THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Emergency Communications and Interoperability

January 16, 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Communications among those responding to a natural disaster, terrorist attack, or other large-scale emergency is the essential component to a successful response and recovery effort and, ultimately, in the ability of the Nation's emergency responders to save lives and property. To ensure a comprehensive preparation for and response to the widest range of crises and incidents, emergency responders must have operable and interoperable emergency communications systems. As evidenced by the communications shortcomings experienced during the September 11, 2001, attacks and Hurricane Katrina, the Nation still remains short of this goal. Interoperability challenges that were recognized during these crises included lack of interoperable equipment at the tactical level, ineffective use of available communications assets caused by poor resource planning, and an overall lack of integrated command structures to enable interoperability.

In response to the issues highlighted during the Hurricanes Katrina, Rita, and Wilma recovery efforts, the President's National Security Telecommunications Advisory Committee (NSTAC) Principals recognized that the NSTAC should play a valuable role in addressing short-term critical issues in advance of the 2006 hurricane season and in supporting resolution of longer-term strategic issues. Consequently, the NSTAC commissioned a two–part effort to:

- Urgently identify specific actions to improve emergency communications and interoperability in the short term; and

- Identify mid- to long-term policy recommendations and technology solutions to enhance collaboration across organizational and jurisdictional boundaries to help our country better prevent, prepare for, respond to, and recover from disasters and emergencies.

The NSTAC initially focused on short-term actions and issued a *Letter to the President on Emergency Communications and Interoperability (The Letter)* in March 2006, outlining emergency communications and interoperability issues and identifying immediately applicable actions to improve responder communications capabilities. The work of the task force continued, and the five NSTAC recommendations presented in this report refine and expand on *The Letter's* short-term recommendations.

The NSTAC Principals view each recommendation as equally vital and deserving of Presidential action; they are presented in no particular order of priority but together represent a roadmap for emergency communications and interoperability improvements. 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*:

- **Expand Use of Deployable Communications Capabilities.** Direct the Department of Homeland Security (DHS) to incorporate into its emergency communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications

infrastructure. The President should also direct the DHS to expand and enhance use of the Wireless Priority Service (WPS) program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi-carrier WPS end-to-end solutions that facilitate the rapid restoration of essential wireless network elements.

- **Enhance the Telecommunications Service Priority (TSP) Program for Wireless Networks.** Direct the DHS and other responsible Federal agencies to explore enhancements to the TSP program to accommodate expanded requests from national security and emergency preparedness (NS/EP) users of wireless telecommunications services at critical sites. The President should also direct Federal agencies, and encourage State and local agencies, to fully utilize the existing provisions of TSP and to apply for the enhanced wireless TSP coverage provisions as they are developed for use at their critical sites.

- **Improve NS/EP Policy to Support Emergency Communications.** Modernize existing NS/EP policy guidance to clarify and consolidate Federal Government emergency communications roles and responsibilities. Specifically, additional Presidential policy guidance is required to:

  - Clearly delineate the NS/EP and emergency communications roles and functions of the National Communications System, the National Cyber Security Division, and the new Office of Emergency Communications, as established by the *DHS Appropriations Act of 2007*, and any other DHS organization, such as the Science and Technology Directorate and the Federal Emergency Management Agency, with a role or responsibility in the area of emergency communications;
  - Preserve and maintain critical NS/EP functions and capabilities that support the National leadership; and
  - Ensure Executive oversight across the Federal Government for a fully coordinated, integrated, and interoperable emergency response communications function and capability.

- **Include Critical Elements in the *National Emergency Communications Strategy (NECS)* and the *National Emergency Communications Plan (NECP)*.** Incorporate the following critical elements in the development, maintenance, and execution of the *NECS* and associated implementation guidance, and direct the DHS and other responsible Federal agencies to incorporate the elements into the *NECP*:

  - Large-Scale State and Regional Shared Public Safety Networks and Federal Grants;
  - Yearly Benchmarks for Achieving Defined Interoperability Objectives;
  - Nationwide Outreach to Support Emergency Response Communications;
  - Consolidation of Operations Centers to Increase Coordination and Situational Awareness; and
  - Identification of Specific Private-Sector Emergency Communications and Interoperability Support Roles.

- **Address Emergency Communications in the Converged Environment.** To encourage responsive emergency communications capabilities in the converged environment, establish and incorporate the following capability objectives into the *NECS* and associated implementation guidance, and also direct the DHS to incorporate the capability objectives into the *NECP*:

  - Support for a Significantly Expanded User Base;
  - Full Leveraging of Network Assets;
  - Internet Protocol-based Interoperability;
  - Assured Access for Key Users through Priority Schemes or Dedicated Spectrum;
  - National Scope with Common Procedures and Interoperable Technologies;
  - Deployable Elements to Supplement and Bolster Operability and Interoperability;
  - Resilient and Disruption–Tolerant Communications Networks;
  - Network–Centric Principles Benefiting Emergency Communications; and
  - Enhanced Communications Features.

The NSTAC continues to evaluate and develop recommendations pertaining to emergency communications and interoperability; a long-term report is planned for publication in June 2007. The report will identify additional mid- to long-term policy recommendations and technology solutions, including evolution of emergency communications, transition to the converged environment, and application and use of alternate communications capabilities such as satellite services and high-altitude platforms, for example aerostat-based devices. The long-term review will investigate how such solutions can be economically extended to supplement terrestrial networks and support NS/EP and emergency communications needs.

1.0 INTRODUCTION

In the last five years, as a result of the attacks of September 11, 2001, and the devastating hurricane season of 2005, the Nation has witnessed firsthand the consequences of not having fully operable and survivable emergency communications capabilities in place to support the mission–critical needs of our emergency responder community.[1] Communications among those responding to a natural disaster, terrorist attack, or other large-scale emergency is the essential component to a successful response and recovery effort, and ultimately in the ability of responders to save lives and property. In light of these high stakes, the need for the Nation's emergency communications systems, plans, processes, and strategies to account for and mitigate the impact of massive communications infrastructure damage, including the destruction of telephone lines, public safety networks, cellular towers, and sustained loss of power, remains paramount.

In addition to concerns about emergency communications system operability, a further major barrier to effective responder communications is the widespread lack of interoperability that impedes communications and critical information sharing across dissimilar emergency responder systems.[2] Interoperability challenges recognized during the Hurricane Katrina response included lack of interoperable equipment at the tactical level, ineffective utilization of available communications assets caused by poor resource planning, and an overall lack of integrated command structures to enable interoperability.[3] The Department of Homeland Security (DHS) has also identified communications interoperability as one of the key national priorities for first responders to achieve the National Preparedness Goal and has identified interoperable communications as an essential target capability needed to respond to a major event.[4]

1.1 Background and Charge

In response to issues highlighted during Hurricanes Katrina, Rita, and Wilma response efforts, the President's National Security Telecommunications Advisory Committee (NSTAC) Principals recognized that the NSTAC should play a valuable role in addressing a number of short-term

---

[1] The *Final Report of the National Commission of Terrorist Attacks Upon the United States*, December 2001, the White House's report, *The Federal Response to Katrina: Lessons Learned*, February 2006, and the *Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks—Report and Recommendations to the Federal Communications Commission*, June 12, 2006, all documented the numerous failures in the ability of emergency responders to effectively communicate in response to these incidents. The term "emergency communications capabilities" refers to the ability to provide and maintain, throughout an emergency response operation, a continuous flow of information among emergency responders.

[2] Communications interoperability refers to "the ability of emergency responders to talk across disciplines and jurisdictions via communications systems and to exchange voice and/or data with one another on demand, in real time, when needed, and as authorized." Department of Homeland Security, SAFECOM Program, http://www.safecomprogram.gov.

[3] "Hurricane Katrina was the most destructive natural disaster in U.S. history. The storm crippled thirty-eight 911 call centers, disrupting local emergency services, and knocked out more than 3 million customer phone lines in Louisiana, Mississippi, and Alabama. Broadcast communications were likewise severely affected, as 50 percent of area radio stations and 44 percent of area television stations went off the air." White House Report, *The Federal Response to Katrina: Lessons Learned*, February 2006.

[4] The National Preparedness Goal guides Federal departments and agencies, State, territorial, local, and tribal officials; the private sector; non-Government organizations; and the public in determining how to most effectively and efficiently strengthen preparedness for terrorist attacks, major disasters, and other emergencies. *The Department of Homeland Security's Interim National Preparedness Goal, Homeland Security Presidential Directive 8: National Preparedness, March 31, 2005.*

critical issues in advance of the 2006 hurricane season and supporting resolution of longer-term strategic issues.[5] The Principals also recognized that industry and Government must work together in partnership to develop a preparedness strategy that incorporates lessons learned from actual events to anticipate the necessary level of preparedness for the next event. Consequently, the NSTAC commissioned a two-part effort to:

- Urgently identify specific actions to improve emergency communications and interoperability in the short term; and

- Identify mid- to long-term policy recommendations and technology solutions to enhance collaboration across organizational and jurisdictional boundaries to help our country better prevent, prepare for, respond to, and recover from disasters and emergencies.

In February 2006, the White House released its *Report on the Federal Response to Hurricane Katrina: Lessons Learned (Lessons Learned Report)*. The report specifically suggested the review of our current laws, policies, plans, and strategies relevant to communications and the development of a *National Emergency Communications Strategy (NECS)* that supports communications operability and interoperability. In soliciting the support of the NSTAC, the White House recommended the following:

> "The development of an overarching *National Emergency Communications Strategy* should address a full range of hazards; and should consider the direction of the telecommunications industry and supporting recommendations of the President's National Security Telecommunications Advisory Committee."

In response to this direction, the NSTAC broadened the scope of its emergency communications and interoperability effort to provide inputs to the White House's *NECS* and the Congressionally directed DHS *National Emergency Communications Plan (NECP)* and to undertake a review of current procedural and jurisdictional concerns regarding communications operability and interoperability.[6]

[5] Critical issues discussed by the Principals included examining the *National Response Plan*, Emergency Support Function #2, Communications, approaches to enhance situational awareness from the local level up to the President, existing interoperability-related standards, and leveraging the commercial infrastructure to support emergency responders.

[6] Although not a requirement for the NSTAC's development of inputs, the *National Emergency Communications Strategy (NECS)* had not been formally published by the White House for review at the time this report was issued. The NSTAC welcomes the opportunity to provide further comment and input upon its publication. *DHS Appropriations Act of 2007* also directs the DHS, in cooperation with other Federal agencies, emergency response providers, and the private sector, to develop a *National Emergency Communications Plan (NECP)* to provide recommendations to ensure, accelerate, and attain interoperable emergency communications nationwide. NSTAC recommendations in this report are relevant to both the *NECS* and the *NECP* and are offered as guidance and input to developing both documents and to any consequent implementation guidance.

1.2 Approach

The NSTAC submitted a *Letter to the President on Emergency Communications and Interoperability (The Letter)* in March 2006, outlining emergency communications and interoperability issues and identifying immediately applicable actions to improve responder communications capabilities in advance of the 2006 hurricane season. A copy of *The Letter* is presented in **Appendix A**. Work continued to address the emergency communications and interoperability issues, and the NSTAC recommendations presented in this report refine and expand on *The Letter's* short-term recommendations.[7]

Imperative to the success of the effort were the contributions of representatives of the NSTAC's member companies, Government participants, and the external subject matter experts (SME) who were invited to share their valuable perspectives on emergency communications and interoperability issues. **Appendix B** provides a list of the NSTAC's members, other participants, and Government personnel who participated in this effort.

The NSTAC continues to evaluate and develop recommendations pertaining to emergency communications and interoperability. A long-term report, planned for publication in June 2007, will identify additional mid- to long-term policy recommendations and technology solutions, including evolution of emergency communications, transition to the converged environment, and application and use of alternate communications capabilities such as satellite services and high-altitude platforms, for example aerostat-based devices. The long-term review will investigate how such solutions can be economically extended to supplement terrestrial networks and support NS/EP and emergency communications needs.

1.3 Scope of the NSTAC Review

Several systematic reviews of significant emergency communications and interoperability challenges faced by emergency responders were documented in the months following both the September 11, 2001, attacks and the Hurricane Katrina response. The 9/11 Commission's *Final Report of the National Commission of Terrorist Attacks Upon the United States* provides a complete account of the circumstances, preparedness for, and immediate response to the attacks.[8] Ineffective incident command and control, lack of planning and standard operating procedures (SOP), and lack of non-interoperable equipment all contributed to emergency communications difficulties. Reports issued in response to Hurricane Katrina by Congress, the White House, and other agency reviews, including those completed by the General Accounting Office (GAO) and the Federal Communications Commission (FCC), collectively deliver a comprehensive picture of the critical technological, organizational, jurisdictional, and policy barriers to more effective operable and interoperable emergency communications.

This NSTAC review focuses primarily on solutions, achievable in the short- to mid-term, to overcome impediments to emergency responder command and control and decision making, particularly during events characterized by catastrophic loss of communications infrastructure

[7] The NSTAC notes that, while the recommendations presented in this report are intended for immediate action, full realization of the benefits of their implementation may take a longer period of time. For example, implementation of all operational-and policy-oriented recommendations necessarily will depend on operations planning, policy development and revision schedules, and available resources to enact any required changes.

[8] *Final Report of the National Commission on Terrorist Attacks Upon the United States*, December 2001.

and involvement of multiple responder organizations. Technological, organizational, and policy impediments and related NS/EP implications were identified, and mitigation approaches and recommendations were then evaluated. **Figure 1** illustrates the increasing criticality of expanded information sharing and communications across responder organizations as a function of the level of devastation and frequency of occurrence.

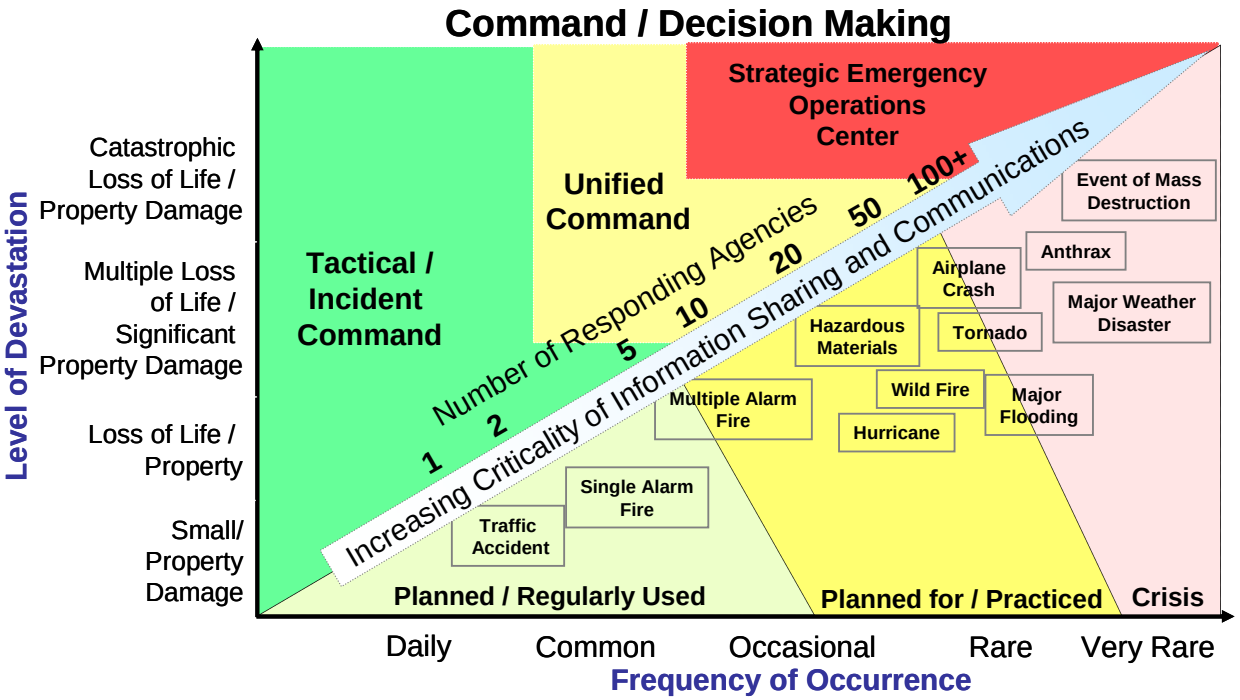

Figure 1—Criticality of Information Sharing and Communications

As an incident escalates, the level of devastation, the potential for catastrophic loss of life, property damage, and subsequent impairment to the communications infrastructure makes an already bad or problematic situation worse. For example, a scenario that begins as a simple traffic accident may escalate into a hazardous spill or ultimately may evolve into chemical, biological, radiological, or nuclear terrorism. The organizational command structures most suited to a specific incident response will vary from a tactical incident command at the local level to additional unified or strategic command layers. As events unfold, critical information sharing and coordinated, interoperable communications increase in complexity to meet the requirements of a potential responder community that could include tens or potentially hundreds of organizations.

From a technology and tools perspective, the communications solutions and devices used by emergency responders on a day-to-day basis will be expected to provide the necessary capability during special events or in support of a widespread crisis. In the post-September 11th environment, realizing the need for increased practice and planning for incidents, including those rare crisis events that may require a coordinated strategic command component, is a welcome trend. Our Nation's emergency responders require a communications architecture that will provide both day–to–day operability and interoperability when needed in response to NS/EP events.

1.4 Report Organization

In reviewing emergency communications and interoperability issues from the command and control, information sharing, and technology and tools perspectives, the NSTAC distilled recommendations that address short- to mid-term operational, organizational, or technological improvements to enhance emergency communications and interoperability.

Five recommendations are presented in this report. The NSTAC Principals view each recommendation as equally vital and deserving of action; they are presented in no particular order of priority, but together represent a roadmap for emergency communications and interoperability improvements. The remainder of this report is organized into three sections:

- **Section 2.0—Expansion of National Security and Emergency Preparedness Priority Services and Deployable Capabilities** presents two recommendations intended to enhance existing industry–Government programs and ensure that they can scale to meet the increasing reliance on wireless communications in crises:

  - **Section 2.1—Deployable Communications Capabilities.** Use of deployable communications capabilities is recommended to provide reliable communications to emergency responders in the event of a regional catastrophic failure. The recommendation also urges expanded use of the WPS program though multi-carrier WPS end-to-end solutions to facilitate rapid restoration of essential wireless network elements; and

  - **Section 2.2—Telecommunications Service Priority Enhancement for Wireless Networks.** Enhancing the Telecommunications Service Priority (TSP) program is recommended to accommodate expanded requests from NS/EP users of wireless telecommunications services at critical sites and to ensure that wireline and wireless carriers, in conjunction with the Government, have a consistent perspective on provisioning and restoration priorities during crises.

- **Section 3.0—Inputs to the *National Emergency Communications Strategy*** presents three recommendations to fulfill the request made by the White House for communications industry input into the *NECS*:

  - **Section 3.1—Expansion of National Security and Emergency Preparedness Policy to Support Emergency Communications.** Expanding and clarifying NS/EP policy guidance is recommended to better encompass the Nation's emergency communications needs and objectives;

  - **Section 3.2—Critical National Emergency Communications Strategy Elements.** Critical elements are recommended for incorporation into the Government's planned development and execution of the *NECS* and *NECP*; and

  - **Section 3.3—Emergency Communications in the Converged Environment.** To assure a more survivable and interoperable emergency communications architecture, the NSTAC's perspective on a strategic direction for the future is presented. Incorporating specific critical capability objectives for emergency communications in the converged environment of the future is recommended.

- **Section 4.0—Conclusion** summarizes the report.

2.0 EXPANSION OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS PRIORITY SERVICES AND DEPLOYABLE CAPABILITIES

In *The Letter* of March 2006, the NSTAC identified immediate actions that would markedly improve the Nation's emergency communications capabilities before the 2006 hurricane season. Specifically, the NSTAC recommended, in part, that the President direct the DHS and other appropriate agencies to:

> "(1) create a deployable communications capability… focusing on rapidly deployable, interoperable mobile communications solutions that could provide reliable communications to emergency responders at all levels of Government in a disaster-inflicted region; and (2) formally integrate the NCS NS/EP priority services (*e.g.*, Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) into the National Emergency Communications Strategy."[9]

After issuing *The Letter*, the NSTAC continued to solicit input from private- and public-sector SMEs, evaluate and debate alternative solutions and approaches, and further develop its original short-term recommendations. This section presents two refined recommendations to enhance existing industry–Government programs and ensure that they can scale to meet the increasing reliance on wireless communications during crises and to ensure that responders have the following:

- Communications capabilities that can be rapidly deployed after a catastrophic event and an enhanced rapid service restoration capability for WPS users through the use of such deployable assets; and

- An expanded and more responsive NS/EP provisioning and restoration prioritization capability in the wireless domain.[10]

[9] *NSTAC's Letter to the President on Emergency Communications and Interoperability*, March 2006, presents recommendations to support the White House's *Lessons Learned Report*, Recommendations #34 and #37, February 2006.

[10] The NSTAC encourages proactive planning, implementation, and periodic testing of the improved capabilities recommended in this section. Several Government reports addressing the Hurricane Katrina response—reports issued by the White House, the Department of Homeland Security, the Federal Communications Commission's Independent Panel, and Congressional committees—underscore the need for Government agencies to contract critical services before a disaster strikes.

2.1 Deployable Communications Capabilities

Recommendation: **The President should direct the Department of Homeland Security (DHS) to incorporate into its emergency communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications infrastructure. The President should also direct the DHS to expand and enhance use of the Wireless Priority Service (WPS) program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi-carrier WPS end-to-end solutions that facilitate the rapid restoration of essential wireless network elements.**

The NSTAC has studied the effectiveness of existing programs and capabilities in the private and public sector designed to ensure that adequate telecommunications resources are available to emergency responders. The telecommunications industry has invested billions of dollars to reinforce their networks and prepare for disasters.[11] The public sector at the Federal, State, local, and tribal levels has also taken significant actions to improve and enhance its emergency response plans and capabilities to mitigate issues specifically identified during the Hurricane Katrina response.[12] As a result of these improvements and enhancements to the emergency communications infrastructure, the capacity of emergency response organizations to mount effective response efforts has vastly improved, particularly during the last 18 months.

Fortunately, catastrophic events of the magnitude of Hurricane Katrina rarely occur. Of all severe tropical and seismic events in recent months, only Hurricane Katrina resulted in the long-term loss of telecommunications network infrastructure. A more typical scenario is that connectivity to wireless communications sites is lost because of the loss of power, the loss of transport, or both. In these situations, deployment of generators, backhaul through unlicensed microwave or satellite, and/or deployable solutions including public safety radio systems and Cell Sites on Wheels (COW) will usually restore service relatively quickly.[13]

However, in a regional catastrophic failure that involves complete or significant loss of communications or supporting infrastructure, carriers' normal network restoration capabilities or "quick fixes" are generally not sufficient to meet the immediate communications demands of the emergency responders in the incident area. Loss of regional switching capacity, loss of commercial power, and lack of transport connectivity between switches in both wireline and wireless networks are all potential causes of isolation and result in the inability of emergency responders to communicate.[14] In these situations, responders' terrestrial,

---

[11] The *Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks—Report and Recommendations to the Federal Communications Commission*, June 12, 2006, recognized the success of wireless operator deployment of more than 100 Cell Sites on Wheels (COW) and Cell Sites on Light Trucks (COLT) to the impacted region. During Hurricane Katrina, these COWs and COLTs were brought in to restore commercial service. The Panel also found that satellite networks appeared to be the communications service least disrupted by Hurricane Katrina.

[12] Numerous Federal actions include developing new Emergency Support Function policies and procedures, clarifying roles and responsibilities, designating emergency personnel, improving information sharing and situational awareness approaches, and identifying Government deployable resources and assets.

[13] NSTAC ECITF membership deliberation.

[14] The *NSTAC Report to the President on Telecommunications and Electric Power Interdependencies: The Implications of Long Term Outages* addresses issues created by the increasing interdependencies between the North American telecommunications and electric power sectors from a long-term perspective.

infrastructure-dependent devices are rendered useless. Establishing their ability to rapidly resume communications can be achieved by using alternative communications solutions that do not depend on the lost infrastructure or temporary or permanent restoration of the underlying infrastructure.

Deployable communications capabilities are critical to all emergency communications solutions. Where existing infrastructure continues to function to some degree, mobile deployable units such as cellular, Land Mobile Radio (LMR), and mesh networks; Wireless Fidelity (WiFi) hotspots; MSS; satellite access through Very Small Aperture Terminal (VSAT) services; and, in the near future, hybrid satellite–terrestrial devices, can all be used to bolster the available bandwidth that supports emergency response personnel and the populace within regions impacted by an incident. Where existing infrastructure has been lost or is no longer operable, deployable components can replace the failed infrastructure while providing connectivity to all personnel and organizations within the region of a communications outage. The key to these solutions is having the deployable equipment and services pre-arranged and available within the region of the emergency to allow the most rapid deployment and re-establishment of communications, providing both operability for failed networks and interoperability to allow communications and coordination among the full range of emergency communications users and responders.

The NSTAC recognizes the critical emergency communications role that satellite-based communications devices played during the Hurricane Katrina response and undoubtedly will continue to play in future incident responses.[15] Furthermore, the NSTAC has urged additional provision and use of alternate communications capabilities such as satellite-based devices for an expanded range of emergency responders that would most benefit from the flexibility such capabilities can provide.[16] Such capabilities are effective specifically for responders who have ready access to satellite-based devices and are trained and familiar with device use in an operational emergency response environment. Reasonable efforts should be made to provision and train first responders in the use of alternative communications devices—such as satellite phones, VSATs, aircraft, and aerostat-based devices. The NSTAC also notes that several companies are developing hybrid satellite–terrestrial systems that potentially make satellite devices more readily available and cost-effective for responders. The proposed approach below serves to provide Government with a mechanism for rapid restoration of communications capabilities for responders in an incident area who have no other communications alternative other than the cellular and/or WPS devices on their persons.

As the Federal, State, local, and tribal Governments continue to develop and refine their emergency communications strategies and plans, more effective incorporation of deployable components is one of several vital capability objectives that deserve emphasis. In addition to pre-arranged deployable component plans, the NSTAC recommends that critical capability objectives also be considered, including support for a significantly expanded user base that fully leverages all network assets, Internet Protocol (IP) –based interoperability, assured access for key users through priority access schemes or dedicated spectrum, and based on a national scope with common procedures and interoperable technologies. **Section 3.3** of this report further

[15] The Federal Communications Commission (FCC)'s Independent Panel Reviewing Hurricane Katrina noted that more than 20,000 satellite phones were deployed to the Gulf Coast region in the days following Hurricane Katrina.

[16] The *NSTAC Report to the President on Satellite Communications*, February 2004, The *NSTAC Report to the President on Next Generation Networks*, March 28, 2006.

expands on these and other critical capability objectives and recommends incorporating them into the *NECS* and *NECP*.

2.1.1 Deployable Solutions to Reconnect Wireless Priority Service Users

The key finding of the NSTAC's review of alternative solutions for catastrophic incidents is that both private- and public-sector resources can be better leveraged to address the needs of responders to effectively communicate. Today, the WPS program provides priority for WPS users experiencing call congestion. The program assumes that infrastructure services are available. The NSTAC proposes that an expanded capability using deployable solutions be established. Specifically, the WPS program should be expanded to address restoring wireless infrastructure services to support the WPS community.

Figure 2 illustrates a scenario for rapid communications restoration using deployable COWs and Cell Cites on Light Truck (COLTs) to restore infrastructure services and reconnect authorized WPS users to the surviving portion of the infrastructure. As illustrated in the figure, WPS-authorized handsets and personal digital assistants (PDAs) served by wireless operators in the disaster area (Operators A and B) can be reconnected to available base station controllers (BSCs) and mobile switching centers (MSCs) through any available wireline, microwave, or satellite-based links. Once connectivity to the surviving infrastructure is achieved, responders in the area can use existing WPS and Government Emergency Telecommunications Service (GETS) capabilities to address any over-use issues. The WPS program provides a critical existing operational and administrative platform on which users can be identified, authenticated, and authorized to use the capability once it is deployed. To effectively realize these operational improvements will require significant pre-planning, wireless operator development of processes and procedures, and training.

It is envisioned that Federal and State emergency management agencies would contract carriers to provide this service for re-establishing wireless coverage for WPS support. Equipment would be deployed to affected areas by wireless operators under direction of the Government contracting entity. This equipment is owned, securely stored, and maintained by the wireless operators. The equipment is specifically designed to interface with the wireless operator's BSCs and MSCs, as it will depend on the vendor and technology of connected switching equipment. Depending on the severity of the situation, the Government may need to assist in transporting, deploying, and securing the equipment and establishing connectivity from the mobile asset to an MSC. Policy and procedures should be established for such Government assistance. The mobile assets can be redeployed within a disaster area as the communications needs of the NS/EP personnel change and as commercial service is restored to sections of the disaster area.

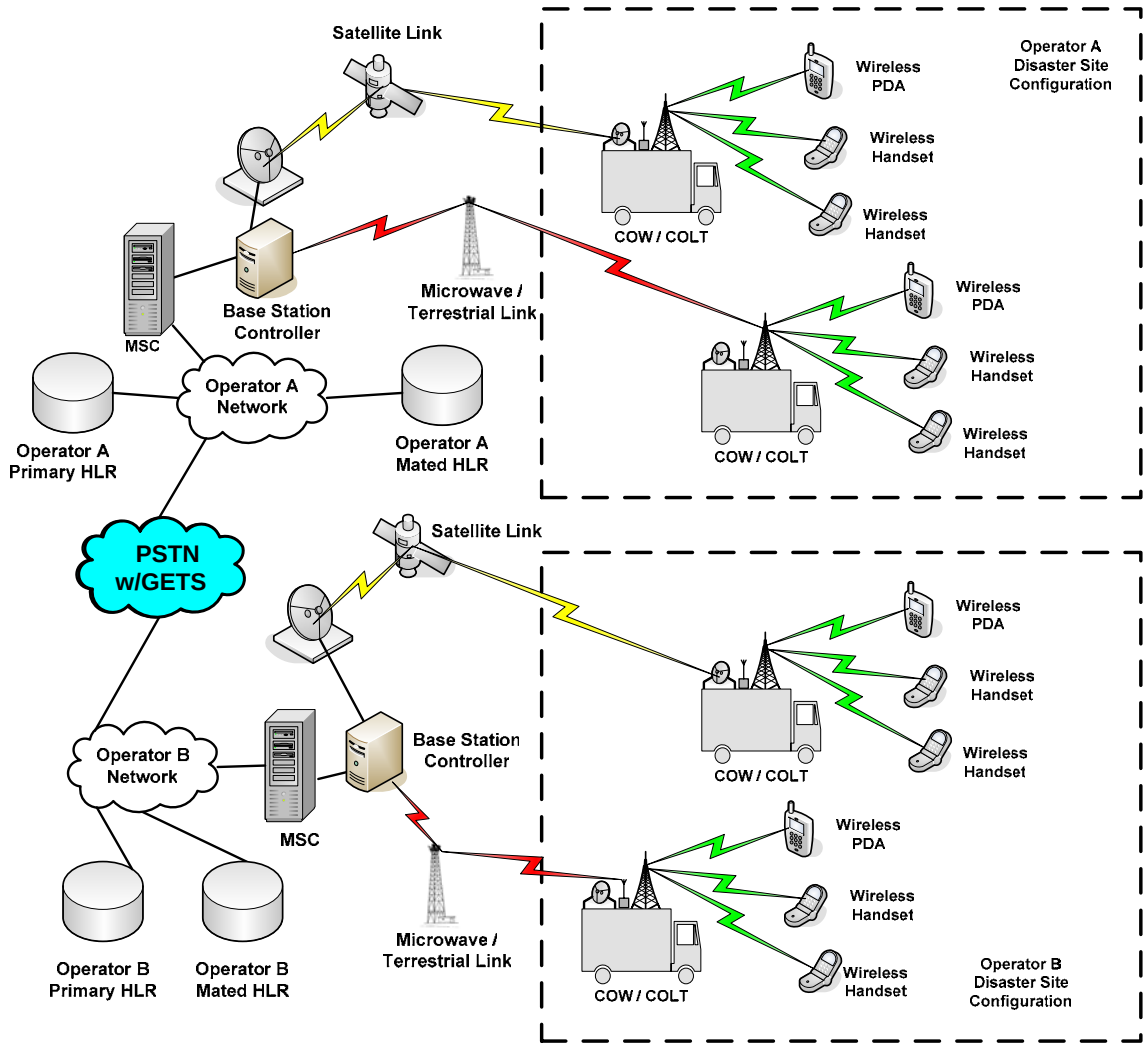

Figure 2—Rapid Restoration of WPS in Incidents of National Significance[17]

During hurricanes, other natural disasters, and many other possible scenarios, chemical, biological, radiological, nuclear, and explosive (CBRNE) events or security hazards may, for a protracted period of time, impede wireless carriers from entering an area to restore wireless services. Using this contracted services approach would better enable the Government to provide pre-planning and support to position these sites and/or facilities. Joint industry–Government research should be supported to explore the technical and financial feasibility for the use of satellite-based technology, aircraft, or aerostat-based communications equipment to provide temporary restoration of service in areas where security and/or CBRNE events prevent access for such restoration.

Expanding the WPS program would complement the actions that carriers have taken to harden the core of their infrastructure. As is typically engineered in today's wireless networks, the home location registry (HLR), illustrated in **Figure 2**, would have both the redundancy and

[17] The diagram only reflects circuit-switched services, such as voice, that are associated with Wireless Priority Service (WPS). Packet-based services are currently not associated with WPS but are under study by the National Communications System (NCS) and could be incorporated.

geographic diversity to maximize survivability when a catastrophic incident occurs. These HLRs contain the databases authorizing WPS service for NS/EP personnel. HLRs communicate with the MSCs through signaling networks, such as signaling system #7, to authenticate and authorize services to wireless subscribers, including WPS subscribers. Wireless operators incorporate the hardening of HLR sites by establishing multiple diverse communication paths for HLR database synchronization and verifying that the HLR configuration for redundancy and geographic diversity maximizes the probability of survivability.

The NSTAC necessarily remains agnostic regarding specific implementation and operational details of a deployable communications program to support an expanded WPS program. Specific development and implementation of this recommendation and assigning roles and responsibilities must accommodate a variety of carrier-specific requirements and incorporate guidance from a diverse cross-section of industry and public-sector stakeholders.

2.1.2 "End-to-End" Priority Services

The FCC and the National Communications System (NCS) should explore whether it is technically and financially feasible for WPS calls to automatically receive GETS treatment when they reach landline facilities. In current implementations of WPS and GETS, a WPS subscriber must have a separate GETS account to receive access to the GETS network. A WPS subscriber must enter his or her GETS access information once granted access to the wireless facilities through WPS. Having independent WPS and GETS accounts adds a layer of complexity for NS/EP users who attempt to quickly access these communications services. As stated in the *Lessons Learned Report*, "…users who had access to these services did not fully understand how to use them (*e.g.*, that a WPS call requires inputting a GETS code so the call would get priority treatment when it reached the landline network.)"[18]

2.1.3 Increasing the Wireless Priority Service User Base

The recommendation of the *Lessons Learned Report* to expand and publicize the use of WPS must be implemented. Specifically, the FCC and NCS should aggressively promote WPS to eligible Government, public safety, and critical industry groups. Examples of titles eligible for WPS include the following:

- Executive Leadership and Policy Makers—Priority One Access (for example, the President of the United States, Military leaders, State Governors, Secretary of Public Safety and Health, Mayors, County Commissioners, and their staff);

- Disaster Response and Military Command and Control—Priority Two Access (for example, Federal Emergency Operations Center Coordinators, National Damage Assessment Team leaders, and personnel with Continuity of Government responsibilities);

[18] *Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks—Report and Recommendations to the Federal Communications Commission*, June 12, 2006, Section II Recovery Coordination and Procedures, part C—Emergency Communications Services and Programs, pg. 21–22.

- Public Health, Safety, and Law Enforcement Command—Priority Three Access (for example, Federal law enforcement command, State police leadership, local fire and law enforcement command, and emergency medical service leaders);

- Public Services/Utilities and Public Welfare—Priority Four Access (for example; United States [U.S.] Army Corps of Engineers leadership; power, water and sewage, and telecommunications utilities; and transportation leadership); and

- Disaster Recovery—Priority Five Access (for example, medical recovery operations leadership, detailed damage assessment leadership, disaster shelter coordination and management, and critical disaster field office support).

These criteria were selected to meet the needs of the emergency response community and to provide access for the command and control functions critical to management of and response to national security and emergency situations, particularly during the first 24–72 hours following an event. Once the WPS program is expanded and more users are on the network, it is critical for the wireless operators to rapidly restore priority wireless services for NS/EP in a disaster area during this 24 to 72 hour period.

2.2 Telecommunications Service Priority Enhancement for Wireless Networks

***Recommendation*: The President should direct the Department of Homeland Security and other responsible Federal agencies to explore enhancements to the Telecommunications Service Priority (TSP) program to accommodate expanded requests from national security and emergency preparedness users of wireless telecommunications services at critical sites. The President should also direct Federal agencies, and encourage State and local agencies, to fully utilize the existing provisions of TSP and to apply for the enhanced wireless TSP coverage provisions as they are developed for use at their critical sites.**

The adoption of wireless telecommunications services has produced a strong reliance on the wireless infrastructure by NS/EP users of those services. When disasters strike, wireless carriers are flooded with requests from different agencies and jurisdictions for restoration of wireless services to key facilities and the provisioning of deployable equipment to provide service at new field offices. Wireless service providers need the ability to identify key sites before a disaster and have a pre-identified method of allocating their resources, such as personnel, equipment, fuel, and generators, to support the most critical missions. Enhancing the existing TSP program to fully encompass anticipated increased requests to provision and restore wireless infrastructure assets is a logical step and an effective means to ensure that wireline and wireless carriers, in conjunction with the Federal Government, can better act on a shared and consistent view of provisioning and restoration priorities during a disaster situation.

2.2.1 The Telecommunications Service Priority Program Today

The NCS operates the TSP program, which establishes a regulatory, administrative, and operational framework for restoring and provisioning priority telecommunications services. The TSP program provides service vendors with a FCC mandate for prioritizing service requests by

identifying those services critical to NS/EP.[19] A telecommunications service with a TSP assignment is assured of receiving full attention, before a non-TSP service, by the service vendor. The TSP program is widely recognized as a successful and effective initiative to speed the provisioning and restoration of vital services for NS/EP users. Following Hurricane Katrina, the NCS completed more than 1,500 TSP assignments to help restore emergency response capabilities in the Gulf States.[20]

The TSP program has two components—provisioning and restoration. A provisioning priority is obtained to facilitate priority installation of new telecommunications services. Provisioning on a priority basis becomes necessary when a service user has an urgent requirement for a new NS/EP service that must be installed immediately—emergency provisioning—or by a specific due date—essential provisioning—that can be met only by a shorter than standard service-vendor provisioning time frame. A restoration priority is assigned to new or existing telecommunications services to ensure restoration before non-TSP services. Priority restoration should be assigned to a new service when interruptions may have a serious, adverse effect on the supported NS/EP function.[21]

While the current TSP program has proven to work effectively and as designed in providing rapid NS/EP telecommunications service provisioning and restoration, TSP application in the wireless network environment can be improved. Historically, TSP has been applied to wireline telecommunications services, connecting two geographic locations (Point A to Point B). Today, wireless service providers qualify for TSP authorization, which they have used primarily for landline trunks that serve cell sites—designated by TSP Priority 3. Other wireless network assets could also benefit from TSP coverage. The actual telecommunications service provider—the wireless carrier, in this case—is usually not apprised of the criticality of the telecommunications service or of its ranking relative to other priorities that must be addressed in a disaster. Wireless carriers have other tools that they can use to restore coverage in the absence of landline backhaul—microwave links, COWS, COLTS, or by repositioning directional antennae from adjacent sites to augment coverage. In many cases, landline backhaul is only one condition that must be addressed to restore service. To be returned to service, the site may need a temporary generator, antennae repairs, cable replacement, or new electronics. Wireless carriers are also deprived of the liability relief TSP offers to landline carriers juggling disparate demands for restoration during a disaster.

2.2.2 Enhancements for Wireless Networks

The NSTAC recommends that the TSP program be enhanced to encourage and include requests from wireless NS/EP users, beyond traditional TSP assignments that apply to landline trunks serving cell sites, to include pre-identified wireless service assets such as cell sites (and associated trunks) that serve critical NS/EP sites and wireless assets that may become critical,

---

[19] The Telecommunications Service Priority (TSP) program is underpinned by FCC rules that require telecommunications service providers to give provisioning or restoration priority to critical circuits supporting NS/EP functions. To qualify for TSP, an applicant must file a formal request to the NCS, meet specific NS/EP criteria, and be granted a TSP assignment (Levels 1–5) by the NCS. The rules of *Title 47* require carriers to restore telecommunications services with TSP assignments before other, non-TSP services are restored. (See *Title 47 C.F.R. Pt. 64*, Appendix A.)

[20] *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, U.S. House of Representatives, September 15, 2006.

[21] TSP Service Description, http://tsp.ncs.gov.

based on an expected event or impending disaster. Initiating an enhanced TSP request process would benefit eligible participants—Federal, State, local and tribal Governments and groups in the private sector such as banking and utilities—to evaluate their emergency communications plans and identify critical NS/EP missions and associated locations that require commercial wireless telecommunications services to carry out those missions. These parties would then submit applications to the NCS to obtain TSP designations for those critical wireless services. The NCS would notify wireless carriers of requests that had been approved and prioritized and the carriers would identify the appropriate wireless service points, for example cell sites. New assignments may also be requested for mobile assets that support temporary NS/EP user locations such as a Federal Emergency Management Agency (FEMA) Joint Field Office.

Because of the dynamic nature of the wireless network environment, characterized by user mobility and roaming capabilities, the NSTAC recognizes that further exploration of current TSP processes and procedures is warranted to identify what revisions are required to better support enhancing TSP efforts for wireless networks. For example, processes may need to be revised to ensure that applying TSP–level assignments for wireless assets and the wireline assets that support them is consistent. Specifically, the local access circuit between the cell tower and switch site, which may qualify for a TSP Level 3 designation under the program today, may need to be examined to ensure that sufficient priority is assigned based on the mission(s) being supported. Existing priority-level assignments should be consistent with any new priority level granted to the wireless service as a result of a new request under the program. The NSTAC stands ready to assist the TSP Oversight Committee in identifying rule or process revisions, if required, and developing an implementation approach to enhance the TSP program, as recommended.

The development of enhanced TSP features for wireless networks will require considerable study and may also require that changes be made in the relevant FCC Report and Order, thus subjecting the implementation of new enhancements to the full regulatory process of the FCC.[22] In the interim, wireless carriers should be encouraged to make full use of the existing provisions of TSP currently applicable to wireless networks. The NSTAC also recommends that the President direct Federal agencies, and encourage State and local agencies, to apply for the enhanced wireless TSP coverage at their critical sites when those provisions become available. The NSTAC endorses the associated finding of the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks to actively and aggressively promote GETS, WPS, and TSP to all eligible Government, public safety, and critical industry groups.[23] The Priority Services Working Group (PSWG), a working body of the NCS Committee of Principals (COP), also recently endorsed increasing outreach to users of NS/EP telecommunications services and mitigating the cost barriers to greater TSP participation.[24] The cost of participation is the primary reason that many State and local emergency organizations do not participate in the TSP program. This is unfortunate, because these entities

---

[22] See Footnote 19.

[23] *Report and Recommendations to the FCC*, Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, June 12, 2006.

[24] The PSWG found that many entities that conduct essential NS/EP functions are not aware of the TSP program or the benefits it can provide in improving reliability and restoration of essential communications services. The PSWG report makes a number of recommendations to improve these outreach efforts and to expand their scope. *Report on Telecommunications Service Priority*, NCS Committee of Principals—Priority Services Working Group, June 2006.

provide essential emergency functions during disasters and are key partners with the Federal Government under the *National Response Plan (NRP)*. The NSTAC supports the PSWG recommendation that the DHS make available grant funding specifically for TSP initial costs for 911 centers and State and local emergency operations centers.[25]

[25] The PSWG specifically recommends that the DHS make available a one-time grant of $8 million, as a special set-aside, to enable State and local emergency operations centers and 911 centers to enroll their essential telecom circuits in the TSP program.

3.0 INPUTS TO THE NATIONAL EMERGENCY COMMUNICATIONS STRATEGY

The *Lessons Learned Report* specifically called for the review of current laws, policies, plans, and strategies relevant to communications and the development of an integrated *NECS* to support communications operability and interoperability. In soliciting the advice of its communications sector partners, the White House recommends in the report that:

> "the development of an overarching *National Emergency Communications Strategy* should address a full range of hazards…and should consider the direction of the telecommunications industry and supporting recommendations of the President's National Security Telecommunications Advisory Committee."

Additionally, in the *DHS Appropriations Act of 2007 (The Act),* Congress directs DHS to develop and periodically update the following:

> "a *National Emergency Communications Plan* to provide recommendations regarding how the U.S. should (1) support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and (2) ensure, accelerate, and attain interoperable emergency communications nationwide."[26]

Since its inception, the NSTAC has addressed a wide range of issues regarding the importance of protecting and restoring the Nation's communications infrastructure to maintain vital national NS/EP functions when a national disaster occurs. Per White House and Congressional direction, the NSTAC offers input to the *NECS* and the *NECP* in three areas:

- A recommendation to expand and clarify NS/EP policy guidance to better encompass the Nation's emergency communications needs and objectives;
- A recommendation to consider and emphasize critical elements in the development and execution of *NECS* and *NECP*; and
- A recommendation identifying capability objectives that will assure a more survivable and interoperable emergency communications architecture in the future converged environment.

[26] The NSTAC recommendations in this report are offered as guidance and input to developing the *NECS*, the *NECP*, and any subsequent implementation guidance.

3.1 Expansion of National Security and Emergency Preparedness Policy to Support Emergency Communications

***Recommendation*: The President should modernize existing national security and emergency preparedness (NS/EP) policy guidance to clarify and consolidate Federal Government emergency communications roles and responsibilities. Specifically, additional Presidential policy guidance is required to:**

- **Clearly delineate the NS/EP and emergency communications roles and functions of the National Communications System, the National Cyber Security Division, and the new Office of Emergency Communications, as established by the *Department of Homeland Security Appropriations Act of 2007*, and any other DHS organization, such as the Science & Technology Directorate and the Federal Emergency Management Agency, with a role or responsibility in the area of emergency communications;**

- **Preserve and maintain critical NS/EP functions and capabilities that support the National leadership; and**

- **Ensure Executive oversight across the Federal Government for a fully coordinated, integrated, and interoperable emergency response communications function and capability.**

Executive Order (E.O.) 12472—Assignment of National Security and Emergency Preparedness Telecommunications Functions, signed in 1984 by President Reagan, remains the guiding authority for NS/EP telecommunications.[27] E.O. 12472 established the NCS as a Federal interagency group assigned NS/EP telecommunications responsibilities throughout the full spectrum of crises and emergencies. Under the policy objectives stated in E.O. 12472 and National Security Decision Directive 97, these responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunications resources to support the Government during any emergency.

E.O. 12472 also establishes an organizational framework through which the NCS can accomplish its mission, which includes the COP that serves as a forum for NCS member agencies to evaluate NS/EP telecommunications programs and activities; and the National Coordinating Center, which serves as the operational hub for joint industry–Government operational planning and support for NS/EP service coordination, restoration, and reconstitution. The E.O. also charters the Joint Telecommunications Review Board (JTRB) for adjudicating resource needs in a crisis.

For more than 20 years, the NS/EP telecommunications policy framework instituted by E.O. 12472 has served the Nation well. However, fundamental changes in organizations, missions, and structures; rapid evolution of underlying communications technology and

[27] "NS/EP Communications" is defined in 47 CFR 201.2(g) as "communication 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 U.S."

infrastructures; and an increasing number and range of threats require some fundamental policy realignments to assure readiness and functionality for future crises.

From the organizational perspective, consolidation of several operational missions related to NS/EP and emergency communications was achieved with the creation of the DHS in 2002.[28] Under the existing E.O. 12472 policy framework as augmented by a number of Homeland Security Presidential Directives (HSPD),[29] organizational consolidation under DHS continues to present opportunities to realize efficiencies through activity and mission coordination and to leverage shared resources to better meet NS/EP and emergency communications needs. From the technology perspective, today's evolution toward a primarily digital packet-based communications infrastructure capable of supporting high-speed multi-media communications among a diverse range of end-user devices is an enormous leap forward from the analog, circuit-switched, voice-based technologies that prevailed when E.O. 12472 was signed. From the threat perspective, the post-September 11th environment is characterized by a fundamentally different type of threat as compared to the monolithic nation-state threat of the Cold War era, in that it emphasizes a greater need for assuring emergency response and critical infrastructure communications. All these changes underscore the need for continued vigilance in ensuring that existing NS/EP telecommunication policy framework remains responsive to evolving NS/EP and emergency communications needs.

With the recent issuance of *The Act*, the need for Presidential implementation and policy guidance is critical to ensure seamless integration of NS/EP and the new legislative requirements for emergency communications. Through *The Act*, Congress has mandated the reorganization of the DHS preparedness capabilities, establishing several new organizational entities:

- The Emergency Communications Preparedness Center will serve as the focal point for interagency efforts and as a clearinghouse to support and promote emergency response provider communications and interoperable emergency communications;

- Regional Emergency Communications Coordination (RECC) Working Groups will assess the sustainability and interoperability of local emergency communications; and

- A new Office of Emergency Communications (OEC) will have broad responsibilities for emergency communications and interoperability, including developing and maintaining the *NECP*.[30]

---

[28] The DHS was established by the *Homeland Security Act of 2002*.

[29] Since 2003, the President has issued several important directives for overcoming the significant challenges related to establishing national-level emergency communications, command, and coordination capabilities in response to significant all-hazard incidents. HSPD-5 directs the development of a new *NRP*, based on the *National Incident Management System* template, to align Federal coordination structures, capabilities, and resources into a unified, all- discipline, and all-hazards approach to domestic incident management. HSPD-7 requires DHS to maintain "a focal point for cyber security analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems." Additionally, NSPD-28 calls for a "national command and control capability."

[30] Under *The Act's* subtitle addressing emergency communications, "*21st-Century Emergency Communications Act of 2006*," the Office of Emergency Communications is established with several responsibilities, including SAFECOM [a communications program of the DHS's Office for Interoperability and Compatibility] and program administration roles within the Integrated Wireless Network; promoting interoperable emergency communications, requirements and standards; coordinating the NCS; developing best practices and Standard Operating Procedure; information sharing; emergency communications plan reviews; and developing and maintaining the *NECP*.

Each new organizational entity is granted legislative authority for responsibilities that often complement but also overlap existing NS/EP roles within the DHS and NCS as authorized under E.O. 12472. The NSTAC fully endorses the goals of *The Act*, including the creation of the new OEC, to better consolidate emergency communications interoperability functions. However, additional guidance from the President is required to clarify the appropriate authorities, roles, and responsibilities across the multiple stakeholders to ensure full coordination and consistency of all Government emergency communications planning and response. For example, such guidance could ensure that critical communications issues from the newly created entities can access the JTRB through the Manager of the NCS. Further, such guidance may modify the current COP and Council of Representatives process or potentially establish a new interagency policy mechanism to support the NCS and the newly created functions. Modernizing the NS/EP framework and structure set forth in E.O. 12472 ensures that the Executive Office of the President (EOP) and all levels of Government can rapidly respond to and manage incidents of national significance.

The NSTAC membership also advocates Presidential clarification and expansion of NS/EP policy to realize additional, vital organizational and operational benefits. First, organizational emergency communications responsibilities, as delineated in *The Act*, clearly recognize and incorporate lessons learned from the Hurricane Katrina response. HSPD-5, HSPD-7, HSPD-8, and National Security Presidential Directive 28 (NSPD 28) are also informed by and reflect the post-September 11th environment in which they were issued. Additional guidance from the President would serve to unify various emergency communications roles and responsibilities in E.O. 12472 with other salient policy documents and plans—*NRP, National Infrastructure Protection Plan*—and ensure that critical elements of the HSPDs are fully integrated with the new requirements of *The Act*.

Second, issuance of additional policy guidance, such as an E.O. or HSPD, could explicitly address, at the President's discretion, the ambiguity between the traditional interpretation of "NS/EP" (that is, support of national security leadership) and the more expansive interpretation of roles related to NS/EP and emergency communications to include first responders, critical infrastructure sector owners and operators, and cyber security and public warning stakeholders. Such clarification would enable more focused and integrated planning and execution of crisis-related communications across the appropriate range of stakeholders while ensuring no dilution of support to the critical "high-end" NS/EP telecommunications needs, up to and including Enduring Constitutional Government. It would also afford an opportunity to re-affirm the essential EOP oversight role and provide clarity of leadership and focused understanding necessary to address complex integration issues associated with the impeding emergency communications and interoperability agenda prescribed by *The Act*.

The NSTAC recognizes that the NS/EP telecommunications concept builds on decades of legal, regulatory, and policy precedence, thereby providing a solid foundation for broad mission execution. Furthermore, the NSTAC recognizes the multiple efforts to review the NCS functions and missions in light of convergence; the basic tenets of E.O. 12472 have been judged to be sound. However, the scale, scope, and character of change brought about by *The Act* obligate careful consideration of whether clarifying direction from the President, particularly with regard to emergency communications roles and responsibilities, is warranted. The NSTAC member companies believe that issuance of such policy guidance reflecting the President's intentions for

the new realities of emergency communications will keep Federal, State, local, and tribal Governments on the path to continued success.

3.2 Critical National Emergency Communications Strategy Elements

Recommendation*: The President should incorporate the following critical elements in the development, maintenance, and execution of the *National Emergency Communications Strategy* and associated implementation guidance, and also direct the Department of Homeland Security and other responsible Federal agencies to incorporate the elements into the *National Emergency Communications Plan:

- **Large-Scale State and Regional Shared Public Safety Networks and Federal Grants;**
- **Yearly Benchmarks for Achieving Defined Interoperability Objectives;**
- **Nationwide Outreach to Support Emergency Response Communications;**
- **Consolidation of Operations Centers to Increase Coordination and Situational Awareness; and**
- **Identification of Specific Private-Sector Emergency Communications and Interoperability Support Roles.**

In evaluating barriers to effective emergency communications operability and interoperability and approaches to further enhance emergency response command and control and situational awareness, the NSTAC has identified several critical elements for Government consideration and emphasis in its development and execution of the *NECS*. These elements should also be considered and emphasized by the new OEC in its development and implementation of the *NECP* and other relevant emergency communications plans, processes, and initiatives. Additional detail on each identified element is provided in the following sections.

3.2.1 Large-Scale State and Regional Shared Public Safety Networks and Federal Grants

A key enabler and best practice for public safety communications interoperability is the existence or planned deployment of statewide or regional networks. Many States and regions have significant investments in these large-scale, shared, public safety networks, and much of the communications equipment used by emergency responders is being upgraded to standards-based digital equipment. These networks offer a high degree of interoperability within their geographic coverage areas and can be linked to other networks through gateways, which improves communication between State and local Governments and between neighboring local jurisdictions. The NSTAC supports encouraging, developing, and promoting by incentives those large-scale State and regional shared public safety networks to enable cost-effective and common-approach, public safety, interoperable emergency response capabilities.

Beyond the technology implications, Federal grants that encourage increased levels of coordination and cooperation among Federal, State, local, and tribal public safety agencies by establishing multidisciplinary, cross-jurisdictional governance structures will improve regional

collaboration and promote efficient use of funding devoted to public safety communications. Failure to use grant funding in accordance with relevant State and regional interoperability plans would be grounds for denial of future grant applications from that jurisdiction.

Additionally, in its November 2006 report, *Strategies For States To Achieve Public Safety Wireless Interoperability,* the National Governors Association (NGA) recommends institutionalizing a governance structure that fosters collaborative planning among local, State, and Federal Government agencies.[31] The report also recommends encouraging the development of flexible and open architecture and standards. The NSTAC endorses these recommendations and plans to fully consider the NGA findings as a part of its ongoing emergency communications and interoperability efforts.

3.2.2 Yearly Benchmarks for Achieving Defined Interoperability Objectives

The NSTAC supports yearly benchmarks for achieving defined emergency communications and interoperability objectives with Federal grants tied to measurable progress along an interoperability continuum.[32] As stipulated in *The Act*, an emergency communications baseline assessment includes a national interoperable emergency communications inventory and seeks to identify the interoperable emergency communications systems used by public safety agencies in the U.S.[33] Once the RECC Working Groups are established, the first priority of each group must be the development of a comprehensive, integrated interoperability plan for its region. That regional plan will then provide the framework for local implementation of the *NECP*. To ensure consistency between the regional plans and the *NECP*, all Federal interoperability grants to regional, State, local, and tribal authorities must be predicated on the recipient's participation in and adherence to their respective regional or State interoperability plan.

3.2.3 Nationwide Outreach to Support Emergency–Response Communications

To implement comprehensive and wide-ranging emergency communications and interoperability functions authorized by *The Act*, the DHS must work closely with professional organizations of fire fighters, police, and emergency medical technicians (EMT); national associations of U.S. cities, counties, tribes, and States; mayors, governors, industry leaders, and other interested parties. Improving emergency communications and interoperability requires both a national focus and a local engagement. To ensure that forward–focused strategies and policies can be implemented in ways that best serve America's first responders and the public they protect, the assistance and expertise of knowledgeable representatives from *bona fide* National-level public safety associations are required to effectively develop Federal NS/EP and emergency communications strategies and policies.

Establishing strong relationships with key stakeholders will enable the NCS and the OEC to understand and foster increased interoperability among emergency responders. By making information about the status of interoperability progress available to all stakeholders, including public officials and the media, the OEC can enhance the likelihood that its efforts will be

---

[31] *Strategies For States To Achieve Public Safety Wireless Interoperability,* National Governors Association, November 20, 2006.

[32] Benchmark objectives should include statements on standards and investment directives for State and local agencies.

[33] *The Act,* Section 1803, Assessments and Reports.

successful. Widespread dissemination of information will also permit the public, along with public safety and emergency agencies across the country, to benefit immediately from the OEC's efforts. *The Act* imposes several reporting obligations on DHS and/or the OEC. The OEC should embrace those reporting requirements and, in fact, augment them wherever necessary to ensure maximum transparency of both the progress toward and the challenges to achieving the goal of nationwide emergency communications interoperability. Once the OEC completes the initial *NECP*, it should consider annually reporting the progress towards the Plan's objectives. Given the heightened risks faced by urban and high-threat areas, the OEC should consider delivering a series of semi-annual reports on interoperability progress in those jurisdictions. Finally, in light of the urgent need for agreement on technical standards to facilitate interoperability efforts, the OEC should also consider semi-annual reports on the progress of developing national voluntary consensus standards. Collecting information to be used in such reports will also aid DHS in ensuring that Federal interoperability grant funding is being used in an appropriate and timely manner.

3.2.4 Consolidation of Operations Centers to Increase Coordination and Situational Awareness

The Federal Government currently separates various coordination and operational functions by expertise. According to a recent GAO report, DHS operates approximately 25 different 24x7 operations centers, only four of which function as multi-agency entities.[34] For example, the Network Operations Center, the National Infrastructure Coordination Center, the National Communications Center, the United States Computer Emergency Readiness Team (US-CERT), and other emergency operations all operate separate assets and processes that must be integrated into a logical framework. The autonomous nature of these entities creates some organizational flexibility but also individual bureaucracies that must compete for resources within the DHS system.

Assessing their respective strengths, authorities, resources, and intellectual properties could enable the DHS to organize the functions into architecture that supports a national-level command and control situation awareness capability, which currently does not exist. The DHS can move beyond operations with big-screen broadcasting of popular news channels and seek to access and leverage information feeds directly from the source. Rather than competing for better information sources, DHS operations centers, where appropriate, may be able to gather data in a cohesive and sophisticated manner that will yield powerful situational insights and better equip decision makers to act with clarity. Furthermore, once programmatic elements and their budgets are organized into an overarching program, the DHS can better budget and resource the overall functions, in much the same way that the Joint Staff provides national-level support to its Chairman in concert with relevant agencies—the Department of Defense (DOD) and the Central Intelligence Agency (CIA)—to support National Command Authorities. Establishing and maintaining a national command and coordination capability requires programmatic support and training for interagency knowledge-management systems that can be accessed by responders in all circumstances.

[34] *Opportunities Exist to Enhance Collaboration at 24/7 Operations Centers Staffed by Multiple Department of Homeland Security Agencies*, Government Accountability Office, October 2006 (GAO-07-89).

3.2.5 Identification of Specific Private-Sector Emergency Communications and Interoperability Support Roles

The NSTAC's identification of private-sector support and coordination roles can ensure the success of the emergency communications policy framework and objectives of *The Act*. The NSTAC's overarching goal in identifying this element of the *NECS* and *NECP* is to enhance collaboration across organizational and jurisdictional boundaries to help our country better prevent, prepare for, respond to, and recover from disasters and emergencies. The NSTAC and other organizations reviewing Hurricane Katrina findings all recognized the need for a unified response. Congress recognized consolidation was required and *The Act* unifies Federal emergency communications and interoperability programs under a single office to clarify and improve jurisdictional and organizational roles and responsibilities.

As defined in *The Act*, the *NECP* requires interagency coordination and cooperation and the consolidation of significant activities across the DHS, including many non-DHS entities. For example, the plan contemplates input from Federal departments and agencies, State, local, and tribal Governments, the NCS, emergency response providers, and the private sector. Emergency communications capability and interoperability requires more than technology; integrating all elements requires a comprehensive, coordinated strategy: governance, SOPs, technology, strategy, training and exercises, and use. The NSTAC will make available the combined experience and expertise of its membership to share industry's perspective and help the OEC and other parties to develop this critical *NECP*, including the following:

- Providing industry assistance in the development and periodic update, as appropriate, of the *NECP;*
- Advising and providing industry input to the NCS to establish a national response capability when a catastrophic loss of local and regional emergency communications services occurs;
- Providing industry technical assistance toward developing interoperable emergency communications capabilities;
- Helping facilitate nationwide outreach to support emergency–response communications for Government officials and emergency responders;
- Participating with and providing industry coordination resources for the RECC Working Groups; and
- Capturing and promulgating best practices with respect to using interoperable emergency communications capabilities for incident response.

A wide range of Government and private-sector partners bring core competencies that add value to the strategy and plan. Industry ownership and management of a vast majority of communications infrastructure, and visibility into these assets, networks, facilities, functions, and other capabilities, combined with the ability to take initial actions to respond to incidents and the

ability to innovate and to provide products, services, and technologies to quickly focus on requirements, point to the value of industry participation.

3.3 Emergency Communications in the Converged Environment

***Recommendation*: To encourage responsive emergency communications capabilities in the converged environment, the President should establish and incorporate the following capability objectives into the *National Emergency Communications Strategy* and associated implementation guidance, and also direct the Department of Homeland Security to incorporate the capability objectives into the *National Emergency Communications Plan*:**

- **Support for a Significantly Expanded User Base;**
- **Full Leveraging of Network Assets;**
- **Internet Protocol–based Interoperability;**
- **Assured Access for Key Users through Priority Schemes or Dedicated Spectrum;**
- **National Scope with Common Procedures and Interoperable Technologies;**
- **Deployable Elements to Supplement and Bolster Operability and Interoperability;**
- **Resilient and Disruption-Tolerant Communications Networks;**
- **Network-Centric Principles Benefiting Emergency Communications; and**
- **Enhanced Communications Features.**

As a starting point in its evaluation of emergency communications in the future converged network environment, the NSTAC reviewed its previous findings regarding the provision of NS/EP services on the Next Generation Network (NGN). The convergence of wireless, wireline, and IP networks into global NGNs fundamentally impacts Government needs for NS/EP and emergency communications today and in the future. As bandwidth and software continue to improve, the NGN will offer significant improvements for both NS/EP and emergency communications, but the transition to the converged environment will present challenges for ensuring the security and availability of these communications assets.[35]

New communications capabilities, including greater access to data and new services, will support NS/EP and emergency communications functions in critical ways by enabling emergency responders, for example, to obtain real-time access to voice, data, and video necessary for the most effective completion of their missions. The NGN will also naturally increase network robustness and resiliency by the nature of its architecture, offering many possible paths for

[35] *NSTAC Report to the President on Next Generation Networks* recommends assistance to "first responders and public safety organizations in making the transition to the NGN…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…[and] also aid interoperability in cases where 'operability' of first responder and public safety networks and the NGN itself are present."

service and redundancy of equipment and servers. In short, the future converged environment will provide new capabilities and greater resiliency. For example, recent work within the International Telecommunications Union on NGN has identified emergency communications services as a core capability to be supported by the NGN. Furthermore, wireless IP Multimedia Service (IMS) has been identified as an important first step toward the NGN. With deployment of IMS expected within the next few years, IMS requirements to support NS/EP capabilities should be developed so that emergency communications services can benefit from its deployment. The potential exists for improvements in WPS and integration with and augmentation of stand-alone public safety communications systems. The NSTAC recommends incorporating specific vital and critical capability objectives into the *NECS*, *NECP*, and associated implementation guidance. The capability objectives are detailed in the following sections.

3.3.1 Support for a Significantly Expanded User Base

While disaster preparedness and response to most incidents remains a State and local responsibility, recent events have demonstrated the need for greater integration and synchronization of preparedness efforts among a dynamically expanding user base beyond traditional first responders, such as public safety, National Guard personnel, critical infrastructure providers, NS/EP users, and public health system users. Capabilities and approaches that are scalable to meet the needs of a potentially significantly expanded user base of approximately 8-10 million emergency responders must be investigated. Users embrace technology preferences that have evolved to support missions and roles and provide an ease of use gained through a user's experience with such systems and technologies. Interoperability is essential across these technologies and their underlying network assets. Solutions need to empower existing technologies rather than provide users with new devices or capabilities in the heat of an emergency. Users need to be able to turn to the "trusted" solutions with which they are familiar.

Current emergency communications processes focus primarily on traditional first responders (fire, police, and EMT), with primary interest in voice communications. During the first few hours of a major regional or local emergency, the communications of "first responders" are vitally important in saving lives and coordinating response actions, and the bulk of these communications have historically been voice communications. As the emergency continues to unfold and response actions proceed, additional types of responders become increasingly important in coordinating response and recovery. This broader range of organizations and individuals play critical roles in response and recovery. This population totals approximately 8-10 million users nationally and encompasses the following representatives:

- 2.5 million First Responders (Police, Fire, EMT);
- National Response and Federal Response Plan users;
- National Incident Management System (NIMS) users;
- NS/EP users;

- Federal Agencies with Public Safety, Investigation, and Asset Protection Missions, for example Federal Law Enforcement, Transportation Security, Border Security, and the FEMA;
- Critical Infrastructure owners, operators, decision makers;
- Key municipal leadership and decision makers;
- Military Support, for example U.S. Northern Command and the National Guard;
- Public health systems, for example hospitals, the Red Cross, and the Center for Disease Control and Prevention (CDC); and
- Licensed Amateur radio operators.[36]

Another way to characterize the emergency communications and interoperability user base is to clarify what types of organizations these individuals represent, including more than 100,000 organizations[37] comprised of the following:

- 19,000 law enforcement offices and agencies;
- 33,000+ fire and rescue organizations;
- 7,500+ Public Safety Access Points (PSAP's) handing 911 and similar services;
- 8,000+ public–health departments;
- 5,600 hospital emergency departments;
- 5,000+ critical-care facilities;
- 1,000+ emergency management departments;
- Private–Sector Non-Governmental Organizations;
- Public works and transportation officials;
- Federal agency response coordination officials, for example the DHS, the Department of Health and Human Services, and the CDC; and
- State and Municipal leadership (Governors, Mayors, and other key municipal leaders and decision makers).

[36] Licensed amateur radio operators, numbering more than 700,000, may be the single largest group of trained communications operators in the U.S.

[37] This is the focus that one coordinating body, COMCARE, Emergency Response Alliance , uses to characterize users, including more than 100,000 organizations.

Emergency communications solutions must be able to serve these expanded populations of users, including providing interoperability among the differing technologies that these users and organizations use and prefer. Interoperability must be improved today, taking advantage of the rapid evolution of emerging technologies while ensuring interoperability with existing communications capabilities. A more formal understanding of the specific services, requirements, and technical characteristics associated with emergency communications is required to better leverage existing and future communications capabilities.

With the ubiquity of multi-function wireless devices such as phones and PDAs, individuals can capture voice, imagery, and textual descriptions of the "on-the-ground" situation. In some instances, circumstances may enable ordinary citizens to assist with emergency response or emergency–alerting roles; designers of emergency communications architectures should contemplate how these systems might scale, contend with, and support inputs from these ad hoc participants, particularly in critical circumstances.

3.3.2 Full Leveraging of Network Assets

Vital decision makers who use existing emergency communications systems employ a broad range of technologies that span a breadth of networks. See **Figure 3**. Solutions should encompass the benefits of new technology and capabilities while leveraging existing investments in current infrastructures and training. New and old networks must interoperate, and wireless devices may be required to work in a variety of networks.[38] Together, they will form the system of systems, with the following natural network hierarchy:

- Personal Area Networks—These support inter-device communications for devices carried by first responders, such as health monitors, hazardous materials sensors, and breathing apparatus;

- Incident Area Networks—These include temporary networks created for specific incident management and coordination, including deployable capabilities that restore lost network capabilities or bolster and supplement existing network communications assets;

- Jurisdictional Area Networks—Main communications networks for first responders. These include all non-incident area voice and data traffic and any incident area network traffic that requires access to general networks and provides connectivity to extended area networks; and

- Extended Area Networks—These networks link city, county, regional, State, and National systems.

[38] *Statement of Requirements for Public Safety Communications & Interoperability*, Department of Homeland Security, SAFECOM Program, Version 1.0 of March 10, 2004.

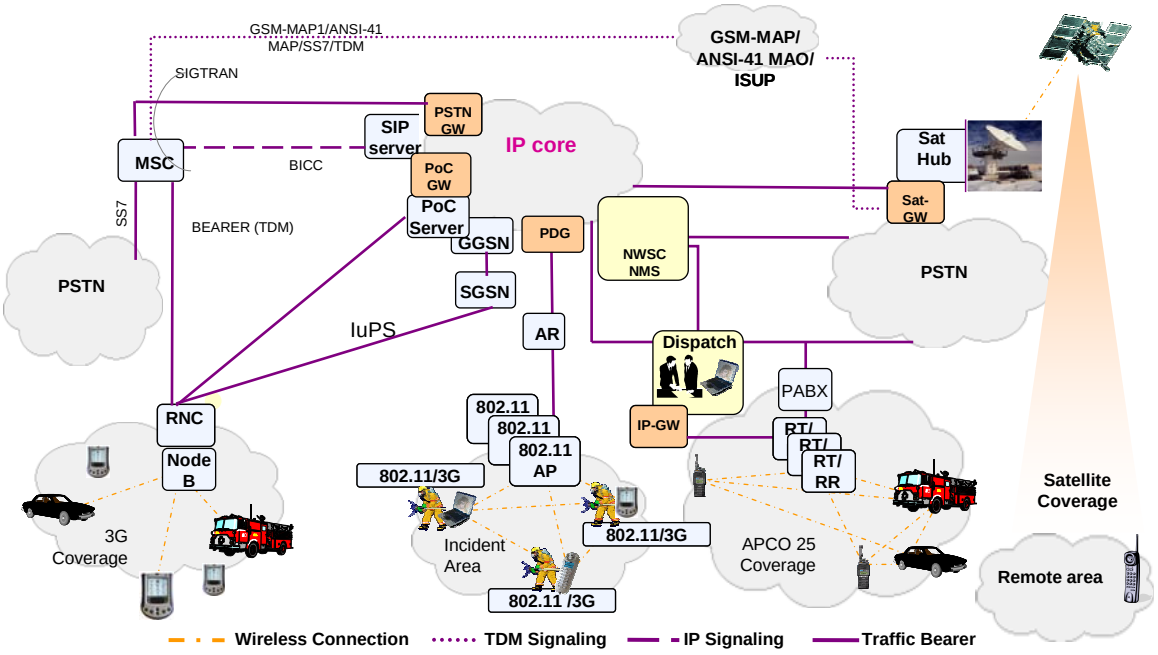

Figure 3—Example of Emergency Communications in the Converged Environment[39]

The goal is to provide interoperable communications infrastructure shared across cooperating Federal agencies, public safety agencies, and regional response teams and their leadership. This approach will support the use of heterogeneous access technologies while taking advantage of the latest advances in the full range of wireless technologies. Furthermore, network approaches should provide access to common services regardless of the air interface technology, including the following:

- Real and non-real-time IP multimedia services;
- Common authentication, mobility and security services;
- Push-to-talk services across all interfaces; and
- Unique, mission–critical, public safety features and functionality.

The worldwide convergence of communications on IP networks provides a strong base on which to build future interoperability.

3.3.3 Internet Protocol–based Interoperability

Public safety wireless networks are being built on a mission-critical IP backbone that leverage multi–cast IP protocols to efficiently and effectively distribute mission-critical voice and data in what are predominantly group-oriented communications. Many of today's interoperability gateways support bridging of disparate communication technologies by converting LMR and

[39] Source: Project MESA http://www.projectmesa.org.

cellular voice audio into Voice over IP (VoIP) protocols and then leveraging the ubiquity of wired IP networks as a common transport medium to unify disparate agency networks. Multiple vendors have introduced scalable IP-based systems for interoperability that are designed to work with existing and future radio-based and wireline systems, including legacy public safety radio networks, new radio networks, and other communications platforms—cellular, cellular push-to-talk, satellite, VoIP, and telephony. Gateways retransmit across multiple frequency bands and/or systems, thereby providing an interim interoperability solution as agencies move toward shared systems. Today's various IP gateways do not interoperate in part because of conflicting VoIP protocols.[40] Furthermore, they often support only a basic audio patch to the different access networks; to improve end-to-end services and achieve interoperability between these IP gateways, it will be necessary to drive the adoption of interoperable protocols for transporting emergency communications services across IP networks.

Adopting interoperable protocols, including the development of a shared core of emergency services such as authentication, authorization, directory, and alerting services, could provide to users the ability to extend emergency communications services seamlessly across all wired or wireless IP networks, whether a Government-owned network or a public or enterprise-owned network. This would allow user devices that supported either one or all multiple standards, including Project 25, 3G Cellular/4G broadband, and Wi-Fi (2.4 GHz and 4.9 GHz), to interoperate with common end-to-end audio and security with the radios carried by first responders. Emergency responders with either multiple single-mode access devices or with new multi-network access devices would then be able to use any multiple available access network for their emergency communications. Some next generation satellites will have IP routing capabilities that will permit true broadband interoperability and performance. MSS providers will incorporate NS/EP features in their next generation satellites.

3.3.4 Assured Access for Key Users through Priority Schemes or Dedicated Spectrum

Key decision makers among the full range of national responders must have assured access to communications channels to support their ability to coordinate response and recovery throughout all stages of emergencies, even in worst-case scenarios. Assured communications can be provided through a variety of methods and technology approaches, including the following:

- Priority access processes such as the Wireless Priority Access Service that was developed and implemented by the NCS following September 11th. This system established priority access for key NS/EP users of cellular communications networks (both Global Systems for Mobile Communications [GSM] and Code Division Multiple Access [CDMA]). Such processes would use existing commercial bandwidth to provide assured access for key emergency communication decision makers and thus would be possible only if the existing bandwidth supports such assured access for priority users; and

[40] In some cases, VoIP protocols do permit disparate systems to communicate and negotiate common parameters, thereby allowing such communication. Additional barriers to interoperability include a lack of or dissimilar back-office systems providing authentication and authorization. To achieve full interoperation, integration and/or interoperation of gateway control systems and/or architectures is required.

- Dedicated channels for key decision makers supported by dedicated spectrum, should existing commercial bandwidth be inadequate.

3.3.5 National Scope with Common Procedures and Interoperable Technologies

A solution for emergency communications must be national in scope, with commonly understood procedures and interoperable technologies to allow key decision makers, local responders, Federal and industry responders to interoperate as required, anywhere in the Nation. Wherever responders deploy, they should be supported by a range of interoperable solutions and approaches, with functionality built in to our communications infrastructure and complemented by deployable, drop-in mobile capabilities to supplement regional infrastructures that may have been rendered inoperable. Further, this flexibility should be supported by developing commonly understood procedures for responding to and managing communications challenges. This national scoping should not only support national responders, but also include provisions to allow the public to have assured access to communications, such as 911, in emergencies.

3.3.6 Deployable Elements to Supplement and Bolster Operability and Interoperability

As recommended in **Section 3.1** of this report, deployable elements are critical to all emergency communications solutions and can be used to bolster the available bandwidth that supports emergency response personnel and the populace within regions impacted by an incident. In addition to the DHS incorporation of rapidly deployable, interoperable mobile communications solutions, the NSTAC emphasizes that the use of capabilities such as cellular, LMR, mesh networks, WiFi hotspots, MSS, satellite access through VSAT services, hybrid satellite–terrestrial devices, and Rapid Overhead Communication Operational Networks[41] be considered and integrated into all Federal, State, local, and tribal emergency communications planning processes. The NSTAC recommendation specifically encourages broader use of deployable elements if existing infrastructure has been lost or is no longer operable, and notes the criticality of equipment and service pre-arrangement and coordination.

3.3.7 Resilient and Disruption-Tolerant Communications Networks

Terrestrial networks, no matter how hardened, are subject to destruction in a major terrorist event or natural disaster. Technologies that facilitate the seamless delivery of voice and data communications across redundant and/or parallel systems that withstand natural and man-made disasters, such as satellite or broadband mesh networks, are important tools. Mesh devices can self-form networks and LMRs can talk unit-to-unit today, but at an incident without any surviving infrastructure, how do users communicate out of the incident scene or support a geographically large incident area? Seamless mobility across all networks will provide a higher probability of finding a surviving infrastructure, but, in the extreme, there may be no surviving infrastructure. Satellite communications can provide backup communications for emergency purposes by extending the IP backbone to the scene of the incident and providing connectivity for deployable networks when existing terrestrial infrastructure is not available. Satellite systems cover vast regions and are immune from earthquakes, hurricanes, and most terrorist

[41] Rapid Overhead Communication Operations Network (ROC-ON) capability is described in *ROC-ON* Joint Capabilities Technology Demonstration (*JCTD), FY07-09.*

attacks. Thus they play an important role when terrestrial systems have been destroyed by a recent disaster and in sparsely populated areas in which terrestrial coverage is unavailable or too expensive to be widespread. Networks must include some form of satellite communication to be fully resilient and redundant.

3.3.8 Network-Centric Principles Benefiting Emergency Communications

During the late 1990s, the DOD began to evolve a new type of operational doctrine labeled "network-centric."[42] Net-centric principles are characterized by agile, flat, rapidly changing connections and relationships. Such flat hierarchical structures allow information to move rapidly among stakeholders and participants. National-level emergency communications begin and grow organically from various "on-the-ground" elements, including individual citizens, local responders, for example police, 911 operators, and fire fighters. Local nodes such as PSAPs often act as sensors and situational awareness points that are essential to developing a common operational understanding of an incident. The overlapping jurisdictions at State, local, and tribal organizations can also potentially create redundant communication paths and "flat" networks that can support the needs of a national-level command control situational awareness structure envisioned by the NIMS and NSPD 28. A network-centric approach to emergency communications will require the close coordination of the NCS, the OEC, and the NCSD and buy-in from State, local, and tribal Governments and private enterprises and citizens to develop, maintain, and execute in times of crisis.

3.3.9 Enhanced Communications Features

Solutions for emergency communications capabilities need to incorporate the range of features, such as voice, data, multimedia, and push-to-talk, that best support the needs of all potential users. Future-focused technologies are rapidly increasing the range of features, devices, applications, and available bandwidth that support incident response and recovery. Greater acceptance of and familiarity with a wider range of enhanced features will also occur in the converged environment of the future as members of today's young, technology-savvy generation become members of tomorrow's emergency responder community.

[42] This "networking" uses information technology via a robust network to allow increased information sharing, collaboration, and shared situational awareness, which theoretically allows greater self-synchronization, speed of command, and mission effectiveness.

4.0 CONCLUSION

As the result of multi-billion dollar investments made by industry to reinforce its networks and prepare for disasters and significant efforts by public-sector entities to improve and enhance existing emergency response capabilities and plans, major strides have been realized in mitigating the critical communications issues identified during the September 11th and Hurricane Katrina responses. The timing and scope of the next catastrophe or major crisis cannot be predicted, but history informs that the next crisis will undoubtedly occur with unanticipated impacts. The NSTAC membership believes that more can and must be done to ensure that the Nation and its precious resource—our Emergency Responders—are fully coordinated, informed, trained, equipped, and prepared to handle the widest range of incidents and circumstances.

In the short term, the NSTAC recommends additional resilient, deployable capabilities be leveraged to achieve a faster restoration of the underlying communications infrastructure, particularly in response to the harshest of incident environments. Greater expansion and use of proven existing NS/EP priority services, and particularly TSP provisioning and restoration as applied to wireless networks, is a common-sense mandate and a cost-effective approach to enhancing basic emergency responder communications operability and availability.

In addition to these technology- and service-based enhancements, emergency responders deserve a clear, modern, and relevant NS/EP and emergency communications policy framework to establish effective organizational authorities, roles, and responsibilities. Finally, fully integrated and coordinated Government emergency communications strategy and planning must emphasize lessons learned from past incidents, remain responsive to the needs of a growing and increasingly technically sophisticated emergency response community, and fully leverage advances and opportunities presented by the converged network environment.

APPENDIX A
THE NSTAC LETTER TO THE PRESIDENT ON EMERGENCY COMMUNICATIONS AND INTEROPERABILITY

March 28, 2006

The President
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—Department of Defense, National Guard, Federal, critical infrastructure sector, non-Governmental organization and State and local—response and recovery entities. Your February 2006 report, *The Federal Response to Hurricane Katrina: Lessons Learned [Lessons Learned Report]*, 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 immediately applicable actions that will markedly improve the Nation's emergency communications capabilities in advance of the upcoming 2006 hurricane season. Without prompt action, effective coordination of response to National incidents will remain severely hampered this summer and beyond. The NSTAC recommends that you direct the Department of Homeland Security (DHS) to —

1. Establish a uniform protocol working with Federal, State, and local Government organizations that can dynamically identify their emergency management and coordinators' contact information, especially during times when regular contact information is changed by event situations, and a capability to share that information with DHS (*e.g.*, via websites). This capability should be administered by the National Communications System (NCS) National Coordinating Center (NCC) to assist in its execution of Emergency Support Function #2, Communications. The capability will enable rapid contact and coordination with response entities pursuant to Recommendation #35 of the *Lessons Learned Report*.

2. Accelerate efforts to create an initial 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-inflicted 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 maintenance of law enforcement requirements.

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 authorizing 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,

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
The NSTAC Principals and Industry Executive Subcommittee Members

APPENDIX B
TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

CTIA—The Wireless Association	Mr. Jim Bugel, Co-Chair
Motorola, Incorporated	Mr. Mike Alagna, Co-Chair
AT&T, Incorporated	Mr. David Barron
	Ms. Rosemary Leffler
Bank of America Corporation	Mr. Roger Callahan
The Boeing Company	Mr. Robert Steele
Computer Sciences Corporation	Mr. Raymond Lehr
CTIA – The Wireless Association	Mr. Rick Kemper
Intelsat, Limited	Ms. Sallye Clark
Lockheed Martin Corporation	Mr. Allen Dayton
Lockheed Martin Corporation	Mr. David Wye
Lucent Technologies, Incorporated	Mr. Brenton Greene
Lucent Technologies, Incorporated	Mr. Bernie Malone
Microsoft Corporation	Mr. Paul Nicholas
Nortel Networks Corporation	Dr. Jack Edwards
Qwest Communications International, Incorporated	Mr. Thomas Snee
Raytheon Company	Mr. Frank Newell
Rockwell Collins, Incorporated	Mr. Ken Kato
Science Applications International Corporation	Mr. Hank Kluepfel
Sprint Nextel Corporation	Ms. Allison Growney
Sprint Nextel Corporation	Mr. John Stogoski
Telcordia Technologies, Incorporated	Ms. Louise Tucker
VeriSign, Incorporated	Mr. Michael Aisenberg
Verizon Communications, Incorporated	Mr. James Bean

OTHER PARTICIPANTS

AT&T, Incorporated	Mr. Harry Underhill
George Washington University	Dr. Jack Oslund
Intelsat, Limited	Mr. Richard DalBello
Intelsat, Limited	Mr. Kalpak Gude
Northrop Grumman Corporation	Mr. Peter Hadinger
Telecommunications Industry Association	Mr. Daniel Bart
SES-Americom, Incorporated	Ms. Leslie Blaker

GOVERNMENT PARTICIPANTS

Department of Defense	Ms. Hillary Morgan
Department of Homeland Security	Mr. William Fuller
	Ms. Christina Watson
Federal Communications Commission	Mr. Walter Johnston
General Services Administration	Mr. Jim Russo
National Telecommunications and Information Administration	Mr. William Belote
	Mr. Thomas Hardy
	Mr. Charles Hoffman