USAWC STRATEGY RESEARCH PROJECT

RELIABLE AND RELEVANT NATIONAL COMMUNICATIONS SYSTEM

by

Lieutenant Colonel Timothy L. Lake
United States Army National Guard

COL James H. Thomas
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Reliable and Relevant National Communications System	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Timothy Lake	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**26**	

ABSTRACT

AUTHOR: Lieutenant Colonel Timothy L. Lake

TITLE: Reliable and Relevant National Communications System

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 26 CLASSIFICATION: Unclassified

The National Communications System is a federal government command and control emergency communications system that requires a complete, comprehensive review and emerging technological overhaul to ensure its reliability and relevance. Since its establishment in the early 1960s, the system has gone through several organizational restructurings and System upgrades. With our nation under increased terrorist threats within our borders, the reliability of the National Communications System is under extreme scrutiny. In 2002, a Presidential Directive transferred oversight of the organization from the Department of Defense to the newly established Department of Homeland Security.

This paper will analyze the current National Communications System, review its origins and recommend emerging technological improvements to support the National Security Council. It also will review the needs of federal, state and local governments, and then recommend implementation of emerging technological capabilities to enhance system reliability and relevance. Today, more than ever before, the commercial telecommunications infrastructure provides critical communications connectivity for our government's daily operations as well as emergency communications. The roles of civilian communications companies and their infrastructure also will be analyzed as it applies to emergency national communications support.

TABLE OF CONTENTS

LIST OF TABLES

RELIABLE AND RELEVANT NATIONAL COMMUNICATIONS SYSTEM

THE NATIONAL COMMUNICATIONS SYSTEM

The National Communications System (NCS) is a federal government command and control emergency communications system that requires a complete, comprehensive review and emerging technological overhaul. The NCS was established to unify control of federal, state and commercial communication systems to better serve the Office of the President, the National Security Council, the Department of Defense and other federal, state and local governmental agencies during times of peace, emergencies or periods of operational concerns. Over the past three years, the NCS critical infrastructure has failed to provide uninterrupted communications support at all levels of the government during critical times of need. The terrorist events of September 11, 2001, and the northeastern states power grid failure in August 2003 are recent national events that reaffirm the requirement to leverage emerging technologies to streamline and integrate our nation's communications system at all levels of government as well as to improve our critical civilian telecommunications infrastructure.

This paper analyzes the current National Communications System, reviews its origins, and recommends emerging technological improvements to support the National Security Council and the National Homeland Security Council, both of which advise the President on Homeland Defense. It will define the issues that government and the private sector must address in order to ensure that National Security and Emergency Preparedness telecommunication services will be available in times of crisis for the President, other national leaders, state governors, and the emergency preparedness and response community. This paper will review the needs of federal, state and local governments, and then recommend implementation of emerging technological capabilities to enhance system reliability and relevance.

TELECOMMUNICATIONS

> "The largest Interconnected machine in the world is the telephone system. Every country on the face of this planet has a telecommunications infrastructure. Most businesses depend heavily on their use of telecommunications, not just for sales, but also for the entire operation. A poor or non-existent telecommunications system, even for a short period of time can often generate significant revenue lost, and do immeasurable damage to your reputation."[1]

Over the past 150 plus years telecommunications have played an intricate role in our nation's industrial and governmental growth? Today, telecommunications remain at the core of our nation's domestic growth and support to our global influence. Telecommunications is the

infrastructure that supports our national elements of power on a daily basis. That is the support of our diplomacy negotiations, economic maneuvers, information dissemination, and the command and control of our military.

Telecommunication is defined as any transmission, emission, or reception of signs, signals, writing, images and sounds or information of any nature by wire, radio, optical or other electromagnetic system.[2] Commercial telecommunication networks provide today approximately 95 percent of the communication requirements critical to the support of our national security. Communications have played a vital role in Presidential decision-making since the development of the telegraph in 1843. President Abraham Lincoln walked across the White House lawn to visit the War Department Army Signal Corps telegraph office almost daily during the major campaigns of the Civil War. He spent hours reading messages and sending orders to his generals.[3] During the Spanish-American War, President William McKinley established the first War Room in the White House, and equipped it with telegraphic instruments, telephones, and war maps so that he could follow the progress of American troops and the American fleet in and around Cuba. On the eve of World War II, President Franklin D. Roosevelt and British Prime Minister Winston Churchill installed a direct telephone link between their offices to enable the two leaders to have direct communications.[4]

WHY A NATIONAL COMMUNICATIONS SYSTEM

The need for a reliable communication system came to the attention of our national leaders when President John F. Kennedy and his National Security Council experienced procedural and technical delays in communicating critical information to federal agencies, and Soviet Union leadership during the Cuban Missile Crisis. The United States was hours away from an authorized decision to execute air strikes, and a land invasion of Cuba. After a 12-hour delay, communication between President Kennedy and Soviet Premier Khrushchev finally lowered tensions and established the foundation for an agreement to avert a possible nuclear catastrophe.[5]

President John F. Kennedy directed his National Security Adviser, McGeorge Bundy, to establish a communications capability that would support Presidential decision-making. The Presidential mandate was for the communications system to focus on national and international interconnectivity and survivability.[6] On August 21, 1963, a National Security Action Memorandum was published establishing the National Communications System.[7]

BRIEF HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM

The rapid technological development of telecommunications and our reliance on its infrastructure to meet our daily needs have resulted in both organizational and technological system changes over the past 43 years. The NCS is responsible for ensuring that national security and emergency preparedness communications function successfully, including interconnectivity and survivability during times of congestion or when the networks have been damaged or destroyed.

The world events during the Reagan Administration inspired major improvements in national security and emergency telecommunications. The pace of technological change provided a growth opportunity for system improvements and new opportunities for diversity and deregulation. Due to the growing number of commercial telecommunication companies and the break-up of the Bell Telephone Company, Congress, the courts and the regulatory agencies began instituting new telecommunication requirements. To ensure compliance as well as availability of emerging technology and its support to the NCS, President Ronald Reagan in 1982 created the National Security Telecommunications Advisory Committee (NSTAC) with Executive Order 12383. The NSTAC was established as the executive agent to oversee the NCS and to provide industry-based analyses and recommendations to the President and the executive branch regarding policy and enhancements to national security and emergency preparedness telecommunications.[8]

The NSTAC provides analyses and recommendations on policy and technical issues related to telecommunications, information systems, information assurance, information protection, and national security and emergency preparedness concerns. NSTAC is comprised of up to 30 Presidential appointed telecommunication and industry leaders. Table 1 depicts the current NSTAC organization.

LOCKHEED MARTIN (Chair)	BELLSOUTH (Vice Chair)	
AT&T	BANK OF AMERICA	BOEING
CISCO SYSTEMS	CSC	DELL
EDS	LUCENT	MICROSOFT
MOTOROLA	NORTEL	ORACLE
RAYTHEON	ROCKWELL	QWEST
NORTHROP GRUMMAN		SAIC
SBC	SPRINT	TELEDESIC
TRW	UNISYS	USTA
VERISIGN	VERIZON	WORLDCOM

TABLE 1: NSTAC MEMBERSHIP

President Ronald Reagan signed Executive Order (E.O.) 12472 in April 1984, which superceded President Kennedy's Memorandum on the NCS. This executive order assigned the NCS with the support of 23 Federal departments and agencies (see table 2) the mission to assist the President; the NSC; the Director of the Office of Science and Technology Policy; and the Director, Office of Management and Budget in coordinating the planning for and the assurance of systems capability. The NSC was directed to have the capability to support national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attacks, recovery and reconstruction. The executive order also assigned the NCS the responsibility of ensuring the national telecommunications infrastructure is developed and capable of meeting the needs of our nation. This remains the core responsibility of the NCS.[9]

Department of State	Department of Treasure
Department of Defense	Department of Justice
Department of Interior	US Department of Agriculture
Department of Commerce	Health and Human Services
Department of Transportation	Department of Energy
Department of Veteran Affairs	Central Intelligence Agency
Federal Emergency Management Agency	The Joint Staff
General Services Administration	NASA
Nuclear Regulatory Commission	National Telecom and Information admin
National Security Agency	US Postal Services
Federal Communications Commission	Federal Reserve Board

TABLE 2: NCS MEMBER ORGANIZATION

The numerous executive orders and presidential memorandums reinforce the significant roles the NCS performs for our national security and homeland defense. The NCS has enhanced its capabilities throughout its 43-year history to meet the demands of our changing environment and to continue providing proactive solutions to our current and future communication requirements (see table 3).

As a result of September 11, 2001, terrorist attacks, President George W. Bush issued Executive Orders 13228 and 13231 redefining the role of the NCS in national and homeland security. Executive Order 13228 established the White House Office of Homeland Security and tasked the Office of Homeland Security to coordinate efforts to protect critical public and private owned information systems within the United States for terrorist attacks. The Office of

Homeland Security is also mandated to coordinate the efforts that would ensure the rapid restoration of telecommunications and critical information systems after disruption by a terrorist threat or attack.[10]

The establishment of the President's Critical Infrastructure Protection Board with Executive Order 13231 renamed the NCS Committee of Principals as the Committee for National Security and Emergency Preparedness Communications and assigned the group as a permanent standing committee in the Office of Homeland Security. Executive Order 13231 reiterated the reporting functions and responsibilities established in Executive Order 12472.[11]

1962	Executive Order 10995	Establishment of the Director of Telecommunications Manager
1963	Presidential Memorandum NSAM 252	Establishment of the NCS
1970	Executive Order 11556	Establishment of Office OTP (of Telecommunications Policy)
1982	Executive Order 12382	Establishment of NSTAC (National Security Telecommunications advisory Committee
1984	Executive Order 12472	Establishment of NS/EP Telecom
1998	Exec. Order 12656	Primary guidance for the NS/EP
2001	Exec. Order 13228	Establishment of OHS
2001	Exec. Order 13231	Establishment of CIP

TABLE 3: TYPES AND DATES OF ESTABLISHED EXECUTIVE ORDERS

In 2003, The Office of the President published three National Security Presidential Directives (NSPD), also referred to as Homeland Security Presidential Directives (HSPD). NSPD-5, Management of Domestic Incidents; NSPD-7, Critical Infrastructure Identification, Prioritization, and Protection; and NSPD-8, National Preparedness are directives establishing policies to strengthen the preparedness of the United States to prevent and respond to threats or actual domestic terrorist attacks, major disasters, and other emergencies.

CURRENT SYSTEMS

The NCS became part of the Information Analysis and Infrastructure Protection Directorate of the Department of Homeland Security in March 2003.[12] The NCS currently provides national security and emergency preparedness priority telecommunications service to Federal, State, and local governments, industry and other authorized national security and emergency preparedness organizations. The NCS Critical Infrastructure Protection Division provides the following priority telecommunications services:

Government Emergency Telecommunications Service (GETS) is a government managed program that utilizes the commercial communication infrastructure to provide emergency phone service to federal, state and local governments, as well as industry, and non-governmental organization personnel in performing national security and emergency preparedness missions. It provides users with emergency access and priority call processing in the public switch telephone network. It is an emergency telecommunication capability to be used during periods of natural or man made emergency or crisis that causes congestion on the public switch telephone network. GETS telephone service is designed to be used when national security and emergency preparedness personnel are unable to complete emergency calls through normal telecommunication means.[13]

GETS is necessary because of the increasing reliance on telecommunications. The economic viability and technical feasibility of such advances as nationwide fiber optic networks, high-speed digital switching, and intelligent features have revolutionized the way we communicate. This growth has been accompanied by an increased vulnerability to system failures. Although backup systems are in place, disruptions in service can still occur. Recent events have shown that natural disasters, power outages, fiber cable cuts, and software problems can have catastrophic impact on the telephone services of entire regions. Additionally, congestion in the public switched telephone network, such as the well-documented "Mother's Day phenomenon," can prevent access to circuits. However, during times of emergency, crisis, or war, personnel with national security and emergency preparedness missions need to know that their calls will be processed and completed more often than routine calls.

GETS addresses this basic requirement. Using regulatory enhancements on existing commercial technology, GETS allows the national security and emergency preparedness community to communicate over existing public switched telephone network infrastructure with a high likelihood of call completion during the most severe conditions or high-traffic congestion and disruption. The result is a cost effective, easy to use telephone service that is accessed through a simple dialing plan and Personal Identification Number card verification methodology, similar to a commercial calling card. GETS is maintained in a constant state of readiness and provides a cost-effective means to overcome network outages through such methods as enhanced routing and priority treatment.[14]

Wireless Priority Service (WPS) is a White House directed service in response to the events of September 11, 2001, to be used by key leaders during emergency situations. The WPS provides an end-to-end nationwide wireless priority communications capability to key

national security and emergency preparedness personnel during natural or man-made disasters or emergencies that cause congestion or network outages in the public switch telephone network. The WPS is complementary to, and is expected to be used in conjunction with the GETS to ensure a high probability of call completion in both the wire line and wireless portions of the public switch telephone network.[15]

Telecommunication Service Priority (TSP) system is the regulatory, administrative, and operational system authorizing and providing for priority provisioning and restoration of critical national security and emergency preparedness telecommunications circuits. Critical circuits are defined as those that are critical to maintaining a state of readiness for, responding to, or managing telecommunications during an event or crisis that could cause harm to the population, damage to property, or threaten the security of the United States. As a result of natural or man-made disasters, telecommunications service vendors may become overwhelmed with requests for new telecommunications services and requirements to restore existing telecommunications services. The TSP Program provides service vendors with a Federal Communications Commission mandate for prioritizing service requests by identifying those services critical to national security and emergency preparedness. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.[16]

Emergency Notification Service (ENS) Pilot is designed to provide alternative emergency notification and information to critical national security and emergency preparedness decision makers and other Federal, State and local governmental officials, including public health and safety personnel, and emergency command centers using multiple communication channels. Emergency notification is distinguished from emergency alerting in that notification targets specific individuals or groups of individuals and may require confirmation for specific communications.[17]

SHAred RESource (SHARES) High Frequency (HF) Radio Program provides a single, interagency emergency message handling system by bringing together existing HF radio resources of federal, state and industry organizations when normal communications are destroyed or unavailable for the transmission of national security and emergency preparedness information.[18] SHARES is one of the first national emergency systems managed by the NCS. It provides both data and voice, however it uses dated technology and network architectures.

INFORMATION SHARING AND HOMELAND SECURITY

Our nation's communication infrastructure contributes to every aspect of homeland security and is a vital foundation for the homeland security information gathering efforts. Every government official performing homeland security missions depends upon information and information technology.

Although American information technology is the most advanced in the world, our country's information systems do not adequately support the homeland security mission. Today, there is no single agency or computer network that integrates all homeland security information nationwide. Instead, much of the information exists in databases scattered among federal, state and local agencies. Databases used for law enforcement, immigration, intelligence, and public health surveillance have not been connected in ways that allow us to recognize information gaps. As a result, government agencies storing terrorism information have not been able to systematically share that information with other agencies.[19]

We need a communication system that enables the sharing of essential homeland security information to national security and emergency preparedness responder. This information must be shared "horizontally" across each level of government, and "vertically" among federal, state, and local governments, as well as private industry. As the NCS transitions to a more robust next generation voice and data network, it must be prepared to support the expanded daily requirements foreseen by homeland security network requirements and emergency responders.

PRIMARY OVERSIGHT

Today federal, state, and local governments are attempting to develop survivable, interoperable communication infrastructures to support national security and emergency preparedness. Throughout the history of this great nation, the strategic management of the National Communications System became the responsibility of the federal government coupled with emerging technological recommendations from the NSTAC and the commercial telecommunications community. However, the operational requirements and capabilities placed upon the state and local emergency responders are not always interoperable with their federal counterparts.

Throughout the history of the NCS, the national communications requirements and capabilities have been transferred among the War Department, Office of the President, Department of Defense, and now transferred to the Department of Homeland Security. As primary responsibility of the NCS has transferred between federal departments, the Department

of Defense was always required to execute managerial oversight of the National Communications System day-to-day operations. The director of the Defense Communications Agency is dual-hatted as Manager, National Communications System.[20] The Director, Defense Communications Agency now Defense Information System Agency, focuses on both international command and control as well as national. Very rarely did the Defense Information System Agency focus on state and local emergency preparedness communications capabilities or requirements.

Today, management responsibility of the NCS has been transferred to the newly established Department of Homeland Security.[21] With this transfer, federal, state and local governments now have a domestic focused communications requirement management team that will focus on assisting federal as well as state and local emergency responders interoperable communication concerns.

ENHANCE THE SYSTEM

The events of September 11, 2001 reaffirmed the requirement for enhanced technological improvements in the National Communications System because of public switch telephone network saturation. Two years later, the August 2003 northeastern states' power grid failure highlighted a system failure based on the infrastructure power requirements. Both events limited communications service to critical national security and emergency preparedness personnel.

Although some improvements were made as a result of lessons learned from these events, federal, state, and local governments are again requesting that the National Communications System enhance its capabilities to ensure reliable connectivity during emergencies. The telecommunication services that support national security and emergency preparedness depend on a national telecommunications infrastructure that provides timely, continuous, assured, robust and reliable communications between the President, his security councils, and the federal departments and agencies during a national security emergency, as defined in Executive Order 12656. Our national infrastructure has to support and enable national security and emergency preparedness telecommunications by wire, radio, fiber optic, or other electromagnetic means provided by commercial, government, and privately owned telecommunications provides. The required capabilities must assure flexibility, adaptability, interoperability, and seamless connectivity at any location either fixed or mobile. The government emergency telecommunications system must be expanded to include mobile state and local governmental emergency responders, as well as critical private business responders.

National security and emergency preparedness telecommunication services must help support a continuous telecommunications readiness. We must poses the ability to respond, and manage any event or crisis that degrades or threatens the national security and emergency preparedness of the United States or which could cause harm to the population or loss of property. We must prepare to minimize the damage and recover from any future terrorist attacks that occur despite our best efforts at prevention. Past experience has shown that preparedness efforts are key to providing an effective response to major terrorist incidents and natural disasters. Therefore, we need a comprehensive national system to bring together and command all necessary response assets quickly and effectively.

LEVERAGING EMERGING TECHNOLOGY

Over the past decade the government has transitioned from its dependency on government controlled, dedicated communication support provide by various federal agencies to a more cost effective, dynamic architecture that uses shared commercial telecommunication infrastructures. As technological advancements continue to evolve, the convergence of today's voice and data networks will fundamentally change the technology and security environment in which national security and emergency preparedness telecommunication services are provided. Today, the public switch network is beginning to support next generation interconnection for fixed and mobile voice communications, as well as both fixed and mobile internet-data communications. As more mobile data and voice users communicate over the commercial network with these current and emerging communications devices, the current types of communication equipment and service provided to national security and emergency preparedness responders will also require replacement if reliable services are to be available in the foreseeable future. New services and capabilities are being developed that may be useful or desired by the President, other national and state leaders as well as private industry. With the next generation networks, these new communication services will be streamlined into a converged seamless data and voice architectural network. Pat Gelsinger, Senior Vice President and Chief Technology Officer Intel Corporation, commented about the future of Communications:

> "The convergence of computing and communications will bring a new level of productivity to business, reducing costs and extending the reach of communications across the globe, opening up new opportunities on a scale we can't imagine today. Intel is committed to accelerating towards this future, through continued technology advancements and close collaboration with industry and governments worldwide."[22]

The technological developments that are driving the convergence of today's voice and data networks are largely positive. These developments are enabling capabilities and services that were not considered a decade ago and are driving innovation. The developments of the emerging next generation network technologies for which these services will be provided are currently outpacing the current advancements in national security and emergency preparedness telecommunication services. Telecommunications convergence refers to the merging of traditional circuit switched networks with packet-based networks as they, along with wireless, cable, satellite, and other networks, evolve into the next generation network. The next generation network will transport voice, data and video information over a common packet-based transmission medium.[23] This transformation to package switching and IP technology will be accompanied by numerous new applications and services. To pioneer this transformation, Homeland Security Secretary Tom Ridge appointed the Department's Assistant Secretary for Infrastructure Protection, Robert Liscouski as Manager of the National Communications System. As the new manager, Mr. Liscouski was also granted $141 million dollars from the President's fiscal year 2004 budget to support development and deployment of emerging next generation network communication capabilities.[24]

TRANSFORMATION CHALLENGES WITH NEXT GENERATION NETWORK

The migration of voice traffic from the conventional circuit-switched network to packet-switched networks has begun. The large-scale shift in network structure from circuit switched to packet switched networks using Internet Protocol (IP) technology will have a wide range impact on national security and emergency preparedness telecommunications services. Telecommunications services such as the Government Emergency Telecommunication Service and the Telecommunication Service Priority were developed based on the public switch telephone network architecture. The Federal Emergency Management Agency and the state and local emergency management agencies' all have developed emergency response activities that rely heavily on the public switch telephone network. The challenge facing the National Communication System and the national security and emergency preparedness community is the continued support of their missions through the transition into the next generation network. Today's missions are accomplished through primarily voice services, and the transition to package technology is requiring the development of new applications and services.[25]

Standards development will be critical as industry and the President's National Security Telecommunications Advisory Committee ensures that national security and emergency preparedness protocols and priorities are integrated into the next generation network

architecture. Table 4 depicts perceived national security and emergency preparedness functional requirements in the next generation network.

NS/EP Telecommunication Services Functional Requirements	Description
Enhanced Priority Treatment	Services supporting NS/EP missions must be provided priority treatment over other traffic.
Secure Networks	Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
Non-Traceability	Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
Restorability	Should a disruption occur, services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis.
International Connectivity	Services must provide access to and egress from international carriers.
Interoperability	Services must interconnect and interoperate with other selected government or private facilities, systems, and networks.
Mobility	The communications infrastructure must support transportable, redeployable, or fully mobile communications (e.g., personal communications service, cellular, satellite, high frequency radio).
Ubiquitous Coverage	Services must be readily accessible to support the national security leadership and inter- and intra-agency emergency operations, wherever they are located.
Survivability / Endurability	Services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
Voice Band Service	The service must provide voice band service in support of presidential and other communications.
Broadband[1] Service	The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, multimedia).
Scaleable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
Affordability	Services must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf technologies, services).
Reliability / Availability	Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

TABLE 4: TELECOMMUNICATION SERVICE FUNCTIONAL REQUIREMENTS[26]

For the foreseeable future the current voice and data networks will coexist and operate with tomorrow's emerging architecture. The converging networks will provide an expanded set of existing and new telecommunication services that will benefit national security and emergency preparedness personnel. However, the process of convergence will impact the provision of national security and emergency preparedness telecommunication services traditionally provided by the public switched telephone network.

RECOMMENDATIONS

To assure reliability of the next generation network and to mitigate challenges, the Office of Manager, National Communication System should:

- Identify a dual use multipurpose mobile phone or PDA that can support our national security and emergency preparedness community with both voice and date communications. The instrument must be capably of using the emerging terrestrial base public switch communication network via IP packet switch, and have the capability to utilize satellite technology to facilitate assured connectivity.
- Continue working with national standards organizations to ensure required telecommunications functional requirements are integrated in the developing next generation wireless standards.
- Expand the technical expertise currently on the staff to include greater representation of Internet technology specialist. This will assist in future system development, deployment, and management. The expansion of technical expertise should also reduce the overarching dependence, and influence of independent telecommunication contractors that are profit base.
- Encourage the telecommunication industry and Internet provides to continue evaluating the Internet interoperability with the public switch telephone and the evolving next generation network technologies. We must ensure that appropriate protocols and software enhancements are in the public switch networks to provide priority services to our national security and emergency preparedness community.
- Assess the interoperability between circuit switching, packet switching and the next generation network architecture to minimize or eliminate future risk with system reliability and availability during support to the national security and emergency preparedness community.
- Replace SHARES, the current terrestrial means of communications for emergency response with a mobile satellite capability.
- Integrate emerging High Altitude Airship technology as well as commercial and Department of Defense satellites into its national emergency preparedness architecture. Space based transmissions support stations can argument the ground mobile and fixed telecommunication infrastructure, which is subject to regional incident or system malfunctions.

CONCLUSION

In times of crisis, the national leadership depends on assured national security and emergency preparedness telecommunication services, but the unprecedented scope and pace of changes unfolding in the telecommunications sector of the nation's critical information infrastructure places such assured services at risk. The transformation of voice communication over traditional circuit switched networks to packet switched networks using Internet Protocol (IP) has begun. This shift in network structure will impact our current national security and emergency preparedness telecommunication services. National security and emergency preparedness telecommunication services such as the Government Emergency Telecommunication Service and the Telecommunication Service Priority program were all developed to work on the public switch telephone network architecture. The Federal Emergency Management Agency, as well as state and local governments emergency management agencies' response activities depend heavily on the public switch telephone network. The current challenge facing the National Communication System and our national security and emergency preparedness community is the assurance of continued priority support by the commercial infrastructure during the convergence and transformation into the next generation package switch network IP architecture.

WORD COUNT=4636

ENDNOTES

[1] Global Enterprise Network Limited, Global Telecommunications System and Support "The Largest Interconnected Machine in the World," 6 January 2004; available from <http://www.gentelecom.net/home.htm>; Internet; accessed 6 January 2004.

[2] American National Standards, Telecom Glossary 2000, "Telecommunication," 6 January 2004; available from <http://www.atis.org/tg2k/>; Internet; accessed 6 January 2004.

[3] Richard T. Loomis, *A History of the National Communications System: The First 25 Years, 1963-1988* (Arlington: the MITRE Corporation, 1990), IV.

[4] Office of the Manager, National Communications System, *Leadership Excellence in Technology, 1963-1998* (Arlington: National Communications System, 1998), 2.

[5] McGeorge Bundy, *Danger and Survival: Cuban Missile Crisis* (New York: Random House, 1998), 438-445.

[6] Loomis, 2.

[7] Office of the Manager, National Communications System, "Background and History," 1 March 2003; available from <http://www.ncs.gov/ncs/html/NCSHistoryBkgrd.html>; Internet; accessed 25 January 2004.

[8] Office of the Manager, National Communications System, NSTAC, "Fact Sheet," 12 October 2003; available from <http://www.ncs.gov/nstac/nstac.htm>; Internet; accessed 25 January 2004.

[9] Executive Order 12472, "Assignment of National Security and Emergency Prepared Telecommunications Functions," 28 February 2003; available from <http://www.ncs.gov/NCS/HTML/EO-12472%20with%20EO-13286%20changes.htm>; Internet; accessed 25 January 2004.

[10] Office of the Manager, National Communications System, *Ensuring Essential Communications for the Homeland*, (Arlington: Office of the Manager, National Communications System), FY2002, 3.

[11] Ibid., 3.

[12] DefenseLINK News, "National Communications System Joins Homeland Security Department," 10 March 2003; available from < http:/www.defence,ink.mil/news/mar2003 >; Internet; accessed 25 January 2004.

[13] Office of the Manager, National Communications System, GETS Program Information, "The GETS Concept," 29 December 2003; available from <http://www.gets.ncs.gov/program_info.html>; Internet; accessed 25 January 2004.

[14] Ibid.

[15] Office of the Manager, National Communications System, “Wireless Priority Service,” 24 November 2003; available from <http://wps.ncs.gov/index_body.html>; Internet; accessed 25 January 2004.

[16] Office of the Manager, National Communications System, “Telecommunication Service Priority,” 4 December 2003; available from <http://www.tsp.ncs.gov/index_body.html>; Internet; accessed 25 January 2004.

[17] Office of the Manager, National Communications System, “Emergency Notification Service,” June 2003; available from <http://www.ens.ncs.gov>; Internet; accessed 25 January 2004.

[18] Office of the Manager, National Communications System, “Overview, SHARES HF Radio Program,” June 2003; available from <http://www.ncs.gov/shares/overview.htp>; Internet; accessed 25 January 2004.

[19] Office of Homeland Security, National Strategy for Homeland Security, “*Information Sharing and Systems*” (Washington, D.C.: Office of Homeland Security, July 2002), 55.

[20] Loomis, 5.

[21] John Graves, Project Manager, National Communications System; Interview by author, 10 October 2003.

[22] Pat Gelsinger, Senior Vice President and Chief Technology Officer Intel Corporation, “The future of Communications,” 3 February 2004; available from <http://www.intel.com/technology>; Internet; accessed 3 Feb 2004.

[23] Business Communications Review, Next Generation Networks, “Convergence & IP”,3 Feb 2004; available from <http://www.bcr.com/ngn/tracks/convergence asp>; Internet; accessed 3 February 2004.

[24] Telecom News, *“National Security and Emergency Preparedness”* Office of the Manager, National Communication System, Issue 1, 2004, 1, 2.

[25] Graves.

[26] Contract Data Requirements List B001, *Future Service Plan VIII, Volume III*, 20 June 2003, 13.

BIBLIOGRAPHY

American National Standards. Telecom Glossary 2000, "Telecommunication." <http://www.atis.org/tg2k/>. Internet. Accessed 6 January 2004.

Bundy, McGeorge. *Danger and Survival: Cuban Missile Crisis*. New York: Random House, 1998.

Business Communications Review. Next Generation Networks. "Convergence & IP." 3 February 2004. Available from <http://www.bcr.com/ngn/tracks/convergence.asp>. Internet. Accessed 3 February 2004.

Campen, Alan D. *The First Information War*. Fairfax, VA: AFCEA International Press, 1992.

Contract Data Requirements List B001. *Future Service Plan VIII, Volume III*, 20 June 2003.

DefenseLINK News. "National Communications System Joins Homeland Security Department." 10 March 2003. Available from <http:/www.defenselink.mil/news/mar2003>. Internet. Accessed 25 January 2004.

Executive Order 12472. "Assignment of National Security and Emergency Prepared Telecommunications Functions." 28 February 2003. Available from <http://www.ncs.gov/NCS/HTML/EO-12472%20with%20EO-13286%20changes.htm>. Internet. Accessed 25 January 2004.

Gelsigner, Pat, Senior Vice President and Chief Technology Officer Intel Corporation, "The Future of Communications." 3 February 2003. Available from <http://www.intel.com/technology>. Internet. Accessed 3 February 2004.

Global Enterprise Network Limited. Global Telecommunications System and Support. "The Larges Interconnected Machine in the World." Available from <http://www.gentelecom.net/home>. Internet. Accessed 6 January 2004.

Graves, John, Project Manager, National Communications System. Interview by Author, 10 October 2003.

Loomis, Richard T. *A History of the National Communications System: The First 25 Years, 1963-1988.* Arlington: the MITRE Corporation, 1990.

Office of Manager, National Communications System. Government Emergency Telecommunication Services Program Information. "The GETS Concept." 29 December 2003. Available from <http://www.gets.ncs.gov/program_info.html>. Internet. Accessed 25 January 2004.

Office of the Manager. National Communications System. "Background and History." 1 March 2003. Available from <http://www.ncs.gov/ncs/html/NCSHistoryBkgrd.html>. Internet. Accessed 25 January 2004.

Office of the Manager. National Communications System. "Overview, SHARES HF Radio Program." June 2003. Available from <http://www.ncs.gov/shares/overview.htm>. Internet. Accessed 25 January 2004.

Office of the Manager. National Communications System. “Telecommunication Service Priority.” 4 December 2003. Available from <http://www.tsp.ncs.gov/index_body.html>. Internet. Accessed 25 January 2004.

Office of the Manager. National Communications System. “Wireless Priority Service.” 24 November 2003. Available from <http://wps.ncs.gov/index_body.html>. Internet. Accessed 25 January 2004.

Office of the Manager. National Communications System. *Ensuring Essential Communications for the Homeland.* Arlington: Office of the Manager, National Communications System, 2002.

Office of the Manager. National Communications System. *Leadership Excellence in Technology*, 1963-1998. Arlington: Office of the Manager, National Communications System, 1998.

Office of the Manager. National Communications System. NSTAC “Fact Sheet.“ 12 October 2003. Available from <http://www.ncs.gov/nstac/nstac.htm>. Internet. Access 25 January 2004.

Telecom News. “*National Security and Emergency Preparedness”* Office of the Manager, National Communication System, Issue 1, 2004.

U.S. Office of Homeland security. National Strategy for Homeland Security. *Information Sharing and Systems. Washington, D.C.: U.S.* Office of Homeland Security, July 2002.