual or based in an existing 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 can best garner recognition and support from industry and government entities. In addition, their task force should examine how best to assist Secretary Chertoff's goal of establishing a core disaster workforce able to take full advantage of existing assets, resources, and capabilities. This will also address your goal of ensuring situational awareness through the establishment of rapid deployable communications and the institution of a structure for consolidated operational reporting.

Mr. President, these steps, if taken immediately, will provide meaningful results well in advance of the hurricane season of 2006. NSTAC member companies are committed to assisting the Nation in this effort. Thank you for your ongoing support of NSTAC and we look forward to working with you and your Administration on these and other telecommunications issues critical to our national security and emergency preparedness.

Sincerely,



F. Duane Ackerman
NSTAC Chair

cc:

The Vice President
Secretary of Defense
Director, Office of Management and Budget
Assistant to the President for National Security Affairs
Assistant to the President for Homeland Security
Director, Office of Science and Technology Policy
Chairman, Federal Communications Commission
Assistant Secretary of Commerce for Communications and Information
Secretary of Homeland Security
Under Secretary for Preparedness, Department of Homeland Security
Assistant Secretary for Cyber and Telecommunications/Director, National Communications System
Director of State and Local Government Coordination, Department of Homeland Security
Director of Federal Emergency Management Agency, Department of Homeland Security
Assistant Secretary for Congressional and Intergovernmental Affairs, Department of Homeland Security
Administrator, General Services Administration
NSTAC Principals and Industry Executive Subcommittee Members

Office of the Manager
National Communications System
Customer Service Division
Mail Stop 8510
245 Murray Lane
Washington, DC 20528-8510
(703) 235-5525

www.ncs.gov/nstac/nstac.html
nstac1@dhs.gov