Internet Priority Service (IPS) Request for Information (RFI) Assessment Report

Refer requests for this document to:

National Communications System/N2
P.O. Box 4502
Arlington, VA 22204-4502

Phone (703) 607-6178
Email jeffrey.a.smith@dhs.gov

June 2004

Table of Contents

1 Introduction

This report presents an assessment of Internet industry responses to a Request for Information (RFI) from the National Communications System (NCS) seeking technical information regarding Internet-based assured communications for data applications (see Appendix A), including Voice over Internet Protocol (VoIP). Responses contain technical information on Next Generation Networks (NGN) emerging technologies received from commercial entities, academic institutions, and government departments and agencies. The report also provides a broad assessment of Internet Protocol (IP) emerging technologies, develops a list of major findings, and a list of NCS recommendations.

1.1 Background

The NCS, as directed by Executive Order 12472—*Assignment of national security and emergency preparedness telecommunications functions*, is responsible for the development of a national telecommunications infrastructure responsive to the national security and emergency preparedness (NS/EP) telecommunications needs of the President and Federal departments and agencies.

The NCS defines and administers programs such as the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS), which provide priority access to resources in the Public Switched Telephone Network (PSTN) in wireline and wireless networks. The emphasis of these services is on voice communications and voice band data transmission. In the future, NS/EP communications services will likely encompass various kinds of multi-media communications, allowing users to exchange and retrieve data and video information, as well as voice.

Telecommunications market conditions are pushing many PSTN service providers to transition their networks and services to IP technology by converging voice and data communications on the same physical network infrastructure. Anticipating this convergence, the NCS is looking for ways to provide assured communications for data applications and voice or video applications using the IP technologies.

In November 2003, the NCS posted an RFI (see Appendix A) requesting information on contractor/vendor current IP capabilities and plans for future IP capabilities that might be used to support an Internet Priority Service (IPS) program for NS/EP users. The information received from the RFI responses will be used to help the NCS achieve the following goals.

- Identify plans and emerging technologies for providing priority services through the Internet.
- Accelerate promising technologies by prototyping and proof-of-concept projects.
- Promote industry-wide adoption of these technologies through the industry standardization process.

- Model technologies to determine what enhancements (if any) are required to meet stringent NS/EP requirements.
- Enable the NCS IPS to leverage and enhance future commercial priority service capabilities.

1.2 IPS Problem Overview

There are often competing motivations for deploying priority within the Internet due to different business philosophies within industry and government. This section reflects what was learned before and during the RFI assessment process.

1.2.1 Current NCS business Model

The NCS is responsible for Continuity of Government (COG) communications under stressed conditions. Two existing programs continuing to evolve are the GETS program and the WPS program. GETS provides prioritized voice communications using the PSTN while WPS provides priority calls using cellular network services. Both of these programs are based primarily on voice communications.

The government pays carriers to enable these capabilities within the existing public domain networks. With the ever expanding use of the Internet and data communications in everyday government business, there is a need to develop services that use the Internet as well as IP technologies with similar levels of assurance that are provided by the GETS and WPS services. One of the early NCS requirements for IPS is the migration of GETS services to IP technology services. The GETS carriers already have initiatives to migrate voice services from circuit switched technologies to packet-based technologies. The NCS must ensure that the current service robustness provided by GETS and WPS will be assured in the IP services domain.

To ensure reliability, security and Quality of Service (QoS), mission critical applications are normally deployed within an enterprise's private or managed IP network (e.g. dedicated circuits and/or services with no shared resources). The challenge the NCS faces is deploying an NS/EP IP service to 22 member agencies and state and local responders that do not have a common dedicated IP network infrastructure. These organizations will use various approaches that could possibly use shared commodity IP services or Virtual Private Networks (VPNs) resources both on their Intranet as well as inter-connectivity with other agency's networks. These connectivity approaches do not have QoS guarantees. Furthermore, it is unrealistic for all agencies to deploy private networks and dedicated connections between agencies in support of NS/EP.

An IPS solution that fits within the NCS business model requires that QoS and priority are end-to-end and among network providers. Furthermore, NCS cannot cause a paradigm shift within the Internet to meet these goals. Currently, no carriers are providing a service within a public network environment where QoS and priority markings are recognized and acted upon. However, there is a great deal of emphasis being placed on this general problem due to the

importance of data applications in everyday business communications and the migration of voice services to the Internet.

1.2.2 Internet/Industry Business Model

Telecommunications carriers see a target of opportunity to migrate current voice and data services onto a single networking technology in order to save on life cycle costs associated with maintaining two separate networks. Adopting a single network technology for all services simplifies operations and mitigates high costs of maintaining many diverse technologies providing the same services. IP technology appears to be the preferred migration path for current voice services, as well as for evolving modern data and video services. Voice, data, and video services need to be ubiquitous through the high-speed optical backbone, fixed and mobile wireless, and other broadband networks. Today, the telecommunications industry recognizes that all of the capabilities in the circuit switched world are not necessarily available using the current IP technologies.

Moderate congestion on Inter-carrier peering links and even on Intra-carrier links occurs daily on the Internet, and can result in packet loss and higher latency and jitter. Deploying QoS sensitive applications such as voice in this environment is not an option without additional priority and QoS guarantees. This is a large impediment to deploying IPS. The government needs to continue working closely with industry to develop a strong business case that serves both the industry and the government while upgrading the telecommunications infrastructure to support IPS communications. Deploying IPS within the NCS business model requires that the Internet and IP managed services support priority services ubiquitously, and that priority traffic is effectively controlled as it is transported among carriers.

1.2.3 Current Collaboration Efforts

There is participation from telecommunications and Internet service providers, government (NIST, DISA, DOS, DHS/NCS) and equipment manufacturers in many standards bodies and forums supporting development of standards for advanced IP features and capabilities. Standards organizations supporting IP priority and Emergency Telecommunication Services (ETS) include the Internet Engineering Task Force (IETF), International Telecommunications Union (ITU), and Alliance for Telecommunications Industry Solutions (ATIS). The IETF is addressing Inter-carrier traffic engineering requirements at this time. Moreover, there are industry bodies and consortia such as the “Infranet Initiative” addressing business impetus for deploying priority services in the Internet and exploring how standards can be deployed that are more sensitive to the quality concerns of the Internet users.

One area to be addressed by the ITU effort to develop global standards for NGNs is the concept dubbed "nomadicity," which will give fixed line and mobile users completely seamless communications, so the underlying technology will be invisible to the user regardless of a multi-service, multi-protocol, multi-vendor environment. An ITU-T Focus Group plans to build on

existing fixed/mobile convergence architecture (e.g. 3GPP/3GPP2 IP multimedia subsystem (IMS)) to provide transparency between fixed and mobile networks.

1.2.4 IPS Convergent Network Architecture

Figure 1-1 illustrates the concept of a converged telecommunications architecture that is Internet concentric. In this concept, IP is the common network layer addressing scheme that provides applications and network control layer services between end-systems and the underlying telecommunications infrastructure. There is emerging consensus that IP will be the common network layer protocol across all services due to its robustness, scalability, and large deployed base. Major efforts are underway at both the control and service layers to develop protocols that bind the four layers in this model. There is a need to develop an integrated architecture in which the application layer is able to control the lower layers of the network to meet service requirements. The current Internet architecture adequately provides connectivity between end-systems although it is unable to meet the reliability, security and QoS requirements of more advanced services such as emergency telecommunications, voice or video services.

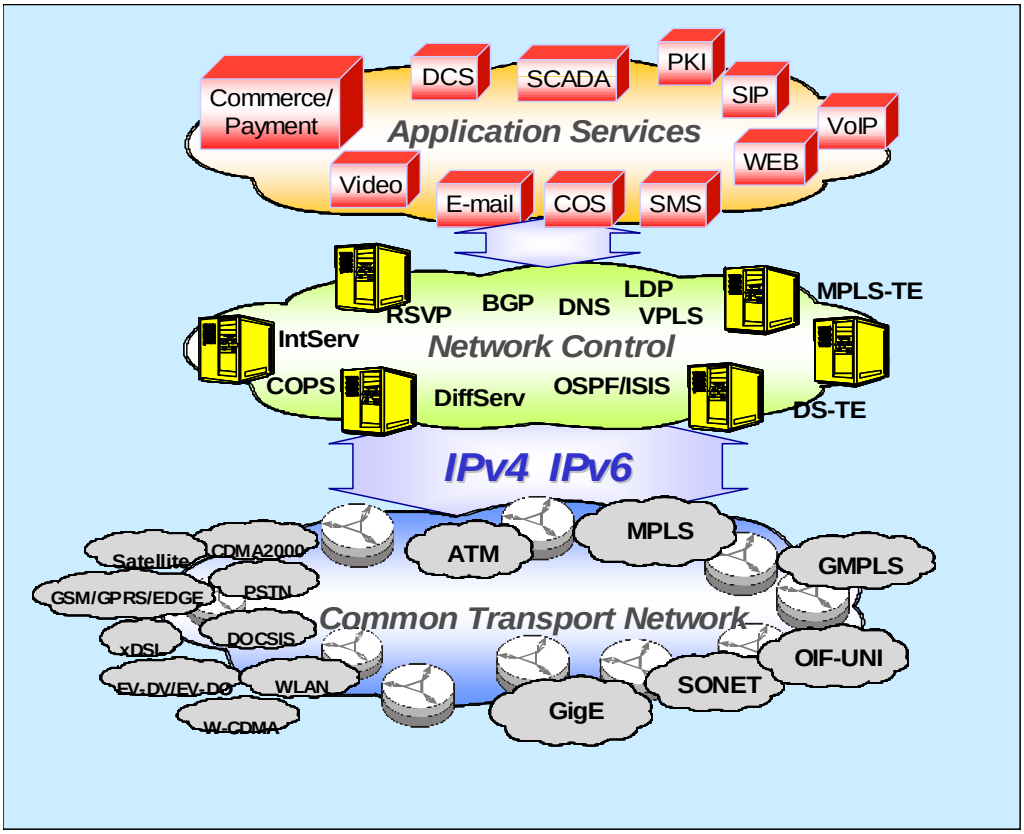

Figure 1-1. Converged Network Architecture

1.3 NGN Functional Requirements

The White House Communications Managers Working Group has developed a set of high-level functional requirements for NS/EP priority communications. From this set of requirements, it was decided that the implementation of the IP NS/EP priority communications, the IPS, must conform to the following functional requirements.

- Service Assurance – NS/EP national leadership must be assured constant availability of NS/EP user-to-user telecommunications services (wire line and wireless), without service degradation in stressed and hostile environments, with highest restoration priority in the event of loss or damage to facilities.

- Interoperability – NS/EP national leadership must be assured seamless systems and services interoperate with current and emerging government and public services systems and networks.

- Priority Treatment – In the event of crisis, NS/EP national leadership must receive end-to-end priority treatment over other users.

- Ubiquitous Coverage – NS/EP national leadership must be assured seamless connectivity to government and public services and systems regardless of location.

- Access and Identity – NS/EP national leadership must be provided the highest level of security against technological vulnerabilities. Features must include user anonymity, non-traceability, and protected access.

- Bandwidth Services – NS/EP national leadership requires assured access to government and public telecommunications services offering integrated high quality voice, scalable data and a full-range of video services for NS/EP telecommunications.

- Quality of Service – NS/EP traffic must be identified with its own class of service – beyond “best effort”.

1.4 Scope of Report

This report presents an assessment of responses to the RFI by industry, government and educational institutions for designing, developing, and providing an IPS. Additionally, it provides an assessment of IPS emerging technologies based on information received from RFI respondents and technical discussions with organizations and institutions providing or conducting IPS research and development. Included in the report is a listing of major findings as well as a list of NCS recommendations. This information will be used for the purpose of defining and developing the future IPS program.

1.5 Approach

The NCS assembled a team of subject matter experts from various technical and programmatic areas to assess the forty-seven (47) responses to the IPS RFI. The responses were

gleaned for information and ideas that could be applicable to follow-on activities supporting the NCS goals.

This report presents ideas, concepts, and protocols that were components of the recommended solutions put forth by the responders, as well as information obtained from other outside sources such as standards bodies, technology forums, technology magazines, and professional organizations (e.g. IEEE, ITU, IETF, etc.). The technologies documented in this report are those that the NCS deems most likely to be used to meet the IPS Next Generation Networks (NGN) NS/EP functional requirements.

1.6 Document Organization

The remainder of this report is organized as follows:

- Section 2 provides an assessment of the RFI responses.
- Section 3 lists the major findings derived from the IPS RFI responses.
- Section 4 contains conclusions and recommendations.
- Section 5 a glossary of terms.

The report also includes several appendices:

- Appendix A contains a copy of the RFI: Internet Priority Service (IPS) Capability Design/Development, issued November 21, 2003.
- Appendix B contains a technical assessment of NGN convergence technologies.
- Appendix C is the list of respondents. [Proprietary]
- Appendix D is a synopsis of some proprietary responses and recommendations. [Proprietary]
- Appendix E contains abstracts for each of the forty-seven (47) respondents to the RFI. [Proprietary]

2 RFI Response Assessment

The technologies documented in this section are those the NCS deemed most relevant to meeting the NS/EP functional requirements. During the assessment of RFI submissions, the RFI submissions were grouped into five general categories based on the submitters' business types as follows:

1. GETS carriers
2. Internet Service Providers (ISPs)
3. Equipment and software vendors

4. Research organizations

5. Consultants/Integrators/Engineers

The following subsections provide an overview of the responses received for the five categories listed above. Each section addresses the applicability of the RFI responses to support the NCS goals. If applicable, an assessment of how the respondents as a whole could meet the NS/EP functional requirements is also provided.

2.1 GETS Carriers

Two RFI respondents provided their NGN migration plans with respect to GETS. Both responses identified program plans, emerging technologies and new areas requiring standardization. Basic guidance was given regarding establishing programs to move forward with GETS migration to Internet based services.

This included private test beds and prototypes within a single carrier to understand possible implementations of IPS, and extension of a test bed across industry to meet ubiquity and interoperability requirements of the NCS.

The solutions centered around using existing standards and off the shelf solutions to achieve a systems design meeting NS/EP requirements. It also included many new standards ideas that could achieve more stringent NS/EP standards. The standards suggested would include priority treatment of NS/EP traffic above all other traffic than could otherwise be achieved with the current protocol standards. Currently there is no consensus among the GETS carriers as to whether deployment on private IP networks is required to mitigate the QoS and security concerns of a public IP network.

2.2 Internet Service Providers

A range of services supporting priority data applications were proposed by several large ISPs operating with either national or regional footprints. These responses were predominantly fixed wire-line services, with the exception of one Cellular IP data proposal.

The responses identified primarily emerging and deployed technologies and services. Some responses identified additional standards required to achieve interoperability among ISPs. The solutions centered around using existing standards and off the shelf solutions to achieve a systems design meeting the requirements of the NCS. The solutions focused on transport layer and network control layer solutions. In general, the responses did not address implementing specific IPS applications. A variety of solutions using either VPNs or public networks were proposed. Some solutions also proposed enhancement of current control layer protocols to achieve a higher service assurance.

2.3 Equipment and Software Vendors

A wide variety of responses were submitted providing information about potential hardware and software solutions in support of IPS. In most cases, the government would procure these

solutions indirectly from service providers, carriers, or integrators in support of IPS. Included were security software, QoS hardware and software, and network equipment such as routers and switches. Some proposals also proposed an IPS framework. These responses were valuable, as they both identified some alternate technologies and corroborated other ideas with respect to those identified by the carriers and ISPs.

The responses identified emerging and future technologies and services. Some responses identified additional standards required to achieve interoperability among ISPs. Some proposals consisted of proprietary implementations that would require standardization.

Many solutions centered on using existing standards and implementations to provide an IPS solution. However, several solutions proposed proprietary mechanisms to more effectively manage network priority and QoS. The solutions centered around transport layer and network control layer solutions, and enhanced security necessary for an IPS.

2.4 Research Organizations

Four responses dealt with research and development (R&D) projects for IPS. The responses proposed a large number of R&D projects covering a wide spectrum of technologies. These included network and architectural modeling, traffic engineering, enhanced routing algorithms, security, optical transport, VoIP, and application environments.

The responses targeted the two NCS modeling and R&D goals and covered the transport, control and applications layers of the converged network protocol model shown in Figure 1.1. Additionally, one vendor suggested modeling the BGP4 protocol in support of IPS to determine behavior of US facilities and interests in a global Internet.

2.5 Consultants/Integrators/Engineers

A large number of respondents in this category provided general information about available consulting services and their company's particular area of expertise. Some of these responses proposed either partial or substantial portions of an IPS architecture. Many of the responses were consistent with the architectures provided by the ISPs and carriers. Some of the responses provided IPS architectures and programmatic approaches for achieving NCS and IPS goals. In a few instances, program plans included obtaining network services from carriers and ISPs, and integrating with the company's applications such as video teleconferencing. However, none of the responses provided a complete end-to-end architecture encompassing the network design and a full range of applications (voice, video, email, messaging and web) in support of NS/EP.

Many of these responses identified standards based emerging technologies and recommended program plans for an IPS. Additionally, some companies recommended modeling and standards work in support of the NCS goals. Solutions encompassed using existing standards, off the shelf solutions, and currently available services in the public domain to achieve a systems design meeting the NS/EP requirements. The solutions included the transport layer and network control layer solutions necessary for IPS, and enhanced security features necessary for an IPS, although there was little emphasis on applications in support of IPS.

3 Findings

The major findings listed below were derived from the formal RFI responses or at subsequent meetings with the responders. The findings are the collective results of the review of the 47 RFI responses, technical sessions, and meetings with industry, government and educational institutions. References in "[]" are either general findings or are attributed to specific respondents. The respondents have been numbered using the number assigned in Appendix D.

- Some companies proposed an overall IPS solution, however, they were not considered a viable, cost effective, open standards solution for an ubiquitous IPS that supports all types of services (e.g. voice, data and video) [General Finding]

- Most telecommunication companies discussed network technologies like MPLS, DiffServ, but were non-committal about actually deploying these technologies with respect to their current business development or to an IPS. [General Finding]

- There is no consensus among carriers on an architecture for providing VoIP services, let alone prioritized VoIP service, although GETS providers and most ISPs offered two VoIP alternatives: [Appendix D/E, #1, 2, 3, and 6]
    - A private IP service using a SONET transport separate from the Internet.
    - Public Internet infrastructure in conjunction with separate voice and data VPNs.

- One telecommunication company proposed a process to develop a VoIP framework to support GETS and SRAS as well as a standards development process for Inter-carrier NS/EP prioritization. [Appendix D/E, #1]

- Market forces could drive carriers to reduce cost by concentrating switched services and IP services onto one IP infrastructure, potentially impacting existing NCS services, like GETS, SRAS and WPS. [Appendix D/E, #1]

- There are emerging IP Quality of Service (QoS) technologies that are being deployed in single provider Intra-AS environments. These technologies are both standards based and proprietary, and can provide QoS through an Intranet, especially in support of Voice over Internet Protocol (VoIP). [Appendix D/E, #1]

- At least one company did propose to offer QoS/prioritization services on the edge/ingress into their network, however, the core would not treat marked packets with higher priority than those without priority markings [Appendix D/E, #2].

- A couple of companies did offer QoS/prioritization in the core and edges of their private IP networks but not on their standard Internet service offerings [Appendix D/E, #1 and 2].

- Companies are actively participating in the standards development processes via national and international standards bodies, organizations, and communities; in the areas of IP VPNs and QoS technologies. [General Finding]

- End-to-end prioritization of VoIP, video and/or data service requires collaboration among carriers to agree on common QoS standards and reliability assurances. Currently there are no mechanisms for providing ubiquitous Inter-Carrier QoS standards and reliability assurances, except for Service Level Agreements (SLAs). [Appendix D/E, #6, 7, and 37]

- Most, if not all, ISPs do not intentionally honor or act upon other ISP's prioritization marking on packets, unless there is a Service Level Agreement (SLA) signed by both parties. [Appendix D/E, #14]

- No company adequately addressed the viability of QoS technologies in a severely damaged network infrastructure. Some addressed the technologies' capabilities in a congested environment, but not with a significantly degraded infrastructure. [General Finding]

- Most companies understood and addressed security concerns with respect to a VoIP deployment and proposed to use a VPN to isolate the voice network from the data networks. However, a significant amount of work needs to be done to ensure the security of SRAS calls and the protection of the Authentication, Authorization and Accounting (AAA) and Connection Admission Control (CAC) systems. [General Finding]

- The IETF Traffic Engineering (TE) Working Group (WG) is developing specifications for providing QoS functions through Multiple Protocol Label Switching (MPLS). [Appendix D/E, #1]

- GETS responders provided both a high level VoIP architecture as well as a prioritized VoIP architecture specifically in support of the GETS system. [Appendix D/E, #1 and 2]

- Industry is aware of the security issues regarding converged networks. [Appendix D/E, #1 and 2]

- Protocols and approaches are being developed by the carriers to make the control systems more secure. [General Finding]

- IPv4 is supported by most RFI responders and continues to be the industry standard. Although IPv6 is not widely implemented at this time, it is supported in most hardware and software being offered today [General Finding].

- The IETF has specified a set of extensions for presence and instant messaging, known collectively as SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), and it has been adopted by the Third Generation Partnership Project (3GPP) and 3GPP2 standards bodies. [General Finding]

4 Conclusions and Recommendations

This section provides conclusions and recommendations reached in the assessment of the IPS RFI responses.

4.1 Conclusions

The IPS RFI assessment effort revealed that there is no overall priority or end-to-end QoS architecture in place on the Internet today. Furthermore, ubiquitous priority and QoS on the Internet is not possible without a significant new investment in network hardware and agreement among the various IPS service providers to honor priorities set on incoming packets. There will also need to be new investment and policy development in configuration control, management, and AAA systems, to ensure proper implementation and control of network resources. There are serious concerns within the network community that a miss-configured prioritization service could be used against the Internet infrastructure and cause significant impact to Internet resources.

Network Service Providers (NSPs) today are deploying QoS and priority techniques, but only within an individual NSP's network and not between NSPs at peering points. When QoS techniques are deployed, they are normally deployed on the edge of the network and only within a customer's VPN. However, since most service providers are not deploying QoS technologies throughout their network, these technologies will not reduce the impact of congestion on a customer's VPN, if the VPN is provided via the NSPs' Internet infrastructure.

Differentiated Services Traffic Engineering (DS-TE) Maximum Allocation Resource (MAR) appears to be the most advanced means for addressing QoS within MPLS networks. It is a draft IETF standard, and routing equipment implementations are just becoming available for carriers to deploy. However, not all router hardware can support this technology. A combination of DS-TE MAR, DiffServ, a second Expedited Forwarding (EF2) queue class for NS/EP traffic, Session Initiation Protocol (SIP) CAC, and other techniques are required to give NS/EP traffic the highest priority and to assure VoIP service in severely degraded network conditions. However, there are some concerns in the network community regarding DiffServ's ability to perform in a severely congested network that has been degraded due to an infrastructure failure. More R&D is required in all areas listed above.

While there is a lack of formalized QoS standards, there is substantial activity within the standards community, hardware and software manufacturers and service providers to formalize these standards. Equipment vendors are developing scaled down versions of QoS standards and service providers are deploying vendor specific versions of the QoS on an Intranet basis. With respect to inter-ISP QoS, there are business considerations regarding NSPs honoring QoS/prioritization technologies among their networks. There are no financial drivers for one ISP to honor prioritization markings from another ISP. Furthermore, if a packet is destined to another network, the nature of the Internet is to hand off that packet to another ISP as soon as

possible. Now there must be a trust relationship between each provider that each will adhere to policies defining what a prioritized packet is and that the other networks will honor prioritization from other ISPs. Since there are so many ISPs and each ISP establishes bi-lateral agreements, consensus regarding QoS parameters and how each network will act on these parameters will be very difficult.

While the IPS RFI provided significant government requirements for migrating NS/EP voice applications (i.e. GETS) to VoIP, it did not adequately address other types of NS/EP application requirements. As a result, the responses were more generally oriented towards voice and focused on network transport and control layers within a single administratively controlled network. However, no responder adequately explained the upper layer protocols (e.g. SIP) and the hardware and software upgrades necessary to support and NS/EP VoIP service.

Due to the best-effort and open systems nature of the Internet, significant implementation and validation of security policies and network architectural approaches for VoIP and other IPS applications should be pursued, because applications will be vulnerable to many of the well-known security vulnerabilities present in the Internet today. More successful and robust VoIP implementations will most likely be deployed within private or restricted networks (e.g. MPLS VPNs) to avoid these security issues. NS/EP services can be made more robust with NGN NS/EP feature enhancement such as those addressed in this report.

The NCS needs to conduct additional studies of new features that can mitigate congestion and network outages and maintain NS/EP services up to 8x overload, since the current NGN model will not support this NS/EP requirement. In order to robustly deploy NS/EP applications to either the public or private IP networks, new standard implementations will be needed to be developed that not only provide end-to-end priority and QoS, but also AAA, CAC, and security protection of both the users traffic and the network resources. NS/EP IP traffic must be given the highest priority to assure that NS/EP national leadership calls will receive end-to-end priority treatment over other users' calls.

4.2 Recommendations

The following is a list of the recommendations resulting from the Internet Priority Service RFI assessment effort. The recommendations provide guidance for the government to follow consistent with the goals expressed in the RFI. These goals include identifying the following areas in support of a future government IPS program: emerging technologies; candidate prototype and proof of concept projects; technologies to model; industry's program plans; candidate R&D projects; and new standardization efforts.

- **Develop Industry Requirements:** The NCS should promote establishing a consortium to develop industry requirements in support of IPS NS/EP missions, including end-to-end highest priority, unique marking of NS/EP traffic, and Inter-provider QoS and priority.

- **Develop Detailed Agency Requirements:** With the support of the Committee of Representatives (COR) the NCS should develop detailed agency requirements and specifications

for IPS NS/EP NGN VoIP service, and for other applications such as video, Web, email and messaging.

- **Drive Government R&D from Industry Requirements:** Industry requirements should drive the government R&D performed in support of IPS and NS/EP over the Internet. This will ensure that the government supports technology that industry is willing to adopt and implement.

- **GETS TDM Voice migration to VoIP**: The NCS should focus on GETS TDM Voice migration to VoIP as a first step to establish the architecture for supporting IPS.

- **Develop New Features:** There is a need to conduct additional studies of new features that can mitigate congestion and network outages. Moreover, these features need to be tested for applicability when networks are stressed at up to eight times normal load. It is important that NCS work with industry to identify the appropriate feature sets to implement.

- **Model Internet Traffic:** The NCS should understand and model the traffic engineering policies, peering policies, and congestion picture of the Internet today consistent with the architecture presented in this document. New COR requirements, industry requirements, and new standardized protocols (such as Inter-provider TE, priority and QoS) should be modeled in an anticipatory fashion.

- **Prototype a GETS migration:** The NCS should establish a program to prototype a GETS migration to VoIP that includes a limited number of nationwide and regional ISPs.

- **Develop Priority Mechanisms with Industry:** The NCS should continue to work with industry to develop priority mechanisms at the per packet level, as well as the per transaction level (e.g. email message, web session, voice call, or video session) to support a full range of NS/EP IPS applications.

- **Implement a Prototype Priority Mobile Broadband Data Project:** The NCS should implement a prototype project for priority mobile broadband data capabilities in the 3G Cellular networks in support of NS/EP communications for email, video, web, and messaging.

- **Understand Network Security:** With respect to NCS services like GETS, it is extremely important for the NCS to work with GETS providers and understand the approach the carriers are going to use to physically secure infrastructure that will carry NS/EP traffic. The Internet has security vulnerabilities that could affect the establishment of a GETS call on a converged network. The systems necessary to establish a GETS calls could have sensitive data accessible via the Internet and must be secured with the latest techniques.

- **Critical Infrastructure Protection:** The NCS should seek participation of the Critical Infrastructure Protection community in the industry requirements process. This will ensure that IPS solutions will be able to provide assured communications to other CI sectors, such as power and other industries, that rely heavily on communications technologies for control and operation (e.g., SCADA systems).

- **Standards Participation:** The NCS should continue to participate in standards community activities in partnership with industry (hardware vendors and Internet Service Providers) to develop an approach to deploy QoS technology ubiquitously across the Internet, in support of the 14 NS/EP functional requirements. The government should also participate in the ITU-T NGN architecture focus group later this year, which will likely morph into a formal study group.

5 Glossary

TERM	DEFINITION
1xRTT	One channel Radio Transmission Technology
3DES	Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AS	Autonomous System
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BGP4	Border Gateway Protocol 4
BMSS	Broadband Multimedia Satellite Systems
BWM	Bandwidth Manager
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Connection Admission Control
CAIDA	Cooperative Association for Internet Data Analysis
CAM	Content Addressable Memory
CASSE	Control and Soft-switch Element
CATV	Cable Television
CDMA	Code Division Multiple Access
CFS	Clustered File System

TERM	DEFINITION
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
COG	Continuity of Government
COPS	Common Open Policy Service Protocol
COR	Committee of Representatives
COS	Class of Service
CPS	Calling Party Category
CPE	Customer Premises Equipment
CTs	Class Types
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DHS	Department of Homeland Security
DID	Direct Inward Dialing
DiffServ	Differentiated Services
DISA	Defense Information Systems Agency
DNIS	Dialed Number Identification Service
DOCSIS	Data over Cable Service Interface Specification
DoD	Department of Defense
DoE	Department of Energy
DoS	Denial of Service
DREN	Defense Research Engineer Network
DRSN	Defense Red Switched Network
DS1	Circuit capacity of 1.5 Mbps
DSCP	Differentiated Services Codepoint
DSN	Defense Switched Network
DS-TE	Differentiated Services Aware Traffic Engineering
DWDM	Dense Wavelength Division Multiplexing
EF	Expedited Forwarding

TERM	DEFINITION
EFI&T	Engineer, Furnish, Install, and Test
EMSS	Enhanced Mobile Satellite Services
ETS	Emergency Telecommunications Services
EV-DO	Evolution Data Optimized
EXP	Experimental
FCC	Federal Communications Commission
FCP	Flow Control Platform
FEC	Forwarding Equivalence Class
GETS	Government Emergency Telecommunications Service
GigE	Gigabit Ethernet
GMPLS	Generalized MPLS
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IEPREP	IETF Internet Emergency Preparedness
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IMS	IP Multi-media Subsystem
IntServ	Integrated Services
IP COS	Internet Protocol Course Grained QoS
IPS	Internet Priority Service
IPSEC	IP Security Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISUP	ISDN User Part
ISP	Internet Service Provider
ITU	International Telecommunication Union

TERM	DEFINITION
JTRS	Joint Tactical Radio System
LDP	Label Distribution Protocol
LEC	Local Exchange Carrier
LLC	Logical Link Control
LLQ	Low Latency Queue
LSP	Label Switched Path
LUN	Logical Unit
MAM	Maximum Allocation Model
MAR	Maximum Allocation Resource
MGCP	Media Gateway Control Protocol
MIS	Mobile Internet Security
MLPP	Multi-Level Precedence and Premption
MPLS-FRR	Multi-Protocol Label Switching-Fast Reroute
MPLS-LSP	Multi-Protocol Label Switching-Label Switched Path
MPLS-TE	Multi-Protocol Label Switching-Traffic Engineering
NAT	Network Address Translation
NCD	Network Connection Device
NCS	National Communications System
NGN	Next Generation Network
NIST-ANDT	National Institute of Standards and Technology Advanced Network Technologies Division
NLR	National LambdaRail
NPRM	Notice of Proposed Rulemaking
NNI	Network to Network Interface
NS/EP	National Security/Emergency Preparedness
NSIS	Next Steps in Signaling
NSLP	NSIS Signaling Layer Protocol
NSP	Network Service Provider
OC-768	Optical Carrier Level 768

TERM	DEFINITION
OC-92	Optical Carrier Level 92
OIF UNI	Optical Internetworking Forum User Network Interface
OMNCS	Office of the Manager NCS
OSPF	Open Shortest Path First
PDP	Policy Distribution Point
PECAN	Policy Enabled Configuration Across Networks
PHB	Per-hop Forwarding Behaviors
PKI	Public Key Infrastructure
PNAP	Proprietary Network Access Points
PoP	Point of Presence
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
R&D	Research and Development
RFC	Request For Comments
RFI	Request For Information
RFP	Request for Proposal
RPF	Reverse Path Forwarding
RQ	Rivulet Queuing
RSA	A public key cryptosystem
RSVP	Resource Reservation Setup Protocol
RTP	Real Time Protocol
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SONET	Synchronous Optical Networks
SS7	Signaling System Number 7

TERM	DEFINITION
SSL	Secure Site Seal
T1A1	Technical Subcommittee T1A1: Performance, Reliability, and Signal Processing
TCP	Transport Control Protocol
TDM	Time Division Multiplex
TFT	Task Force Team
TLD	Top Level Domain
TMP	Transport Morphing Protocol
TOS	Type of Service
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UTRA-TDD	UMTS Terrestrial Radio Access – Time Division Duplex
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WARP	Web Assured Response Protocol
WCDMA	Wideband CDMA
WDM	Wavelength Division Multiplexing
WG	Working Group
WiFi	Wireless Fidelity
WMD	Weapons of Mass Destruction
WPS	Wireless Priority Service
xDSL	All types of Digital Subscriber Lines (DSLs)

Appendix A RFI: Internet Priority Service (IPS) Capability Design/Development

D -- Internet Priority Service (IPS) Capability Design / Development

Notice Date

11/21/2003

Notice Type

Solicitation Notice

Contracting Office

Defense Information Systems Agency, Acquisition Directorate, DITCO-Scott, 2300 East Drive Bldg 3600, Scott AFB, IL, 62225-5406

ZIP Code

62225-5406

Solicitation Number

Reference-Number-NCS-N2

Response Due

1/19/2004

Archive Date

12/12/2003

Point of Contact

Cornelius Hough, Contracting Officer, Phone 618-229-9768, Fax 618-229-9507 Lorraine Jones, Contract Specialist, Phone 618-229-9523, Fax 618-229-9507

E-Mail Address

hough1c@scott.disa.mil, jones2l@scott.disa.mil

Description

NATIONAL COMMUNICATIONS SYSTEM

INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION DIRECTORATE

DEPARTMENT OF HOMELAND SECURITY

INTERNET PRIORITY SERVICE (IPS)

REQUEST FOR INFORMATION

1. INTRODUCTION

1.1 Scope

The National Communications System (NCS) of the Department of Homeland Security is soliciting information regarding assured communications through the Internet. This information is with respect to services or products that carriers, vendors, and third parties can provide, or plan in the future to provide, applicable to designing/developing an Internet Priority Service (IPS) capability to support national security and emergency preparedness (NS/EP) communications. This request for information (RFI) seeks technical information regarding Internet-based assured communications for data, including Voice over Internet Protocol (VoIP). Responses from all organizations including commercial entities, academic institutions, and Government departments and agencies, are encouraged.

1.2 Background

Under the provisions of Executive Order 12472, the NCS is responsible for ensuring that an NS/EP telecommunications infrastructure exists and is responsive to the needs of the President and the Federal departments and agencies using public and private telecommunications systems. In support of this mission, we have initiated several programs designed to overcome network failure and congestion during emergency situations, including the Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS) to address priority services for Federal, State, and local Critical Infrastructure leadership personnel during an emergency. The current implementations of priority service for NS/EP telecommunications consist of voice and voice-band data only in the circuit switched wire-line and wireless networks. Due to the ever-increasing use of the Internet for transmission of all types of communications, we are looking at ways to provide similar types of assured communications for data applications and voice or video applications running over the Internet. Information learned from this RFI will be used to help NCS achieve the following goals:

- Identify plans and emerging technologies for providing priority services through the Internet.
- Accelerate promising technologies by prototyping and proof-of-concept projects.

- Promote industry wide adoption of these technologies through the industry standardization process

- Model technologies to determine what enhancements (if any) are required to meet the stringent NS/EP requirements.

- Enable the NCS's IPS to leverage and enhance future commercial priority service capabilities.

2. AREAS OF INTEREST

The following functional goals of an IPS concept should be considered:

- Enhanced Priority Treatment
- Secure Networks
- Ubiquitous Coverage
- International Connectivity
- Interoperable
- Scalable
- Bandwidth Mobility
- Voice Band Service
- Broadband Service
- Reliability/Availability
- Restorable
- Survivable
- Non-Traceable
- Affordable

Ultimately, the service should be resilient to large-scale outages of the Internet infrastructure in addition to outages of other infrastructures the Internet is dependent upon-such as electric power and telecommunications. It should also be resilient to cyber attacks originating within the Internet itself, such as denial of service, worms, etc. Solutions should have ubiquitous coverage in that they translate to various physical and link layer technologies, locations, applications, and network topologies. Specifically, we are looking for solutions that will provide end-to-end priority in inter-Autonomous Systems (AS) cross-provider environments, as well as within single provider networks.

To enable interoperability, we have IPS standards efforts underway; however, a lack of standards should not preclude a response--we are also interested in concepts and

implementations that may be proprietary in nature, and have not yet been standardized. Responders are encouraged to review the T1A1.2 committee's Roadmap Standards in Support of Emergency Telecommunications Service (***ETS***)? under the project T1A1-19 ?Reliability/Availability of IP-based Networks and Services,? whose concepts are reflected throughout this RFI. An IPS should have a large set of capabilities to potentially be of service during disaster recovery activities.

Since not all of the following features are currently available, responses are not expected to meet all of these criteria; however, IPS features and objectives could include the following:

- Multimedia and telephony services
- Rapid user authentication
- Security protection of user traffic
- Preferential access to telecomm facilities
- Preferential establishment of communications
- Preferential routing of traffic
- Preferential use of remaining operational resources
- Preferential completion of user traffic to destination
- Allowable degradation of service quality
- Interchange of critical telecomm service management information
- Optional preemption of non-emergency traffic (where permitted by regulation)

The objective is to provide priority service for Internet applications critical to essential personnel during a crisis. Preliminary analysis shows that numerous approaches are possible due to the design of the protocol model and state that makes up the Internet; however, prioritized delivery of individual packets at the lower layers of the Internet protocol model does not guarantee that transactions will gain priority processing on end systems and servers. Since any single protocol is likely to be insufficient to guarantee priority, several approaches may need to be combined to form an operational system. In addition to end-to-end solutions, we are interested in individual submissions that may consist of building blocks for an overall IPS architecture. Responses should address *how these building blocks fit within the traditional Internet model to eventually provide an end-to-end solution*. Specifically, the following areas should be addressed:

1. **Link Layer**. A large variety of layer 2 link level technologies are incorporated within the Internet. Enhancements applicable to priority services for High-speed optical backbone technologies such as SONET, Packet over SONET, MPLS, Gigabit Ethernet, DWDM, and ATM are of interest.

Also of interest are enhancements applicable to access technologies such as DSL, cable modem, and fixed wireless, in addition to priority within mobile wireless protocols such as messaging, 3G cellular data, and satellite data.

2. **Network Layer.** Internet Protocol (IP) makes up the entire network layer for the Internet. There are two versions of IP applicable to this RFI. IP Version 4 is the current protocol that operates the majority of the Internet. IP v6 will eventually replace IP v4, with superior addressing, security, priority and other features. We are interested in approaches that are applicable to either or both versions of IP.

3. **Transport Layer**. Protocols designed to assure data transmission end-to-end or hop-by-hop through the Internet often are considered transport layer enhancements. The IETF has standardized a number of approaches, so implementations of these are of interest to us. Additional concepts and proprietary implementations in this area are also of interest.

4. **Application Layer.** Applications control the Internet; as an example BGP and DNS are applications that are considered core infrastructure pieces of the Internet. Applications also make up the services that utilize the Internet. Of interest are application enhancements that will lead to one or more of the fourteen functional goals for an assured IPS. Applications of particular interest include (but are not limited to) email, messaging, web, VoIP, (transport and edge), and video.

5. **Standards and APIs.** We are also interested in standards or APIs that have been developed in these areas, whether or not implemented in products or services.

3. RESPONSE GUIDELINES

3.1 Scope

Most organizations do not have expertise or capabilities in all of the areas described above; therefore, *responses addressing only a subset of or single identified area(s) of interest are also welcome*. Responses should be *clearly labeled* with the areas of interest that are discussed. Length of responses should *be limited to no more than 40 pages.*

3.2 Structure

Provide any materials, suggestions, and discussion you deem appropriate. In addition, please provide ample contact information, including telephone numbers and e-mail addresses, to facilitate any needed clarification or further discussion. Include, as appropriate, the following:

- Description of Products/Technologies/Research/Standards/APIs, including performance information
- Plans for commercial use of these technologies
- Corporate partners who will use the technology
- Feasibility Assessment

- Cost and Schedule Estimates
- Existing Government Contracts
- Corporate Expertise

3.3 Format

Electronic and hard copy formats are both acceptable, although electronic submission is preferred. If provided electronically, submissions should be in a Microsoft Office compatible format or Adobe Acrobat. Copies may be emailed to Mr. Dave Nolan at noland@ncs.gov or mailed to the address below.

3.4 Deadline

Responses are due 60 days after release of this RFI.

4. DISCLAIMER

There is no bid package or solicitation document associated with this announcement. The requested information is for planning purposes and does not constitute a commitment, implied or otherwise, that a procurement action will be issued or a contract awarded. No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of the submission of information. Responses to the RFI will not be returned. The Government shall not be liable for or suffer any consequential damages for any improperly identified proprietary information. Proprietary information will be safeguarded in accordance with the applicable Government regulations. In accordance with FAR 15.202(e), responses to this notice are not an offer and cannot be accepted by the Government to form a binding contract.

Responders are solely responsible for all expenses associated with responding to this RFI.

5. CONTACT INFORMATION

Mr. David J. Nolan NCS/N2 701 South Court House Road Arlington, VA 22204-2198 (703) 607-6190 noland@ncs.gov

Place of Performance

Address: NCS/N2, 701 South Court House Road, Arlington, VA

Zip Code: 22204-2198

Country: USA

Record

SN00474736-W 20031123/031121225532 (fbodaily.com)

Source

FedBizOpps.gov Link to This Notice

Appendix B Technology Assessments

This appendix provides an IPS emerging technology assessment based on information gleaned from the responses as well as technical information received and examined during the writing of this report. IP security technology is also discussed.

1 Converged Network Technologies

This section discusses the major technologies making up the four protocol layers illustrated in Figure 1.1. It discusses the current and evolving technologies for each of the layers, and provides an overview of how RFI respondents addressed the emerging technologies in their RFI responses. Appendix C provides a more detailed discussion of the emerging technologies for readers who are less familiar with network convergence as discussed in this report.

1.1 Transport Layer

The transport layer encompasses the physical and link layers of the TCP/IP protocol model. This section discusses the major technologies associated with the transport layer having the greatest impact on IPS. Many protocols make up the transport layer, as shown in Figure 1.1. Many of the transport technologies have sub-components that reside in other layers of the protocol model. For example, MPLS is a layer 2.5 technology that binds the IP layer to lower physical layers. It also has significant related component protocols operating at the control layer in the protocol model. These sub-component parts are discussed appropriately in the network, control, or service layer sub-sections of this report.

1.1.1 Multi-Protocol Label Switching (MPLS)

MPLS defines a mechanism for packet forwarding in network routers. It was originally developed to provide faster packet forwarding than traditional IP routing, although improvements in router hardware have reduced the importance of speed in packet forwarding. However, the flexibility of MPLS has led to it becoming the default way for modern networks to achieve traffic engineering, Quality of Service (QoS), next generation VPN services, multi-service networking and optical signaling.

Most of the carriers that responded to the RFI have deployed MPLS into their networks making it an important technology for IPS. MPLS has been integrated into their networks to achieve QoS through the underlying layer capabilities such as Asynchronous Transfer Mode Class of Service QoS (ATM COS) or Ethernet 802.1Q, as well as through Differentiated Services Aware Traffic Engineering (DS-TE). Moreover, respondents claim that increased reliability is obtained with MPLS via such things as MPLS fast-reroute and MPLS traffic engineering extensions. Also, MPLS VPNs are able to meet security requirements of certain users by limiting outside connectivity to designated entry points within a network. MPLS technology continues to evolve to provide improved QoS, traffic engineering, and management

functions, as carriers purchase newer router hardware to support newer protocol features such as DS-TE and Multi-Protocol Label Switching-Traffic Engineering MPLS-TE.

Over ten RFI respondents addressed MPLS as a major enabling technology of an IPS. Although a promising and substantial technology, some respondents expressed reservation or concern that MPLS alone may not be able to address the full range of requirements for a converged Internet. MPLS may not contain all of the architectural primitives to meet the reliability and QoS concerns of multi-service networks.

1.1.2 Gigabit Ethernet (GigE)

A number of RFI respondents indicated that Gigabit Ethernet is being widely deployed in Internet exchange points, Metro Fiber networks and campus networks due to its simple architecture and the wide availability of low-cost GigE layer 3 switches. One of the features with applicability to IPS is its ability to provide Class of Service through the use of the 802.1Q VLAN tag header, which provides marking for eight levels of priority. However, current standards and implementations are not adequately developed to translate IP COS (DiffServ) markings to Ethernet priority markings, although there are some methods to manage policy through hardware vendor specific proprietary management applications.

1.1.3 ATM

ATM is currently implemented to provide high bandwidth service for public carriers and is normally deployed in conjunction with a Layer 1 SONET infrastructure. ATM is a feature rich technology offering many different services, but other technologies such as Dense Wave Division Multiplexing (DWDM), MPLS, and GigE are slowly replacing it. ATM has wide support by ANSI and the ITU for carrying a complete range of user traffic for voice, video and data for any type of physical media. ATM scalability is limited, however, due to the high cost of chip sets and limited number of implementations that can exceed OC-192 speeds, as IP device requirements move toward operating at speeds to OC-768.

The IETF has defined a suite of protocols for carrying IP traffic over ATM. These standards not only address delivery of best effort traffic, but also standardize the use of RSVP to signal IP application requirements to the ATM infrastructure to allocate QoS resources. This is known as ATM and RSVP interworking function. Several RFI responders indicated that they plan to continue to use ATM CoS as a means to deliver real-time traffic, although it was not clear whether RSVP would be the signaling method. In addition, they indicated that ATM is still deployed at the edges of their networks. However, new technologies such as DWDM, MPLS and GigE will more tightly integrate network management and provide higher performance for lower cost than ATM is capable.

1.1.4 Lambda Networking-Dense Wave Division Multiplexing (DWDM)

Lambda Networking, also known as Wave Division Multiplexing (WDM) allows for multiple communication channels over a single fiber by using different frequencies of light for each channel. This is significant in that, in the past a single fiber could only transport a single

"carrier", such as Synchronous Digital Hierarchy (SDH) or Synchronous Optical Networking (SONET). Therefore, WDM has the ability to transport multiple SDH/SONET carriers over on fiber, thus increasing the existing fiber infrastructure by orders of magnitude.

Lambda Networking is quickly becoming the transport mechanism of choice by the WAN telecommunications carriers as well as government agencies and academic organizations. Many telecommunication companies offer WDM connectivity between their Points of Presence (PoPs).

Many National and International telecommunication companies, most notably Qwest and Level3, are providing Lambda networking as a commodity service. Moreover, Lambda networking is being used extensively throughout the High Performance Research and Education Networks like the National LambdaRail (NLR), as well as for international connectivity with the Netherland's SURFnet and Canada's Canarie network.

Although Lambda networking is not strictly an Internet technology, as it operates at the lower layers of the protocol model, it will have an impact on IPS due to integrated IP management through the Optical Internet Forum (OIF) User Network Interface (UNI) and Generalized MPLS (GMPLS). In general, these technologies greatly increase the bandwidth and reliability of lower layer transport that can be made available to IP routers. These protocols are based on IP, and they are able to control a Lambda network, provide automatic path provisioning, and affect rerouting as failures occur. In December 2001, the OIF approved UNI 1.0, enabling client devices to establish optical connections dynamically within seconds through GMPLS signaling. Most of the carriers that responded to the RFI indicated that DWDM was a major element of their emerging architectures, and a variety of the respondents in other business types (integrators/consultants/engineers) indicated that emerging technologies in the DWDM area would make networks much more reliable and bandwidth more plentiful.

1.1.5 Mobile Wireless

Third generation cellular mobile data services provide a packet based connectionless service over cellular networks instead of connection oriented dial-up like services of older generation cellular networks. This is an important technology for IPS, as it provides mobile broadband wireless technologies ubiquitously through the cellular networks.

Third generation technologies include GPRS (General Packet Radio Service), which is part of the ITU GSM standard, and 1xRTT and EV-DO, which are part of the CDMA 2000 standard. Major providers of CDMA 2000 are Verizon Wireless, Sprint, and Alltel. Major GSM providers include AT&T, T-Mobile, and Cingular. QoS standards necessary to meet IPS requirements are under development in the 3GPP2 for CDMA2000, and in the ITU for GSM. One RFI responder indicated CDMA2000 1xRTT is available through a broad portion of the US market through two different carriers. Additionally, EV-DO is emerging in the metropolitan markets. One respondent also provided information regarding mobile data services using WCDMA and deploying onto new spectrum allocations.

1.1.6 MPLS VPNs (Layer 2.5: Transport and Network Layer)

Layer 2 and Layer 3 are used to isolate logical networks from other logical networks on a per router hop basis. In a Layer2 VPN, there is no routing (Layer3) information contained in the intermediate router hops. This gives a true Layer3 isolation on all intermediate routers (e.g. no route lookup to forward packets). A Layer3 VPN provides logical separation of networks via "virtual routing tables" kept local on each router. This means each router performs a route look up and based on the virtual routing table attaches a label on the packet for forwarding. Each intermediate router may have many virtual routing tables for multiple VPNs. Several RFI respondents proposed implementing VPNs as a method to provide security protection of the user traffic and systems and/or to provide bandwidth guarantees.

1.2 Network (IP) Layer

There are three Network technologies discussed in this section-IPv4, IPv6, and Mobile IP. The IPv4 protocol has supported the scaling of the Internet to its current global proportions. However, because of a number of IPv4's limitations, IPv6 is envisioned to be its successor, mitigating a number of its shortcomings. Mobile IP promises to provide ubiquitous connectivity to the mobile user, independent of the devices and access technologies.

1.2.1 IP version 4 (IPv4)

IPv4, the current version of the IP deployed worldwide, has proven remarkably robust, easy to implement, and interoperable with a wide range of protocols and applications. Though substantially unchanged since it was first specified in the early 1980s, IPv4 has supported the scaling of the Internet to its current global proportions and is used in most IP-based networks today.

Most RFI respondents stated that, in the near term, IPv4 was sufficient to base an IPS solution upon despite its shortcomings. However, IPv4 is proving inadequate for supporting the increasing use of the Internet for multimedia communications including real-time voice and video, as well as the increasing number of networked devices. The most obvious limitation of IPv4 is its address field (32 bits), which limits the number of unique devices that can be addressed on the Internet. With the proliferation of networked devices including PCs, cell phones, wireless devices, etc., unique IP addresses are becoming scarce, and the Internet is theoretically running out of IP addresses. Although Network Address Translation (NAT) methods are used to overcome the shortage of unique IPv4 addresses, end-to-end Internet model and implementation of IPSEC between end-hosts is sacrificed. NAT implementations do not support H.323 protocols, as changes to the IP header resulting in a mismatch that prohibits control of calls. One vendor suggested using a firewall to guard against intruders, but the firewall should not provide NAT functions for VoIP packets unless it is Q.931 friendly.

1.2.2 IP version 6 (IPv6)

IPv6, the successor to IPv4, retains many of the features of IPv4, includes a transition mechanism designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion, and provide direct interoperability between IPv4 and IPv6 hosts. IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and at the same time still

be efficient for low bandwidth networks (e.g. wireless). In addition, it provides a platform for new Internet functionality that will be required in networks offering IPS. For example, Flow labeling capability has been added to enable the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default QoS or real-time service. However, the IPv6 Flow Label is still experimental and several RFI respondents identified this as an area of additional research to identify possible uses of the Flow Label to improve the Internet's support for real-time communications. IPv6 also natively offers improved security features with support for authentication and privacy, a much-needed feature in an IP packet environment.

Although most of the RFI responses were IPv4 centric, much of the information received emphasized a general consensus that IPv6 was slowly but steadily being deployed, and that any deployment of an IPS would eventually have to address migration and adoption of the new IPv6 standard.

1.2.3 Mobile IP (MIP)

Mobile IP (MIP) is an extension to IP designed to allow portable (mobile) computers to move from one network to another and is an integral component of a 3G Cellular data networks. When mobile data users roam between carriers and different sections of the infrastructure, MIP allows seamless mobility, permitting applications such as email and web to operate without the need for reconfiguration or session re-establishment. Mobile IP is viewed as a significant component of a future IPS design by several of the RFI respondents. With MIP, users are able to meet the mobility (and also broadband) requirements of NS/EP through connection to a broadband mobile wireless carrier such as UMTS, CDMA2000 or WCDMA.

1.3 Control Layer

Much of the reliability in the Internet is provided through fault tolerant designs within the control layer, and within the transport layer. The control layer is designed such that limited outages and non-availability of components does not adversely affect connectivity. However, the reliability of the Internet, being a best effort network, does not have the same reliability standards as the PSTN. A range of factors, including malicious hacking, operator error, and physical outages, can exploit numerous vulnerabilities within layers. Generally, when these events occur, performance or QoS suffers because of congestion, although connectivity is usually still maintained. Congestion can be attributed to additional network loading brought about by additional traffic either generated by worms or viruses, or by alternate routing of traffic due to an outage.

QoS is a growing requirement within the Internet today, as more and more mission critical applications are using the Internet. There are a range of requirements that different types of applications have for the Internet, nominally defined by packet loss, delay, throughput, and jitter. Different QoS requirements are competing for network resources. QoS is a major requirement for migrating TDM voice to VoIP. Two IETF control protocols provide QoS in an IP network environment: Differentiated Services (DiffServ) and Integrated Services (IntServ). NS/EP traffic

must have end-to-end priority treatment over all traffic and must be uniquely recognized by the network.

In this section, the control layer technologies discussed are those limited to network and transport layer control functions. Application control functions are considered service layer functions.

1.3.1 MPLS Control

MPLS-Label Distributing Protocol (LDP) is the basic control protocol used to establish a Label Switched Path (LSP) within an MPLS domain where traffic engineering is not required. Without traffic engineering (TE), LSP setup follows the shortest path based on hop count and routing metrics only. Traffic engineering is the process of distributing load among elements of the network to reduce congestion and more evenly utilize resources of the network. Traffic can be identified, and placed onto a separate LSP based on Forwarding Equivalence Class (FEC). More advanced MPLS deployments use MPLS-TE to signal resource requirements to the MPLS network during the setup of LSPs. Another advanced feature of MPLS is Fast Reroute (FRR), which involves setting up backup LSPs to re-route traffic when failures occur. MPLS fast-reroute is able to meet SONET like rerouting times (say 50 milliseconds). Support for Differentiated Services (DS) within MPLS is a key capability for providing a more capable QoS capability within the Internet and for providing IPS. Most carriers indicated they are deploying MPLS-TE and MPLS-FRR at this time.

1.3.2 Differentiated Services (DiffServ)

DiffServ defines a set of code points for marking traffic and prioritizing on a hop-by-hop basis. Two sets of Per-hop Forwarding Behaviors (PHB) have been defined under DiffServ, primarily used to differentiate between voice and data. DiffServ is valuable on the edge of the network where upgrade of circuit capacity is not cost effective. Respondents said that DiffServ is not deployed heavily in the core of IP networks where over provisioning is the key means to help mitigate congestion.

Deploying DiffServ has significant security concerns since it requires implementing filtering and re-marking of traffic to ensure that forged priority traffic is not able to overload queues and effect the QoS of priority traffic.

DiffServ within an MPLS network is key feature to providing a QoS enabled Internet. Whereby MPLS tunnels are able to support basic prioritization, DiffServ-aware Traffic Engineering (DS-TE) is able to enforce different bandwidth constraints for different sets of Traffic Trunks. By mapping the traffic from a given Diff-Serv class-of-service on a separate LSP, it allows this traffic to utilize resources available to the given class on both shortest paths and non-shortest paths and follow the path that meets engineering constraints (cost, performance, reliability) specific to a given class. Another technique, DS-TE Maximum Allocation Resources (MAR), is the most effective way to reduce packet loss where there is severe congestion. DS-TE is of benefit for networks where bandwidth is scarce, and there are significant amounts of delay sensitive traffic or non-uniform proportions of traffic across the supported classes-of-service.

DS-TE MAR is an emerging capability appearing in the latest router implementations. Carriers will soon be deploying this, as it is in draft standard status with the IETF.

There is some general agreement that these DiffServ techniques alone may meet the more stringent NS/EP requirements to be able to operate in a severely degraded network environment where 10x overload could occur. This is due to the Class of Service (CoS) nature of DiffServ, where traffic class aggregates are assigned to queues.

If a traffic aggregate should exceed its assigned bandwidth (queue capacity) due to network disruption or system overload, that classes' QoS could suffer if there are not spare resources to allocate from other traffic classes. This problem bears much further study, as carriers are firmly committed to DiffServ, and have no other option for providing QoS and priority in the NGN.

NS/EP traffic should be assigned its own traffic class with the MAR model so that it does not compete with other traffic. An NS/EP requirement is that in the event of a crisis, NS/EP national leadership calls must receive end-to-end priority treatment over other users' calls.

Inter-AS MPLS-TE is the next step in the evolution of QoS and TE. With an Inter-AS capability, ISPs would be able to support more granular TE, rerouting, and bandwidth guarantees within LSPs that traverse more than one AS. This is a key component of providing a priority services enabled Internet.

1.3.3 Integrated Services (IntServ)

Integrated Services (IntServ) is implemented in the current generation of Internet routers and hosts but there are significant limitations to the applicability to an IPS. These limitations are with respect to the number of flows classified, the number of queues that can be serviced or scheduled, and the number of messages that are processed. Technical discussions with RFI respondents indicated that in an IPS architecture, it is expected that RSVP capable routers will occur only at the edge of the network where interface speeds are DS1 or lower and the number of RSVP messages is limited. Scaling of IntServ to an Internet wide configuration supported on every router hop is unlikely due to the sheer number of individual flows that would have to be signaled and processed in queues in the core of the network.

However, IntServ may be a QoS technique that is able to support stricter NS/EP requirements to operate in severely degraded network conditions, up to 10x overload. Some respondents indicated a hybrid approach where only certain nodes in key congested locations support IntServ. This is supported within the IntServ model and will likely be deployed to support Internet telephony. DiffServ will be used in addition to IntServ in core routers where large numbers of flows do not permit the deployment of IntServ. NS/EP calls could be identified for priority treatment to Intserv through the SIP Resource priority header. Calls with this priority marking could then be given priority for completion when congestion occurs in the network.

The Multiswitch Forum is developing verification routines to be used at their interoperability event. These validate Softswitch products incorporating the use of the Integrated Services architecture, including COPS policy enforcement, and RSVP signaling.

1.3.4 Resource Reservation Protocol (RSVP)

RSVP is used with a variety of QoS control services. Because QoS control services are designed to be used with a variety of setup mechanisms, RSVP is primarily used for setting up MPLS Traffic engineered flows and for setting up Integrated Services (RFC 2205) per session microflows. RSVP also has optical extensions to include the ability to signal optical wavelengths and shared risk link groups, as well as bandwidth, latency and other link characteristics. RSVP will be an integral part of an IPS since it is the Internet's QoS signaling protocol.

1.3.5 Common Open Policy Service (COPS)

Common Open Policy Service (COPS) is a simple client/server model for supporting policy control over QoS signaling protocols, primarily RSVP. COPS is integrated into many devices that support RSVP, including routers and end-hosts running Session Initiation Protocol (SIP) or H.323 VoIP applications. COPS will be an integral component of IPS, as it is necessary for any fine-grained connection admission control. A unique component that represents NS/EP traffic will be necessary.

1.4 Applications Service Layer

As part of Internet Priority Service, Internet applications such as Instant Messaging (IM), Session Initiation Protocol (SIP), Domain Name Service (DNS), voice over Internet protocol (VoIP), email, web, videoconferencing, and Short Message Service (SMS) can be used in support of the NS/EP community. This section provides of brief overview of the service layer technologies that were addressed by the RFI respondents.

1.4.1 Instant Messaging (IM)

There are many different implementations of IM; hence, interoperability is a problem. In particular, IM servers do not interoperate with one another and IM client software only works with its own IM servers. To resolve the client software issue, one respondent suggested that a web-browser interface should be used to access IM servers. A side benefit to using a web interface is that Secure Socket Layer security can be used to protect NS/EP traffic. Since IM traffic is not encrypted, another respondent offers a product that can manage and control IM traffic in a secure manner.

1.4.2 EmailATM

Although prioritized email is not discussed in the RFI responses, it is technically available in most email implementations. Users can simply set a flag in the email header, which contains an X-priority field. The NCS should consider working with standards organizations to get a unique value in X-Priority field for NS/EP users.

1.4.3 SIMPLE

The IETF has specified a set of extensions to SIP for presence and instant messaging. These extensions, known collectively as SIMPLE, have become widely adopted across the industry as

the mechanism for enabling interoperable presence and IM. It has been strongly embraced by the wireless industry, as evidenced by its adoption by the 3GPP and 3GPP2 standards bodies. Several of the Push to Talk (PTT) applications deployed today make use of SIMPLE in order to add presence capabilities.

1.4.4 WEB

For web applications, websites can be accessed though IPSec VPN tunnels or SSL methods. To improve service availability, web cache technology could be implemented.

1.4.5 Domain Name Service Security (DNS-SEC)

DNS-SEC could be used to support origin data authentication and data integrity of DNS traffic, but it is not commercially deployed. Some ISPs feel that DNS-SEC might cause additional traffic-related stress to the Internet. In addition, legacy equipment cannot currently support it. However, DNS-SEC should be deployed to protect critical Internet traffic, including NS/EP from hackers.

1.4.6 Voice over IP (VoIP)

There are many VoIP responses from the RFI. VoIP can use the following three main approaches: H.323, Session Initiated Protocol (SIP), and Media Gateway Control Protocol (MGCP). These protocols run on top of Real Time Protocol (RTP)/User Datagram Protocol (UDP)/Internet Protocol (IP). Media Gateways are required to interface these protocols. Currently, QoS for VoIP is not adequate in the public Internet, but many ISPs offer enhanced QoS through their own private networks at extra cost. Interoperability for VoIP is still a problem since different telephone service providers have their own ways of implementing VoIP. In order to provide preferential treatment for NS/EP traffic, appropriate markings are required, either at the IP level or application level, depending on the nature of an application.

A detailed assessment of VoIP technologies is beyond the scope of this document. Interested readers should consult the "*National Security/Emergency Preparedness (NS/EP) Voice Over Internet Protocol (VoIP) Telephony Planning for Carriers*" White Paper that was prepared by the Government Emergency Telecommunications Service (GETS) Program Management Office in response to a request for general planning information for use by GETS carriers.

1.4.7 Short Message Service (SMS)

SMS depends upon SS7 networking for transporting short text messages. SS7 is a narrow-band signaling network. The PSTN may be impacted if the SS7 network fails due to over-subscription of SMS users. An appropriate provisioning of SS7 traffic use and access control of SMS users is needed to ensure the operation of the SS7 network.

Most RFI responses were proprietary services/applications either already implemented/ deployed or still in research. Because there are no consistent standard implementations of these applications to support IPS, interoperability is a main problem. As a result, ubiquitous service coverage for the NS/EP community will be difficult to achieve.

2 Security Technologies

In the PSTN, different networks support the call set up (i.e. the Signaling System 7 network) and bearer channels. Conversely, on the Internet all management and control protocols use the same communication path as the actual data traffic. These two differing control philosophies, in-band signaling vs. out-of-band signaling, makes converging these two networks onto a common infrastructure very challenging. One of these challenges is security. Service providers recognize the vulnerabilities and have established policies, procedures and design approaches to safe guard the access to the communication infrastructure.

Many of the protocols that control the NGN have in-band signaling and are potentially vulnerable to Distributed Denial of Service (DDoS), malicious hacking, viruses and worms. These protocols can be secured to some extent with built in authentication, and access control filters as well as separate VPN just for the management and control of the network resources. In some devices, network control traffic is given highest priority so that in the event of severely degraded network conditions, this traffic will be given highest priority. BGP, LDP, RSVP, can all be secured with MD5 authentication. To address the security concerns of in-band signaling, several proposals suggest building a new out-of-band control network for the IPS. However, duplicating the diversity of the in-band network will be difficult and expensive.

Another security concern is the vulnerability of DiffServe to DoS attacks whereby router priority queues are overloaded with forged priority traffic. An attack of this type could affect the QoS of NS/EP voice traffic, causing these services to fail. Appropriate filtering and re-marking must be implemented on the edge of the network to protect DiffServ resources.

The most significant security concerns addressed in many of the RFI responses included Distributed Denial of Service (DDoS) attacks, call interception, signal protocol tampering, presence theft (impersonation), toll fraud, and call handling by commercial operating systems such as Windows and Linux. A review of RFI responses indicated that newer technologies are available in addition to using standard user ID and passwords. Two of the technologies discussed by the vendors are:

- RADIUS/AAA providing authentication, authorization, and accounting, and
- RSA Secure ID using a two-part authentication and authorization such as a PIN and an authenticator.

The implementation of IPS will use many emerging technology components, all subject to attack. The primary drivers for IPS security can be categorized into three areas: confidentiality, integrity, and availability. IPS confidentially addresses a hacker's ability to eavesdrop on data streams, determine the origin or destination of user traffic, and the ability to learn about the overall network infrastructure. Integrity of information addresses concerns about caller identity, authentication of devices to prevent rouge devices impersonating applications, and altering traffic. Availability deals with the ability to resist malicious attempts on the network to cause resets or mitigate attempts to cause denial of service to users. Many already well-known IP

security vulnerabilities can adversely impact the IPS and need to be assessed and mitigated. Today, IPS has serious security risk as well as deployment risk for the following reasons:

- IPS inherits all the problems of typical IP best-effort data applications.
- User demand for IP real-time services place great demands on network quality.
- Many regulatory issues complicate IPS acceptance and deployment.
- Changes in standards make selection of emerging technologies difficult.

Some systems use both these techniques together to protect their systems. One concern that needs to be addressed by the government is what policy should be set-up if users loose their authenticator.

Recently the National Institute of Standards (NIST) published a draft report on recommendations for security considerations for VoIP Systems (Special Publication 800-58). Recognizing that VoIP is one of the most important emerging trends in telecommunications, the publication explains the challenges of VoIP security for agency and commercial users of VoIP. The report outlines steps needed to help secure an organizations VoIP network. VoIP security considerations for the PSTN are largely outside the scope of the report, however, and there may be a need for the NCS to play a greater role in examining IPS emerging technologies through extensive IPS security R&D efforts to provide NS/EP assured services using the PSTN network resources that support the NCS mission. Although VoIP can provide more flexibility at lower cost, today VoIP managed networks are more vulnerable than conventional telephony systems. Because of the integration of voice and data in a single network, maintaining a secure VoIP and data network will be a complex process requiring greater effort than that required for data-only networks. Moreover, privacy and confidentiality will be at greater risk in VoIP systems unless strong controls are implemented and maintained.