THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION TECHNOLOGY PROGRESS IMPACT TASK FORCE REPORT ON CONVERGENCE

MAY 2000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

The national security and emergency preparedness (NS/EP) community depends heavily on priority treatment of voice calls within the public switched network (PSN) to support NS/EP operations. This priority treatment is provided under the Telecommunications Service Priority (TSP) program, a circuit restoration and provisioning service, and the Government Emergency Telecommunications Service (GETS) program, a high probability of call completion service. Telecommunications service providers are rapidly implementing packet-based data networks and plan to transition traffic onto the Next Generation Network (NGN). As a result, the National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) established the Information Technology Progress Impact Task Force (ITPITF) to examine the implications of the evolving public network architecture for priority treatment of NS/EP voice and data traffic. Specifically, the IES directed the ITPITF to examine the potential impact of Internet Protocol (IP) network-PSN convergence on PSN-specific NS/EP priority services.

Purpose

This report identifies implications of Convergence (as defined in Section 1.3) for existing NS/EP priority services, and examines evolving network technologies and capabilities that could assist in satisfying existing NS/EP functional requirements in an NGN environment.

Conclusions

The ITPITF reached the following conclusions:

- The NS/EP community depends heavily on priority treatment of voice calls within the PSN to support NS/EP operations and will remain dependent for the immediate future.
- The public network will change from separate switched voice and packet data networks to an interconnected network and then to a unified NGN over the next several years.
- The potential implications of Convergence and the NGN for GETS services include new blocking sources, lack of ubiquity and interoperability, lack of access to GETS features, disparate congestion handling, and a lack of commensurate network reliability and security.
- NS/EP requirements are unlikely to be incorporated by industry unless the features needed to meet these requirements are standardized by industry, perhaps with prompting from the Government.

- NS/EP traffic requires newly designed and standardized features to overcome new problems associated with packet networks.
- To provide GETS-type services during Convergence and in the NGN, quality of service (QoS) schemes must be expanded to provide services commensurate with NS/EP needs.
- The current level of security safeguards incorporated into GETS is inadequate to maintain NS/EP functional requirements during Convergence and in the NGN.
- TSP, as originally conceived, remains relevant during Convergence because restoration assignments can still be applied to identifiable segments of the PSN.
- A potential implication for the TSP Program during Convergence and in the NGN as discussed by the TSP Oversight Committee (OC) is the inapplicability of the program to Internet service providers (ISP) offering voice services.
- The OC stated that TSP, as currently defined, did not and should not have a role in the NGN, and if the NS/EP community required similar types of priority services for packet networks, a new program would have to be established to support such services.
- TSP-type services in the NGN will provide for the priority provisioning and restoration of network services rather than circuit-based services.
- Although specific NGN standards have not yet been developed to support NS/EP requirements, the NGN technology is capable of supporting these requirements.
- Standards bodies are examining QoS and other new NGN capabilities that may be useful in satisfying certain NS/EP functional requirements in the NGN, and the appropriate departments and agencies should continue active participation in these groups.
- QoS and other new NGN capabilities will require some enhancement to best satisfy specific NS/EP requirements. Therefore, the NS/EP community should determine, as soon as practicable, precise functional NS/EP requirements for the NGN. The appropriate departments and agencies should continue to participate in standards bodies activities related to NGN technologies to ensure that NS/EP requirements are considered during development and implementation phases.
- As the NGN evolves, telecommunications carriers' SS7 networks will become less discrete and more reliant on IP technology and interfaces. Therefore, it is necessary to consider the security, reliability, and availability of the NGN control space as it relates to the provision and maintenance of NS/EP service capabilities.

NSTAC Recommendation to the President

Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies, in coordination with industry, to—

- promptly determine precise functional NS/EP requirements for Convergence and the NGN, and
- ensure that relevant NS/EP functional requirements are conveyed to standards bodies and service providers during NGN standards development and implementation.

NSTAC Recommendation to the IES for Consideration in the NSTAC XXIV Work Plan

Examine potential NS/EP implications related to possible security and reliability vulnerabilities of the control space in the Next Generation Network (NGN). The NSTAC's *Final Report of the Common Channel Signaling Task Force* (January 31, 1994) should be used as a foundation for this analysis.

1.0 INTRODUCTION

1.1 Background

The national security and emergency preparedness (NS/EP) community depends heavily on priority treatment of voice calls within the Public Switched Network (PSN) to support NS/EP operations. Telecommunications service providers are rapidly implementing packet-based data networks and plan to transition traffic onto the Next Generation Network (NGN). As a result, the National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) established the Information Technology Progress Impact Task Force (ITPITF) to examine the implications of the evolving public network architecture for priority treatment of NS/EP voice and data traffic. Specifically, the IES directed the ITPITF to examine the potential impact of Internet Protocol (IP) network-PSN convergence on PSN-specific NS/EP priority services.

The NSTAC was established in September 1982 to provide advice and expertise to the President and the Executive Agent, National Communications System (NCS), on issues and problems related to implementing NS/EP telecommunications policy. Because the NCS serves as the focal point for joint industry/Government planning, the NSTAC and NCS have developed a close partnership. The NCS, under Executive Order 12472—*Assignment of National Security and Emergency Preparedness Telecommunications Functions*, seeks to ensure the development of a national telecommunications infrastructure responsive to the NS/EP needs of the President, Federal departments, agencies, and other entities[1] and capable of satisfying priority telecommunications requirements under all circumstances.[2] Additionally, the NCS is required to develop and test programs and procedures for the Nation's telecommunications resources, including federally and privately owned facilities, to meet NS/EP telecommunications requirements.[3] NSTAC analyses have resulted in the development of many network services to satisfy these needs, including the Telecommunications Service Priority (TSP) Program, Government Emergency Telecommunications Service (GETS), and the High Probability of Completion (HPC) or call recognition services, which enables identification of NS/EP calls. This report should assist the NS/EP community in continuing to meet its objectives and requirements in the future.

1.2 Purpose

This report identifies the implications of Convergence for existing NS/EP priority services and examines evolving network technologies/capabilities that could assist in satisfying existing NS/EP functional requirements in an NGN environment. For the purposes of this report, the NGN is defined as outlined in Section 1.3.

[1] Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, Section 1(c)(1), April 3, 1984.
[2] *Ibid.*, Section 1(c)(2).
[3] *Ibid.*, Section 1(g)(1).

1.3 Definitions

Convergence indicates a process over a 3-to-5 year period of NGN evolution during which traditional circuit-switched networks (including the Advanced Intelligent Network [AIN]) and IP-based data networks will coexist and interoperate to enable end-to-end transmission of voice communications, until IP based networks subsume circuit-switched networks.

The Next Generation Network is a public, broadband, diverse, and scalable packet-based network evolving from the PSN, AIN, and Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence.

1.4 Approach

The approach to this study involves two tasks —

- examine the implications of convergence for existing NS/EP priority treatment services,[4] and
- examine evolving network technologies/capabilities that could assist in satisfying existing NS/EP needs and functional requirements in an NGN environment.

A list of task force members, other participants, and contributing companies and Government agencies is provided in Appendix A.

[4] This priority treatment is provided under the TSP program, a circuit restoration and provisioning service, and the GETS program, a high probability of call completion service.

2.0 NS/EP CONVERGENCE ISSUES

A primary concern related to Convergence is the capability to fulfill specific NS/EP functional requirements, as warranted, in the IP network segments. Table 1 defines NS/EP communications functional requirements as established by Executive Order 12472[5], a 1991 White House Memorandum on *National Level Telecommunications Program Implementation and Functional Requirements*,[6] and best practices established by the Office of the Manager, National Communications System (OMNCS) Requirements Forum (as indicated by "*").

Table 1
NS/EP Communications Functional Requirements

NS/EP Communications Functional Requirements	Description
Enhanced Priority Treatment	Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
Secure Networks	These services ensure the availability and survivability of the network, prevent corruption of or unauthorized access to the data, and provide for expanded encryption techniques and user authentication.
Restorability	Should a service disruption occur, voice and data services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis.
International Connectivity	Voice and data services must provide access to and egress from international carriers.
Interoperability	Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks.
Mobility	The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service [PCS], cellular, satellite, High Frequency [HF] radio).
Nationwide Coverage	Voice and data services must be readily available to support the National security leadership and inter- and intra- agency emergency operations, wherever they are located.
Survivability	Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
Voice Band Service	The service must provide voice band service in support of presidential communications.
Scaleable Bandwidth*	The ability of NS/EP users to manage the capacity of the communications services to support variable bandwidth requirements.
Addressability*	The ability to easily route voice and data traffic to NS/EP users regardless of user location or deployment status. Means by which this may be accomplished include "follow me" or functional numbering, call forwarding, and functional directories.
Affordability*	The service must leverage new public network (PN) capabilities to minimize cost. Means by which this may be accomplished favor the use of commercial off-the-shelf (COTS) technologies and services and existing infrastructure.

[5] Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* April 3, 1984.
[6] White House Memorandum for the Honorable Dick Cheney, Executive Agent, NCS, Oct. 15, 1991.

Functional requirements such as enhanced priority treatment and national coverage are satisfied in the PSN and AIN by GETS. Requirements such as priority treatment, infrastructure restoration, and survivability are satisfied in the PSN by TSP.

2.1 Implications of Convergence on Existing NS/EP Services[7]

The potential implications for GETS and TSP services relating to Convergence are discussed below. GETS and TSP have been associated with voice services and the PSN, however, the NGN will offer voice, data, and video services. Therefore, GETS and TSP services provide only a foundation for analysis of NS/EP services in the context of convergence to the NGN. Other services, such as wireless priority access, dedicated services, and virtual networks, while beyond the scope of this report, also support various NS/EP functional requirements in existing networks. Therefore, separate analysis on the potential implications for these services relating to Convergence may be warranted.

2.1.1 Potential GETS Implications

Developed in response to a White House tasking, GETS provides emergency access and specialized processing in local and long distance telephone networks. A GETS call is identified as an NS/EP call and receives special call setup handling such as enhanced routing and priority treatment. GETS relies on the AIN of the PSN to support identification of NS/EP calls and priority signaling. However, it is uncertain whether evolving IP-based protocols will support all features of the Signaling System 7 (SS7) protocol (such as HPC). Subsequently, the following sections outline potential implications for GETS in an IP environment if the Government and industry fail to define and implement standards that support a GETS type of service.

2.1.1.1 New Blocking Sources

GETS features were designed specifically to overcome operational constraints on circuit switched networks. Examples of such features include exemption from network management controls and trunk queuing. These features may not be germane in packet networks. NS/EP traffic will require newly designed and standardized features to overcome the new constraints associated with packet networks, such as lengthy or variable delays or packet loss. Furthermore, in packet networks, NS/EP priority treatment will be required throughout the call rather than only during call setup (e.g., each packet must be identified for NS/EP treatment through the network). Without such treatment, NS/EP packets could be discarded.

2.1.1.2 Lack of Ubiquity and Interoperability

Voice over IP equipment is being developed by most traditional switch vendors (e.g., Nortel Networks and Lucent Technologies) including many new companies that have not been involved

[7] For additional technical information on network convergence, please refer to Telcordia Technologies, *Network Evolution and Convergence* Report, June 1999, as prepared for the OMNCS.

with GETS previously. These companies are unlikely to incorporate NS/EP requirements unless the needed features are standardized by industry, perhaps with prompting from the Government.[8] Without standardization, many problems could arise. NS/EP calls may not be able to achieve priority access and transport control (e.g., access authorization, routing information). Problems could exist when calls enter a packet network through a gateway from inside an interexchange carrier (IXC) network, inside the local exchange carrier (LEC) network, or at the customer premises.[9] If an NS/EP call is passed directly to a packet network by customer premise equipment (CPE), the call may not be routed to an IXC or to a point in an IXC from which it can reach GETS access authorization.[10] Thus, standards will need to be written and implemented to enable NS/EP call recognition within a packet network and subsequent routing of the call to a GETS IXC.

2.1.1.3 Lack of Access to GETS Features

Many GETS features are triggered on the basis of an NS/EP codepoint[11] associated with the SS7-based HPC capability. It is uncertain whether this codepoint will be transported as part of the signaling associated with call setup in a packet network unless standards are written and implemented because the nature of packet-based transport of signaling information has yet to be defined.[12] Consequently, if the calls are transported through a packet network without standards, NS/EP calls may not be able to access GETS features, particularly on the terminating network.

2.1.1.4 Disparate Congestion Handling

Existing packet switched services react differently to traffic overload than existing circuit switched services. Packet switches allocate bandwidth to packets based on available and/or required bandwidth; circuit switches deny bandwidth to new phone calls until previous calls disconnect. The standards-based NGN will implement a Quality of Service (QoS) feature to allocate bandwidth appropriately between voice, data, and video and between low- and high-priority traffic. With reduced bit rate voice calls, call completion rates for NS/EP traffic may be higher over the NGN. The NS/EP community likely will have useful reliable services, analogous to toll quality GETS services, to support their needs, including real-time interactive sessions and noninteractive sessions.

The QoS schemes being discussed by standards bodies and industry allow specific minimum percentages of bandwidth to be reserved for real-time interactive and non-interactive services. In addition, routing control mechanisms need to be maintained for the duration of NS/EP

[8] *Ibid.*
[9] Graves, John, GETS Briefing to the Network Group, August 5, 1999.
[10] GETS PMO *Voice Over Packet Issue Paper*, May 21, 1999, p 3-3.
[11] SS7 Network Capability ANSI T1.631-1993 that provides for the identification of NS/EP calls. Specifically, an 8-bit NS/EP call identifier (11100010) contained in a calling party's category field of the initial address message. NS/EP calls are assigned signaling priority level 1.
[12] GETS PMO, *Voice Over Packet Issue Paper*, May 21, 1999, p.3-3.

communications to ensure integrity. To provide GETS services during Convergence and in the NGN, existing QoS and routing schemes must be expanded to provide services commensurate with NS/EP requirements. Therefore, GETS calls could be affected if the Government and industry fail to define and implement standards for GETS service within the packet network environment.[13]

2.1.1.5 Network Reliability and Security Implications

The expanded inter-working of the control space of the PSN and Internet technologies during Convergence and the revolutionary open switch architecture of the NGN will likely be areas of network reliability, availability, and security concern to NS/EP users and affect services and functional requirements. One concern is whether a PSN-Internet architecture can handle the intense inter-domain extra-band signaling traffic (a combination of out-of-band signaling like SS7 and in-band signaling of the Internet) among its databases, call agents, routers, switches, and gateways, which could involve millions of call-processing messages a minute.[14] Another critical issue is security, which presents a unique problem because the Internet, with its virtually unrestricted access, is not as protected as the PSN.[15] This could pose unique problems for GETS-type services during Convergence and in the NGN.

Currently, controls against misuse of GETS involve access authorization control, audit, accounting, and fraud control. The planned predecessor to GETS was designed with strong authentication features involving a token-based authenticator to combine *something a person has with something a person knows* (e.g., a password). However, for several reasons including cost, flexibility, and believed limited risk, GETS today relies solely on *something a person knows* for authentication. Although controls to detect fraud and unauthorized access exist, there are presently no other security requirements in place to protect GETS from denial of service attacks or other compromise. In addition, due to Convergence, the security risks of the Internet and the PSN, and the integrity of the SS7 control space, the AIN that supports GETS may be at risk without additional safeguards and requirements. Although security baseline standards exist for SS7 interconnection,[16] they are not specified within GETS functional requirements, service level agreements or current operations. At a minimum, the functionality contained with the SS7 security baseline should be mapped into GETS during Convergence. Additionally, if current security safeguards are employed in the NGN, they will likely be even more inadequate based on existing Internet security risks (e.g., denial of service attacks). Therefore, as the NGN evolves, and as carriers' SS7 networks become less discrete and more reliant on IP technology and interfaces, it will be necessary to consider the security, reliability, and availability of the NGN control space as it relates to provision and maintenance of NS/EP service capabilities. Given

[13] GETS PMO, Voice Over Packet Issue Paper, May 21, 1999, p.3-3.
[14] Telcordia Technologies, *Network Evolution and Convergence*, June 1999, p. ES-3.
[15] *Ibid.*
[16] ATIS NIIF Reference Document, *Part III Installation and Maintenance Responsibilities, SS7 Link and Trunk Installation, and Maintenance Access Service, Attachment I, Network Security Base Guideline*.

NSTAC's responsibility for advising the President on NS/EP telecommunications issues, this study would be consistent with NSTAC's established mission.

2.1.2 Potential TSP Regulatory Implications

Based on an NSTAC recommendation, the Federal Communications Commission (FCC) issued a Report and Order in 1988, establishing the TSP Program. The TSP Program is the regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service.

In July 1999, a TSP Oversight Committee (OC) working group convened to discuss the continued relevance of TSP in the emerging public network, and to discuss the role of TSP in relation to packet-based networks. The results of the discussion offer insight into the potential implications of convergence for TSP.

The working group noted that TSP was conceived to apply to common carriers, and specifically to circuits. (More recently, TSP has been extended to protect important control space facilities and trunk infrastructure between access points). Furthermore, the group stated, "traditional circuit-based technology will remain an integral part of carrier networks for the foreseeable future due to the extensive financial investments that carriers have in the traditional technology and the nascent and relatively unreliable character of packet networks for voice communications**.**"[17] Therefore, the group argued that TSP, as originally conceived, remains relevant in a converged network because restoration assignments can still be applied to identifiable segments of the PSN. These segments specifically include the access portions of carriers' networks and private lines. TSP restoration assignments enable carriers to provide priority restoration of the access portion of critical NS/EP circuits during emergencies when there may be contention for service with other entities. Additionally, because of the recognized top priority of TSP restoration should a disaster occur, carriers and enhanced service providers (e.g., Illuminet) use TSP to augment the dependability of their facilities. In essence, TSP serves to assure physical network facilities.

However, many industry experts believe that due to the increasingly competitive nature of the telecommunications field, the implementation and expansion of packet-based networks by new and existing carriers will take place at an accelerated rate during the next several years. This will result in substantially greater network bandwidth and rich interconnectivity, greatly reducing the likelihood of network outages caused by facility failures. In addition, multiple access technologies (local loop, cable, wireless, fiber, satellite) and multiple competitive local exchange carriers (CLEC) will offer the NS/EP user diverse routing sufficient to overcome many access failures. Working group members asserted that TSP did not and should not have a role in this packet network realm. The working group noted that Internet service providers (ISP) that offer voice services are not classified as common carriers. Therefore, because the FCC *TSP Report*

[17] *TSP Oversight Committee Packet Network Working Group* meeting summary, July 26, 1999.

and Order applies only to common carriers, and ISPs are not now defined as such, they are not obligated to offer TSP services. Also, as previously noted, the *TSP Report and Order* states that the program is applicable only to public switched network services. Consequently, the working group concluded that if the NS/EP community required similar types of priority services for packet networks, a new program would have to be established to support such services.

2.2 Implications of Convergence and the NGN for NS/EP Requirements

Satisfying NS/EP functional requirements during Convergence and in the NGN is an important consideration. Functional requirements such as priority treatment, nationwide coverage, and interoperability may necessitate the translation of NS/EP services and requirements across disparate networks during Convergence. Additionally, requirements such as enhanced priority treatment, infrastructure restoration, survivability, and scalable bandwidth may require the extension or development of specific NS/EP services for the NGN and the expansion of existing security mechanisms. Therefore, the Government, in coordination with industry, should determine, as soon as practicable, the precise functional NS/EP requirements of the NS/EP community during Convergence and in the NGN. A diligent process for determining these needs is required because of the quickness in which packet-based network standards are being developed and implemented. Otherwise, erosion of compliance with NS/EP functional requirements and readiness will occur. Executive Order 12472 assigns responsibility for the execution of NS/EP telecommunications functions to the NCS, the Executive Office, and other Departments and Agencies. Among these responsibilities, Executive Order 12472 directs the NCS to seek to ensure that a national telecommunications infrastructure is developed that "is capable of satisfying priority telecommunications requirements under all circumstances." Therefore, the OMNCS would be the appropriate body to coordinate NS/EP requirements activities. Some guidelines to consider in defining requirements during Convergence and in the NGN are discussed in the following sections. Possible solutions for satisfying potential NS/EP functional requirements in the NGN are discussed in Section 3.

2.2.1 Facilities-based NS/EP Requirements

Although TSP will continue to be relevant for the immediate future, the rapid deployment of IP network technology and diverse access technologies by new and existing carriers precipitates the need to examine NS/EP community priority restoration and provisioning needs during Convergence and in the NGN. It is possible that, in times of emergency, the NS/EP community might require priority restoration and provisioning of the access portion of packet networks, such as copper loops, cable, fiber, satellite, routers, or other packet network infrastructure. It is also possible that some NS/EP users may be able to reduce the need for priority restoration with diverse access.

However, to fulfill any facilities-based NS/EP service requirements during Convergence and in the NGN, regulatory questions may need to be addressed. The FCC *TSP Report and Order* requires all common carriers to offer TSP services. However, because ISPs are not now

considered common carriers, they could offer QoS features by contract to their subscribers whereby they establish guidelines for enhanced restoration and provisioning treatment of facilities. These sorts of guidelines could conflict with those established for the TSP program. Therefore, the NS/EP community must define in a timely manner the need for facilities-based priority services during Convergence and for the NGN and propose the most appropriate and realistic method of satisfying those needs. The Government should examine these issues promptly and thoroughly.

2.2.2 Connections-based NS/EP Requirements

Because GETS continues to be relevant in circuit switched networks, the Government should continue to examine the implications of Convergence for GETS features. For instance, it is conceivable that in times of severe natural/man-made disasters or coordinated attacks, even the broadband packet-based NGN could experience congestion or outages, requiring that qualified GETS users be identified. Consequently, the Government should investigate the connections-based priority services needs of the NS/EP community during Convergence and for the NGN and analyze the appropriate methods of satisfying those needs. Relevant information should be conveyed to the appropriate standards bodies for consideration, as warranted.

The Government has submitted a draft document to the Internet Engineering Task Force (IETF) and European Telecommunications Standards Institute (ETSI) Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) that defines functional requirements for fulfilling the International Emergency Preference Scheme (IEPS) in the newly emerging telecommunications infrastructure. The IEPS is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation that will enable authorized users to have priority availability of telecommunications services and processing of communications for supporting recovery operations during crisis situations.[18] The Government states the features needed to support IEPS emergency communications in IP-based networks (which would encompass domestic NS/EP communications) include priority access, routing, processing, and egress on an end-to-end basis and for the duration of the communication.[19] Specifically, the Government states that IEPS issues to be considered during the phases of transition from circuit switched networks to IP-based networks include —

- The protocol mechanisms of IP-based networks in operation and under development that could convey an HPC-type IEPS indicator to identify an emergency communication. This would enable priority routing and processing ahead of other traffic being carried.
- A field in the header of any candidate protocol to convey an emergency communication indication needs to be identified and space reserved for a codepoint.

[18] National Communications System, *Functional Requirements for Priority Services to Support Critical Communications*, Temporary Document 17TD, presented to TIPHON 17.
[19] *Ibid.*

- Appropriate codepoint(s), which will be used to convey the IEPS indicator through the IP-based environment, will need to be registered.
- Procedures and processes will need to be defined for handling the IEPS indicator in the IP-based environment. This includes priority routing of packets and relying on alternate routing capabilities when congestion is encountered.[20]

Furthermore, as IP-based capabilities evolve, additional IEPS service issues should be considered including maintenance of the priority status of a communication for its duration after setup, alternate routing of IEPS communications when congestion and failure occur, and definition of multiple levels of emergency priority.[21]

The Government should remain actively involved in the IEPS processes in the various standards bodies and industry forums.

2.2.3 Services-based Functional Requirements

The widespread deployment of IP functionality could enable a wide range of essential NS/EP broadband service-based features (e.g., Web-based features, video on demand). Therefore, priority provisioning and restoration of packet network services for the NS/EP community may become a functional requirement in the NGN. As packet-based networks become prevalent, the need for service-based priority services (e.g, preferential treatment for establishment and restoration of E-mail, Web access, file transfer, and broadcast and multicast services for voice, data, and video) for the NS/EP community will be an important question.

[20] National Communications System, *Functional Requirements for Priority Services to Support Critical Communications*, Temporary Document 17TD, presented to TIPHON 17.
[21] *Ibid.*

3.0 SATISFYING EXISTING NS/EP FUNCTIONAL REQUIREMENTS IN NEXT GENERATION NETWORKS

3.1 Potential Protocol Mechanisms for NS/EP

Since bandwidth is finite in any given network, including the NGN, periods will exist when the traffic exceeds the capacity of the network, thereby creating congestion (e.g., many-to-one data flows, interface speed mismatches, and overload conditions).[22] Consequently, protocol mechanisms will be needed to ensure an adequate level of service is provided to each packet flow during periods of congestion.[23] Specific protocol mechanisms strive to provide priority to delay sensitive and mission-critical applications, while sharing the remaining bandwidth among the other applications.[24] Therefore, these mechanisms could be used to satisfy NS/EP priority treatment functional requirements in the NGN. The following sections outline the two prevalent protocol methods and specify how they could assist the NS/EP community.

3.1.1 Signaling Method

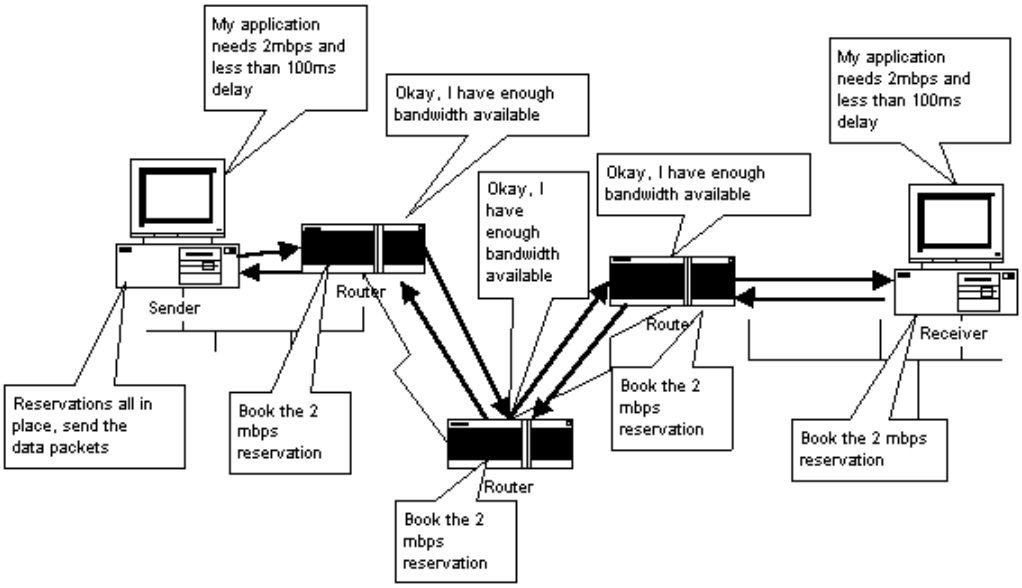
Under the signaling method, an application communicates the characteristics of the traffic it intends to send, and the quality of service (QoS) (e.g., bandwidth and delay) it requires from the network, to each network element via an explicit signaling protocol.[25] In essence, the required resources are reserved from the source to the destination to ensure the data traverses the network. Standards based on the signaling method could support NS/EP priority bandwidth management requirements for communications in packet networks.

3.1.1.1 Reservation Protocol

The Reservation Protocol (RSVP) model, sanctioned by the IETF uses the signaling method. RSVP signals routers to reserve bandwidth to enable a real-time transmission (e.g., voice or video). Figure 1 illustrates how RSVP works.

[22] Rau, Michael, Senior Engineering Manager, Cisco Systems Federal, *QoS Technologies and Call Admission Control* briefing to the ITPITF on Dec. 2, 1999.
[23] *Ibid.*
[24] *Ibid.*
[25] *Ibid.*

Figure 1
RSVP Illustration



The RSVP model could enable priority treatment of and scalable bandwidth for NS/EP traffic provided that some sort of policy control, including access control and user authentication is available. The IETF has set up a working group within its RSVP committee to address such policy issues.[26] The Government should participate in IETF discussions regarding implementation of RSVP to examine the feasibility of its use for NS/EP traffic.

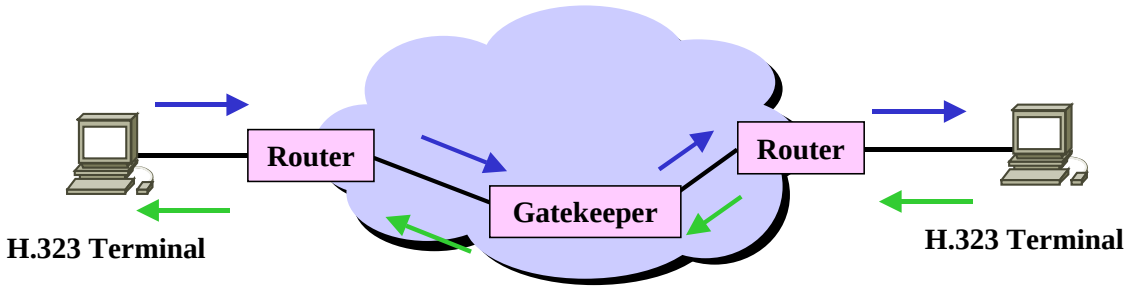
3.1.1.2 H.323

Another variation of the signaling method is the H.323 standard being developed by the ITU. H.323 is a standard that specifies the components, protocols, and procedures that provide multimedia communication services—real-time audio, video, and data communications—over packet networks, including IP-based networks.[27] H.323 networks use gateways that enable connectivity between an H.323 network and a non-H.323 network such as the PSN. This connectivity of dissimilar networks is achieved by translating protocols for call setup and release, converting media formats between different networks, and transferring information between the networks connected by the gateway.[28] Additionally, H.323 networks can use gatekeepers, devices that provide important services such as addressing, authorization, and authentication of terminals and gateways; bandwidth management; accounting; billing; and call-routing services.[29]

[26] Resource Reservation Protocol, http://www.micom.com/WhitePapers/rsvp/wprsvpte.htm.
[27] Internet Engineering Consortium, H.323 Tutorial, http://www.webproforum.com/h323/index.html.
[28] *Ibid.*
[29] Internet Engineering Consortium, *Ibid.*

An H.323 session takes place as illustrated in Figure 2.

Figure 2
An H.323 Session



The steps of an H.323 session are as follows:

1. Source application wanting to set up H.323 session uses Q.931 signaling to set up a call to destination.

2. Call setup includes information about the amount of bandwidth needed to establish call.

3. Gatekeeper tracks available bandwidth between terminal endpoints and determins whether the call will be admitted.

4. Once the call is admitted, the H.323 session can be established.

5. Gatekeeper tracks the session and once the session is terminated releases the bandwidth within the H.323 zone for use by other H.323 sessions.[30]

H.323 could be used to support real-time NS/EP communications through packet networks. Therefore, the Government should continue participation in ITU activities related to H.323 and other evolving signaling standards.

3.1.1.3 Session Initiation Protocol

Another signaling protocol, Session Initiation Protocol (SIP), has garnered much attention of late in the standards community. Developed by the IETF, SIP is a service layer protocol similar to Hypertext Transfer Protocol (HTTP), but it is suitable for both transaction- and connection-oriented services.[31] One of SIP's major virtues is that it provides an inherent service creation

[30] Rau, Michael, Senior Engineering Manager, Cisco Systems Federal, *QoS Technologies and Call Admission Control* briefing to the ITPITF on Dec. 2, 1999
[31] Kozig, Jack, *Standards in the New Millennium*, America's Network, February 1, 2000, http://www.americasnetwork.com/issues/2000issues/20000201/20000201_standards.htm.

capability, enabling users to customize their own service behaviors.[32] In a SIP-based telephony architecture, custom local area signaling service (CLASS) features such as call blocking, call forwarding, and caller-ID can be implemented using a SIP proxy server or in a client device, such as an IP telephone.[33] SIP enables quicker implementation of new voice services than do SS7-based networks.[34] Such efficiency could benefit the NS/EP community as it develops services for mission-critical NS/EP operations.

The Government should continue its active involvement with IETF and contribute NS/EP-relevant recommendations concerning the development of SIP, and other evolving standards. Such standards will be essential in satisfying NS/EP requirements during Convergence and in the NGN.

3.1.2 Packet Labeling Method

Under the packet labeling method, packets are assigned a service class label at the edge of the network and subsequent network elements identify the service class label and treat the traffic accordingly.[35] A small bit pattern in each packet is used to mark a packet to receive a particular forwarding treatment, or per-hop behavior (PHB), at each network node.[36] Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the marking and the policies.[37] In essence, packet labeling facilitates the classification or differentiation of IP network services, enabling the establishment of a differentiated services network architecture.

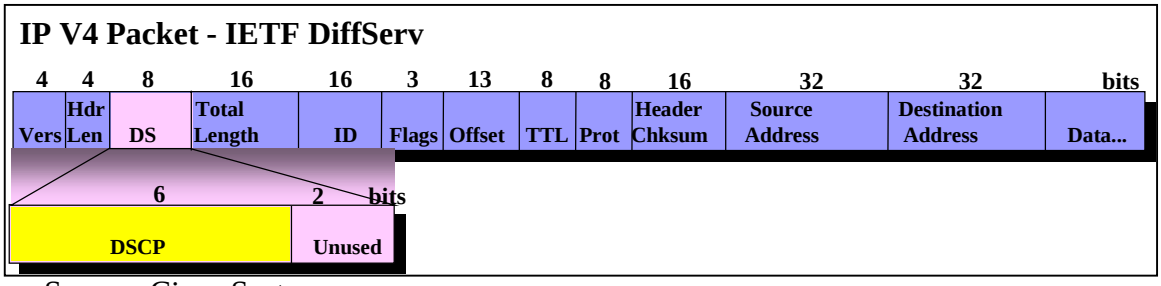
In a differentiated services architecture —

- The IP header includes a differentiated services codepoint (DSCP), indicating the level of service desired.
- The DSCP maps the packet to a PHB for processing by a DS-compliant router.
- The PHB provides a particular service level (bandwidth, queuing, and dropping decisions) in accordance with network policy.[38]

Figures 3 and 4 depict IPv4 and IPv6 packets in the IETF Differentiated Services (DiffServ) model with the DSCP in the headers.

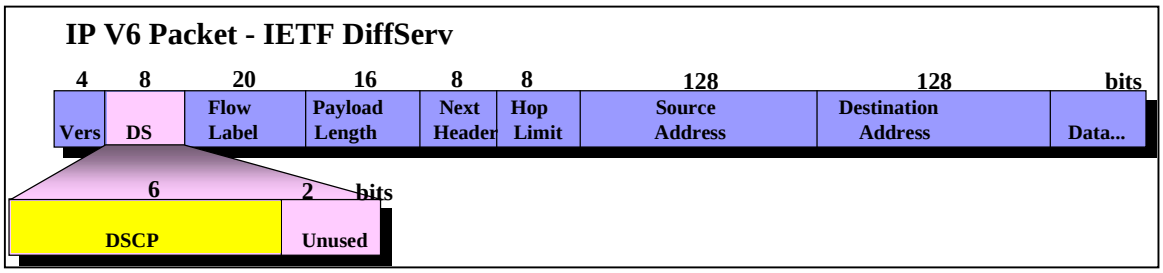
[32] *Ibid.*
[33] Bezaitis, Andrew, and Alkhlaq Sidhu, *Eat or Be Eaten*, America's Network, November 1, 1999, http://www.americasnetwork.com/issues/99issues/991101/991101_eat.htm.
[34] *Ibid.*
[35] *Ibid.*
[36] http://www.nren.nasa.gov/eng/freeman/qos/tsld030.htm
[37] http://kids.intel.com/network/white_papers/diff_serv/diffserv.htm
[38] *Ibid.*

Figure 3
IETF DiffServ IPv4 Packet



Source: Cisco Systems

Figure 4
IETF DiffServ IPv6 Packet



Source: Cisco Systems

Implementation of a differentiated services model in the NGN could facilitate the preferential treatment of mission-critical NS/EP traffic. For example, mission-critical NS/EP packets could be encoded with a DSCP that indicated a high-bandwidth, 0-frame-loss routing path. Conversely, non-mission-critical E-mail and Web browsing data could be coded with a DSCP indicating routine traffic handling with minimal packet drops. The DS-compliant boundary router would then make route selections and forward the packets accordingly as defined by network policy and the PHBs the network supports.[39] Therefore, the highest-class traffic would get preferential treatment in queuing and bandwidth while the lower class packets would be relegated to potentially slower service.[40]

The IETF DiffServ working group is currently examining specific issues related to differentiated services. It is important that the Government remain actively involved in IETF proceedings to ensure consideration of NS/EP services.

[39] *Ibid.*
[40] *Ibid.*

3.1.2.1 Multiprotocol Label Switching

A variation of the packet-labeling method is Multiprotocol Label Switching (MPLS). MPLS is an IETF initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular network, or ISP, to simplify and improve IP - packet exchange.[41] Specifically, MPLS is a routing and switching mechanism and protocol that allows packets within a connectionless network to be switched based on a label that has been appended to the packet.[42] The labels containing forwarding information (i.e., destination, bandwidth, delay, and differentiation) are attached to the IP packets at the edge of the network by a label edge router (LER). This enables the routers in the core of the network, known as label switch routers (LSR), to examine the label more quickly than if they had to look up destination addresses in a routing table.[43] Therefore, MPLS enables router and switches to operate at higher speeds without eliminating address resolution within the network.[44] MPLS could be useful to the NS/EP community because it can be used to create virtual paths that have specific quality and security requirements, which may be available to only specific users. The Government should remain actively involved in IETF discussions regarding MPLS.

3.2 Government Standards Bodies Participation

The Government has developed relationships with many relevant standards bodies including the ITU. Currently, the OMNCS is actively involved in many ITU study groups including Study Group 2 (Network and Service Operation), Study Group 4 (Telecommunications Management Network Studies and Network Maintenance), Study Group 11 (Signaling Requirements and Protocols), and Study Group 13 (General Network Aspects), and Study Group 16 (Multimedia Services and Systems). Study Group 4 is examining a framework for unified management of integrated circuit switched and packet-based networks (with an initial focus on IP-based networks).[45] Additionally, Study Group 13 has developed an ITU-T IP Project which is intended to encompass all ITU-T IP-related work. Area 10 of the ITU-T IP Project is focusing on security.

Additionally, OMNCS is actively participating in the TIPHON group of the ETSI. The objective of ETSI's TIPHON project is to support the market for voice communication and related voiceband communication (such as facsimile) between users. The project's goal is to ensure that users connected to IP-based networks can communicate with users in circuit switched networks and vice versa. TIPHON's products will also ensure communications between circuit switched networks where IP-based networks are used for connection and trunking between the circuit

[41] PC Webopedia, http://webopedia.internet.com/TERM/M/MPLS.html.
[42] Nortel Networks, briefing to the GTI/ITPI, February 25, 2000.
[43] TechWeb Encyclopedia, http://www.techweb.com/encyclopedia/defineterm?term=MPLS.
[44] Nortel Networks, briefing to the GTI/ITPI, February 25, 2000.
[45] ITU Study Group 4 Web Site, http://www.itu.int/ITU-T/com4/questions.html.

switched networks involved.[46] See Section 2.2.2, Connections-based NS/EP Requirements, for information on Government participation in ETSI TIPHON and IETF IEPS deliberations.

The OMNCS is also actively participating in the IETF, the standards body that sets the IP standards most relevant to the NS/EP requirements. Working areas include MPLS, Diffserv, RSVP, SIP, and Policy Framework. In addition, as reported in the NSTAC Embedded Interoperable Security (EIS) Scoping Group Issue Resolution, the Defense Information Systems Agency is working with the IETF IP Security Protocol Working Group (IPSEC) on the development and interoperability of an end-to-end security model based on Public Key Infrastructure (PKI) technology to provide authentication and encryption for mission-critical Internet applications.

The OMNCS continues to work in concert with standards organizations to identify, evaluate, and influence those standards that can enhance the communications capabilities of NS/EP users.

3.3 Summary

Service providers (e.g., ISPs) are currently implementing QoS and priority routing-related technologies on individual networks. As the NGN evolves, end-to-end QoS and priority routing capabilities will be implemented, because they are essential for the transport of voice traffic. These same capabilities will require some modification to best satisfy specific NS/EP requirements at the local, State, and Federal levels. Therefore, the NS/EP community should, as practicable, promptly define specific functional requirements for the NGN. Subsequently, as specific needs are recognized, specific technologies could be identified and, if necessary, modified to satisfy those needs. Additionally, the Government should continue participation in standards bodies activities related to QoS and priority routing technologies to ensure that NS/EP requirements are considered during development and implementation phases. Executive Order 12472 assigns responsibility for the execution of NS/EP telecommunications functions to the NCS, the Executive Office, and other Departments and Agencies. Among these responsibilities, Executive Order 12472 provides the NCS with the authority to seek to ensure that a national telecommunications infrastructure is developed that "is capable of satisfying priority telecommunications requirements under all circumstances." Therefore, the OMNCS would be the appropriate body to communicate NS/EP requirements to standards bodies and participate in NGN-related standards activities.

Another important consideration is that the intelligence of IP networks is periphery-based, and the intelligence of the PSN is centralized. The periphery-based architecture might present additional points of network vulnerability. Therefore, as the NGN evolves, the NS/EP community must consider potential network control space security implications for NS/EP services and operations. Although beyond the scope of this report, this issue warrants further

[46] GETS Program Management Office, *Voice Over Packet Issue Paper*, May 21, 1999.

analysis. Given NSTAC's responsibility for advising the President on NS/EP telecommunications issues, this study would be consistent with NSTAC's established mission.

4.0 CONCLUSIONS

The NS/EP community depends heavily on priority treatment of voice calls within the PSN to support NS/EP operations, and will remain dependent on the PSN for the immediate future. However, telecommunications service providers are rapidly implementing packet-based data networks and plan to transition traffic onto the NGN. Therefore, NS/EP functional requirements may be affected during Convergence and in the NGN.

As discussed in Section 2.1, GETS and TSP services provide only a foundation for analysis of NS/EP services in the context of convergence to the NGN. Other services, such as wireless priority access, dedicated services, and virtual networks, while beyond the scope of this report, also support various NS/EP functional requirements in existing networks.

NS/EP functional requirements such as enhanced priority treatment and national coverage are satisfied in the PSN by GETS. The potential implications for GETS services relating to Convergence and the NGN include—

- **New Blocking Sources.** Newly designed features to support priority NS/EP traffic must be implemented. As yet, there is no guarantee that NS/EP traffic could be given priority over other traffic in a packet network. Therefore, NS/EP traffic requires newly designed and standardized features to overcome new problems associated with packet networks (e.g., the need for a priority mark for NS/EP traffic to facilitate priority treatment for the duration of the call). Without this, NS/EP packets could be discarded.
- **Lack of Ubiquity and Interoperability.** In packet networks, NS/EP calls may not be able to achieve priority access and transport control (e.g., access authorization, routing information). NS/EP requirements are unlikely to be incorporated by industry unless the needed features are standardized by industry, perhaps with prompting from the Government.
- **Lack of Access to GETS Features.** NS/EP calls may not be able to access NS/EP features, particularly on the terminating network, if the calls are transported through a packet network because the nature of signaling associated with call set-up in a packet network has yet to be defined.
- **Disparate Congestion Handling.** Evolving QoS and routing schemes allow specific minimum percentages of bandwidth to be reserved for real-time interactive and non-interactive services in packet networks. However, to provide GETS-type services during Convergence and in the NGN, these schemes must be expanded to provide services commensurate with NS/EP needs.
- **Network Reliability and Security Implications.** The expanded inter-working of the control space of the PSN and Internet technologies during Convergence and the revolutionary open switch architecture of the NGN will likely be areas of network

reliability and security concern to NS/EP users and affect services and functional requirements. The current level of security safeguards incorporated into GETS (e.g., PINs) are inadequate to protect its NS/EP functional requirements during Convergence and in the NGN. Additionally, if current safeguards are employed in the NGN, they will be all the more inadequate based on current Internet security risks (e.g., denial of service attacks).

The TSP Program satisfies NS/EP functional requirements such as priority treatment, for the establishment and restoration of infrastructure in the PSN. The TSP Oversight Committee (OC) discussed the potential implications for TSP during Convergence and in the NGN. The OC stated that traditional circuit-based technology would remain an integral part of carrier networks for the foreseeable future due to the extensive financial investments that carriers have in the traditional technology. Therefore, the OC argued that TSP, as originally conceived, remains relevant during Convergence because restoration assignments can still be applied to identifiable segments of the PSN. However, OC members asserted that TSP did not and should not have a role in the NGN. They noted that ISPs offering voice services are not classified as common carriers and are therefore not obligated to offer TSP services. Consequently, the OC concluded that if the NS/EP community required similar types of priority services for packet networks, a new program would have to be established to support such services. Additionally, the ITPITF asserts TSP-type services in the NGN will provide for the priority provisioning and restoration of network services rather than circuit-based services.

Although specific NGN standards have not yet been developed to support NS/EP requirements, the NGN technology is capable of supporting these requirements. Furthermore, standards bodies are currently examining protocol mechanisms that may satisfy certain NS/EP functional requirements in the NGN. Two prevalent protocol methods are the signaling method and the packet labeling method. These methods could enable priority treatment of and scalable bandwidth for NS/EP traffic provided that some sort of policy control, including access control and user authentication is available.

Service providers are currently implementing these protocol mechanisms on individual networks. As the NGN evolves, end-to-end QoS and priority routing capabilities will be implemented, because they are essential for the transport of voice traffic. These same capabilities will require some modification to best satisfy specific NS/EP requirements at the local, State, and Federal levels. Therefore, the NS/EP community should, as practicable, promptly define specific functional requirements for the NGN. Subsequently, as specific needs are recognized, particular technologies could be identified and, if necessary, modified to satisfy those needs. Additionally, the appropriate departments and agencies should continue participation in standards bodies' activities related to QoS and priority routing technologies to ensure that NS/EP requirements are considered during development and implementation phases.

An important consideration is that the intelligence of IP networks is periphery-based and the intelligence of the PSN is centralized. The periphery-based architecture might introduce

additional points of network vulnerability. Therefore, it is necessary to consider the security, reliability, and availability of the NGN control space as it relates to the provision and maintenance of NS/EP services capabilities.

5.0 RECOMMENDATIONS

The following recommendations are proposed to enhance understanding and awareness of NS/EP requirements related to Convergence and the NGN among the NS/EP community and appropriate standards bodies.

5.1 NSTAC Recommendation to the President

Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies, in coordination with industry, to —

- promptly determine precise functional NS/EP requirements for Convergence and the NGN, and
- ensure that relevant NS/EP functional requirements are conveyed to standards bodies and service providers during NGN standards development and implementation.

5.2 NSTAC Recommendation to the IES for Consideration in the NSTAC XXIV Work Plan

Examine potential NS/EP implications related to possible security and reliability vulnerabilities of the control space in the NGN. The NSTAC's *Final Report of the Common Channel Signaling Task Force* (January 31, 1994) should be used as a foundation for this analysis.

APPENDIX A

TASK FORCE MEMBERS AND OTHER CONTRIBUTORS

TASK FORCE MEMBERS

Nortel Networks	Dr. Jack Edwards, Chair
Cisco Systems	Mr. Jim Massa, Vice-Chair
AT&T	Mr. Paul Waldner
Boeing	Mr. Bob Steele
COMSAT	Dr. Jack Oslund
CSC	Mr. Guy Copeland
GTE	Mr. James Bean
ITT	Mr. Joe Gancie
Lockheed Martin	Dr. Chris Feudo
Raytheon	Mr. John Grimes
SAIC	Mr. Hank Kluepfel
USTA	Mr. Vern Junkmann

OTHER PARTICIPANTS

Cisco Systems	Mr. Robert Gooch
OMNCS	Mr. Harold Folts

COMPANY/AGENCY CONTRIBUTORS

Cisco Systems Federal
Deloitte and Touche, LLP
MCI WorldCom
Nortel Networks
OMNCS
Telcordia Technologies

APPENDIX B

ACRONYM LIST

ACRONYM LIST

AIN	Advanced Intelligent Network
CLASS	Custom Local Area Signaling Service
CLEC	Competitive Local Exchange Carriers
COTS	Commercial Off-the-Shelf
CPE	Customer Premise Equipment
DSCP	Differentiated Services Codepoint
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GETS	Government Emergency Telecommunications Service
HF	High Frequency
HPC	High Probability of Completion
HTTP	Hypertext Transfer Protocol
IEPS	International Emergency Preference Scheme
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Providers
ITPITF	Information Technology Progress Impact Task Force
ITU-T	International Telecommunication Union-Telecommunications
IXC	Interexchange Carrier
LEC	Local Exchange Carrier
LER	Label Edge Router
LSR	Label Switch Routers
MPLS	Multiprotocol Label Switching
NCS	National Communications System
NGN	Next Generation Network
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
OC	Oversight Committee
OMNCS	Office of the Manager, National Communications System

PCS	Personal Communications Service
PHB	Per-Hop Behavior
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PN	Public Network
PSN	Public Switched Network
QoS	Quality of Service
RSVP	Reservation Protocol
SIP	Session Initiation Protocol
SS7	Signaling System 7
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TSP	Telecommunications Service Priority