THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Network Security/Vulnerability Assessments TASK FORCE REPORT

March 2002

TABLE OF CONTENTS

APPENDIX E: LEGISLATIVE AND REGULATORY TASK FORCE REPORT

Executive Summary

At the National Security Telecommunications Advisory Committee (NSTAC) XXIV meeting, Mr. Richard Clarke, then National Coordinator for Security, Infrastructure Protection, and Counterterrorism,[1] requested the NSTAC's continued assistance in assessing and responding to cyber attacks, particularly distributed denial of service (DDoS) attacks, which could impact national security and emergency preparedness (NS/EP) communications in the converged network environment. Responding to Mr. Clarke's request, the NSTAC subsequently tasked the Network Security and Vulnerability Assessments Task Force (NS/VATF) to assess the policy and technical issues related to the evolving public network (PN) supporting NS/EP communications for—

1. Network disruptions, particularly DDoS attacks
2. Security and vulnerability of the converged network control space, including wireless, network simulation and testing, standards and consequence management issues
3. Needed countermeasures (e.g., functional requirements) to address 1 and 2 above.

The September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon renewed concerns regarding physical threats to the PN. While to date the telecommunications infrastructure has not been a direct target of terrorism, it could be in the future. Therefore, it is important that Federal, State, and local government assistance related to preventing, mitigating, and responding to such an occurrence be coordinated through the Telecommunications Information Sharing and Analysis Center (Telecom-ISAC). In addition to the enduring physical threat to the Nation's networks, cyber attacks present a growing threat to the security of U.S. information systems and consequently critical communications of the NS/EP community. As cyber network attack techniques increase in sophistication and intruders continue using DDoS techniques to exploit vulnerabilities, cyber attacks will likely cause greater collateral impacts to NS/EP communications. Because of this environment, industry and Government are focusing their efforts through participation in ISACs to further develop and implement unified and centralized capabilities to identify and mitigate the effects of an attack as it is occurring.

In 2001, the NSTAC Convergence Task Force noted many control space vulnerability

issues related to convergence and the Next Generation Network (NGN) that could impact NS/EP communications. The NS/VATF remains concerned about the security of the control space of the evolving PN and believes additional steps are needed to enhance its security. As network convergence continues, malicious attacks focusing on the network control space are increasingly likely. Because of this volatile environment, the NS/VATF believes industry and Government cooperation is necessary to address control space vulnerabilities and implement remedial tools, including the Internet Protocol Security set of solutions. Furthermore, industry and Government should support the Network Security and Information Exchanges' efforts to develop a cross-industry security posture that could help provide a foundation for protecting the control space of the emerging PN.

The NS/VATF is also concerned about security issues involving wireless protocols and systems, including the wireless application protocol (WAP), wireless local area networks (WLAN), and personal area networks (PAN), when related to NS/EP communications transiting wireless networks and technologies. Accordingly, the NS/VATF recommends that the Government work with standards bodies to ensure consideration of NS/EP communications functional requirements during work addressing the security of the interoperation of wireless and wireline networks and, more specifically, activities addressing WAP. The task force also recommends that the Government deploy WLANs with higher levels of security and consider policies that would allow for PAN devices and yet reduce their risk of compromise.

On the basis of our analysis, the NS/VATF believes some of the best strategies for countering vulnerabilities of the critical telecommunications infrastructure involve—

- Increasing emphasis on, and providing adequate support of, Government participation in standards bodies as well as instituting a coordinated Government approach to standards development

- Specifying security standards elements in contracts and purchase orders to help establish the market. This process would result in more commercial off-the-shelf products and services, which the Government can then procure at reduced cost

- Increasing stakeholder awareness of cyber vulnerabilities and mitigation strategies, including strong cyber security and response plans.

In addition, based on the NSTAC Legislative and Regulatory Task Force report, the NS/VATF concludes that the legal issues underlying the provision of NS/EP priority

services to the Federal Government in an NGN environment are extremely complex and may require further study in response to any proposed legislation or regulation. However, until the standards for packet-based services are established, including provisions for the Emergency Telecommunications Service, and the Government's requirements in the evolving environment are certain, new legislation or regulation is premature.

The NS/VATF then concludes that the PN and its services supporting NS/EP users will continue to be at risk from those seeking to exploit known vulnerabilities by operating in an increasingly technologically sophisticated, well-coordinated manner. Given these factors, industry and Government must continue to work together to devise countermeasures and strategies that would mitigate the impacts of physical and cyber attacks on the PN and other critical infrastructures. Automated rather than manual responses to such attacks would expedite the capability to respond.

Recommendations 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,* and Executive Order 13231, *Critical Infrastructure Protection in the Information Age,* direct the appropriate departments and agencies, in coordination with industry to—

- Coordinate and prioritize through the Telecommunications Information Sharing and Analysis Center, Government assistance to industry to protect the Nation's critical communications assets and to mitigate the effects of an attack as it is occurring

- Encourage and adequately support the development and adoption of baseline standards and technologies including Internet Protocol version 6, Internet Protocol Security, and the Emergency Telecommunications Service scheme, to help bolster core security and reliability of the Next Generation Network

- Support the Network Security and Information Exchanges' efforts to develop a cross-industry security posture that could help provide a foundation for containing the control space of the emerging public network

- Work with standards bodies to ensure consideration of NS/EP communications functional requirements while addressing the security of the interoperation of wireless and wireline networks, and more specifically, activities addressing wireless application protocol

• Ensure that all wireless local area networks used by the Government meet the highest level of security standards available, with priority given to those supporting NS/EP missions

• Develop policies and procedures to support the use of personal area network devices while reducing their risk of compromise.

Definitions

The **PN** is any switching system or voice, data, or video transmission system that is used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks). (The Network Security Information Exchanges, *An Assessment of the Risk to the Security of Public Networks*, National Communications System, Washington, DC, December 12, 1995).

A **widespread outage** is a sustained interruption of telecommunications service that will have strategic significance to Government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country, including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day. (Report on the *Likelihood of a Widespread Telecommunications Outage*, The President's National Security Telecommunications Advisory Committee, December 1997).

Introduction

President George W. Bush's Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, states that the policy of the United States is:

…to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible.[2]

Such protection for the telecommunications sector is essential as more critical communications and data services are now carried over the evolving public network (PN). In fact, national security and emergency preparedness (NS/EP) operations and communications are heavily reliant on, and often inseparable from, the evolving PN, which today increasingly consists of converged information systems networks of traditional circuit switched networks interoperating with broadband packet-based Internet Protocol (IP) networks, including the Internet. In addition, because of the interconnectivity of critical infrastructures, the impact of a widespread outage in the telecommunications sector could ripple through other critical infrastructure operations, such as banking and finance activities. Therefore, an attack on the PN, whether physical or cyber, could have dramatic and detrimental

effects on national security (including national economic security). To understand how this might be possible, it is necessary to examine recent network "events" and their consequences; studying these events could also help predict future attack methods and suggest possible policy actions that could help mitigate vulnerabilities. Recent network events have made it clear that four critical factors are affecting the security and reliability of networks and network services today:

- Difficulty experienced by network managers in tracking their network topology
- Software product features inadequate for the effective control of user access and authentication
- Inadequate administrative practices and procedures for using the available features
- Lack of complete and effective project management processes for tracking and applying available software patches for known vulnerabilities.

Definition

The NGN is a public, broadband, diverse, and scalable packet-based network evolving from the public switched telephone network (PSTN), Advanced Intelligent Network (AIN), and Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence. (NSTAC *Convergence Task Force Report*, June 2001)

Because of these factors, the PN and its services supporting NS/EP users will continue to be at risk from those seeking to exploit known vulnerabilities by operating in an increasingly technologically sophisticated, well-coordinated manner.

Although alternative network architectures and approaches have been developed to address network security issues, with designs ranging from commercial and Government systems that are connected in varying levels to the Internet to dedicated minimum essential networks not connected to the Internet, few networks are truly private or dedicated. Alternative network architectures and approaches seek to enhance reliability and availability of NS/EP communications by condensing security and management into smaller, more controllable components. Despite the benefits of using such dedicated networks, many NS/EP activities today are supported by the PN because of the network's ability to reliably offer "just in time" affordable connections with suppliers, customers, and the general public. Because the PN has become vital for the continuity of business, this study focuses primarily on—

- Vulnerabilities of the evolving PN and their potential for affecting NS/EP

communications

• Possible solutions to help protect the service assurance reliability of the evolving public next generation network (NGN).

(For detailed information on network convergence and the NGN, see Appendix B.) Future analysis by Government could focus on alternative network configurations as they evolve (e.g., GovNet).

Factors Impacting Network Security

The September 11, 2001, terrorist attacks on the World Trade Center (WTC) and the Pentagon renewed concerns regarding physical threats to the PN. The operations of a major Verizon switching center were heavily impacted by the WTC attack, and many service providers suffered either full or partial loss of service in lower Manhattan.[3] Additionally, within days of the terrorist attacks, the "Nimda" worm distributed denial of service (DDoS) attack was launched, affecting Internet services within many organizations. This attack, however, did not cause prolonged Internet damage. While the Internet's ability to rapidly recover from such events is evidence of the resilience of its overall design, the Nimda worm illustrated the potential for economic harm and disruption to communications stemming from such malicious code attacks. In essence, these recent events remind us how important it is, in this time of network evolution and convergence, to consider the wide realm of physical and cyber threats to the evolving PN and its control space, and to make effective policy recommendations to mitigate them.

Physical Vulnerabilities

Definitions

The **Telecommunications Electric Service Priority (TESP) program** promotes, on a voluntary basis, the inclusion of telecommunications facilities considered critical to NS/EP in existing electric utility emergency priority restoration systems.

The **TSP System** is the regulatory, administrative, and operational framework for priority restoration and provisioning of any qualified NS/EP telecommunications service.

To date, the telecommunications infrastructure has not been a direct target of terrorism. However, the infrastructure was an incidental victim of the events of September 11, 2001.

In the future, the telecommunications infrastructure might be the target. Given that eventuality, it may be necessary for the Federal Government to assist industry in protecting the Nation's critical communications assets. The Telecommunications Information Sharing and Analysis Center (Telecom-ISAC) is the best place to coordinate and prioritize Federal assistance to the telecommunications industry.

In addition, the Network Security/ Vulnerability Assessments Task Force (NS/VATF) discussed the responsibility of State and local governments to provide physical protection for the Nation's telecommunications assets. The task force concluded that such efforts could best be facilitated through existing Federal mechanisms and also the Telecom-ISAC.

Because of the changeable threat environment, another important goal is to increase efforts to mitigate impacts to NS/EP services. Reenergizing the Telecommunications Electric Service Priority (TESP) program and supporting the Telecommunications Service Priority (TSP) system could aid this goal.

Although physical security of critical communications facilities is essential,[4] the effects of a physical attack are mitigated by the presence of multiple, diverse facilities-based networks. This alleviates the impact of communications disruption at an affected site and makes it unlikely that any single point of failure would cause regional or national disruption. The NSTAC's *"Last Mile" Bandwidth Availability Task Force (LMBATF) Report* describes essential requirements to maintain multiple access and various methods of backup for critical facilities. The LMBATF noted that facilities should not rely on only wireline infrastructure but also on wireless backup systems. The NS/VATF endorses the LMBATF recommendation that industry and Government cooperate to develop and maintain comprehensive and adequate plans to ensure that multiple paths of communications into critical facilities are in place.

Notwithstanding the discussion above, all of the critical elements of the Nation's

infrastructures cannot be protected against all possible physical attacks.

Cyber Vulnerabilities

In addition to the enduring physical threat to the Nation's networks, cyber attacks present a growing threat to the security of U.S. information systems and consequently critical communications of the NS/EP community. Also, as the U.S. economy becomes ever more tightly connected through telecommunications, electronic signaling systems, power generation, information lines, financial connections, transportation nodes, and other connections involving critical infrastructures, possible disruptions have a far greater potential than ever before to ripple through the economy.[5] The tools and techniques used to attack the PN and information systems supporting NS/EP users have grown considerably in sophistication, while the availability of user-friendly tools has enabled less knowledgeable hackers to conduct attacks with relative ease. These tools are often developed to specifically target known vulnerabilities that are not yet patched, allowing systems to be exploited easily.

In addition, variants of an attack tool are often developed within hours of forensic analysis and distribution of the attack tool source code within the cyber security community. In particular, the PN has witnessed a profound increase in DDoS attacks.

DDoS Attacks

The "Code Red" worms marked the beginning of a new era in sophisticated attack tools and techniques by combining the worm propagation technique with a DDoS attack capability. DDoS involves an attack on a network using multiple infected computers, or "zombies." Code Red exploited a buffer overflow vulnerability in Microsoft Internet Information Server (IIS) Web server software and installed itself onto vulnerable systems. The worm spread until July 20, 2001, at which point all infected hosts participated in a DDoS attack against the White House Web site (www.whitehouse.gov). Code Red then became dormant and reappeared the first day of the next month to restart its cycle. Code Red II, which was the second worm that appeared, used the same Microsoft vulnerability to spread but offered a different payload. Unlike Code Red, which was memory resident, Code Red II left a back door on the infected server to allow attackers to exploit the system.

The Code Red worms illustrated how widespread automated propagation of malicious code has developed into a means for establishing the foundation for DDoS attacks. Furthermore, network topology is evolving to one in which high-powered user devices are connected to the backbone via high-speed connections. This capability, if not

protected, can be subverted by improved methods of launching DDoS and other types of malicious Internet attacks.

As attack techniques increase in sophistication and intruders continue using DDoS techniques to exploit vulnerabilities, cyber attacks will likely cause greater collateral damage.[6] This is of particular significance to NS/EP communications because even if such communications capabilities are not a primary target of specific attacks, they can still be collaterally impacted by attacks on other entities or capabilities.

Collateral damage was witnessed during the Nimda worm incident. In September 2001, the Nimda worm spread through e-mail and unprotected network shares, much like "Sircam," which spread via e-mail in July 2001 and added a new sophistication by merging a virus, worm, and Trojan horse into one malicious code. Nimda also spread from clients to Web servers; the clients actively scanned for and exploited various Microsoft IIS vulnerabilities on Web servers and scanned for back doors left behind from the Code Red and Code Red II worms.[7] The Nimda worm used some of the significant attack profile aspects of Code Red II, allowing it to spread widely and rapidly. It also generated a denial of service (DoS) as a result of network scanning and e-mail propagation.[8] The Nimda worm appeared on the heels of the terrorist attacks of September 11, 2001, contributing to communication congestion and delays experienced by emergency responders.

Attackers' use of source IP address spoofing and the emergence of distributed attack techniques and tools persistently challenge those who respond to and attempt to mitigate the impacts of DoS attacks.[9] This challenge is compounded by the lack of complete and accurate analytical information related to such attacks and a lack of unified response mechanisms to counter the attacks. Infection rates of the Code Red worms were tracked worldwide, but there were divergent reports of infection. For example, one Web page reported 53,000 infections and 250,000 infections, simultaneously. This example of data divergence demonstrates the need for a reliable, coordinated way to count and report infection rates in a public forum. The telecommunications infrastructure operators have taken steps to address this need through the creation of, and participation in, the Telecom-ISAC.

Also needed is a better coordination mechanism for the expeditious disclosure of new vulnerabilities, as well as the availability of patches and their application. These shortfalls are of particular concern because of the speed at which vulnerabilities are being exploited. A vulnerability may remain open to exploit regardless of the availability of a patch because typically, several hours elapse between the announcement of a vulnerability and the implementation of a successful patch. This brief window requires

quicker detection of vulnerabilities, and deployment and application of countermeasures. Because of this threat environment, industry and Government are participating in Information Sharing and Analysis Centers (ISAC) to further develop and implement unified and centralized capabilities to identify and respond to attacks as they are occurring. In addition, each Government organization and private sector enterprise must maintain stringent version control of hardware, software, and current patch releases to ensure effective threat deterrence.

Control Space Vulnerabilities

As network convergence continues, malicious attacks that focus on the network control space are increasingly likely. The NSTAC, and more specifically the Convergence Task Force (CTF), previously addressed key issues regarding the security of the control space of converged networks (see *Convergence Task Force Report*, June 2001). The NS/VATF remains concerned that additional steps are needed to enhance the security of the control space of evolving networks. Therefore, the NS/VATF believes it necessary to reiterate the issues raised by the CTF. The CTF noted that the interoperation of the intelligent network of the public switched telephone network (PSTN) with IP networks via signaling gateways is of particular concern. Specifically, the CTF said, "As this occurs, IP networks could present those with malicious intent a 'back door' into the control space of the PSTN, which could enable malicious activities such as insertion of false Signaling System 7 (SS7) messages. If unauthorized parties gain access to a signaling gateway, they could disrupt or suspend its operations, alter its routing tables, or use it to forward false communications to other signaling gateways. Such activities could precipitate network disruptions and impact overall network reliability and availability. Also, if the operations of a media gateway controller (with SS7 capabilities) were maliciously targeted, all customers whose service depends on that controller would likely experience service disruptions to include Enhanced 911 and NS/EP services. Because the media gateway controller will likely play a critical role in the NGN, and because of its coordinating function among other network elements, security mechanisms are vital to sustain its reliability."

"Another matter of concern involves the coupling of call control with bearer channels in packet networks. In the traditional PSTN, the SS7 network is an out-of-band signaling system that provides call setup and call services separate from the actual transport of the voice data. However, in IP networks, the network intelligence data is transmitted over the same infrastructure as the data itself. Therefore, in IP-based networks, signaling messages are not accorded any higher priority than any other data or voice traffic in the network. During periods of congestion, signaling messages are as likely to be blocked or dropped as any other messages. In a converged network, such events could impact

availability and reliability of the Government Emergency Telecommunications Service (ETS), which relies on the signaling network for functionality."[10]
The NS/VATF believes that industry and Government must continue to work together to secure the control space of emerging networks for NS/EP communications. Foremost, it is essential to secure the command and control mechanisms of the telecommunications infrastructure through interdevice communications. Given that the current command and control mechanisms are evolving toward Transmission Control Protocol/IP-based applications, implementation of secure data transmissions can be facilitated using IP Security (IPSec). IPSec should be implemented in operational systems used in the deployment, management, and provisioning of telecommunications infrastructure.

Ensuring authenticated, secure communications where there is interaction of shared infrastructures (i.e., SS7) is also critically important. In addition, industry must ensure network perimeter security wherever control data transits nonprivate networks, through use of state-of-the-art intrusion detection systems and signaling gateway firewalls. Essentially, the detection and deterrence capabilities of network edge equipment must be enhanced to minimize the negative impacts of distributed attacks.

Definitions

IP version 6 (IPv6) is a new version of the Internet Protocol, designed as a successor to IP version 4 (IPv4), the predominant protocol in use today. The changes from IPv4 to IPv6 are primarily in the following areas: expanded addressing capabilities; header format simplification; improved support for extensions and options; flow labeling capability; and consolidated authentication and privacy capabilities. (Source: The Internet Society, URL: http://www.isoc.org/briefings/001/).

IP Security (IPSec) is a suite of protocols designed to provide high-quality security for Internet traffic. Some of the advantages of IPSec are—

It is below the transport level so it is transparent to applications and end users.
When implemented in a firewall or router, it provides strong perimeter security.
It can provide security to individual users if needed.

The NS/VATF continues to believe that industry and Government must cooperate to address control space vulnerabilities and implement subsequent remedial tools, including IPSec. Future work on IP version 6 (IPv6) is also important for the provision of future NGN communications. It is particularly important that industry and Government work with relevant standards bodies to ensure NS/EP communications functional requirements are considered during their work on network convergence issues, including security of PSTN-IP network SS7 control traffic.

The Government and NSTAC Network Security and Information Exchanges (NSIE) are analyzing possible development of a cross-industry security posture that could help provide a foundation for containing the control space of the emerging PN. This is a preliminary effort focused on developing a standard set of requirements to address the risks created during operation support system (OSS) flow-through and potential attacks at various levels of the

Telecommunications Management Network layers. The premise for this analysis is that a complete solution for securing the control space (i.e., OSS and SS7) of the evolving PN can probably be accomplished only through agreement on and implementation of a single industry-wide, vetted set of techniques. The NS/VATF encourages both industry and Government support of this NSIE-led effort.

Wireless Network Vulnerabilities

Definition
Wireless Access Protocol (**WAP**) is the de facto worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, Personal Digital Assistants (PDA), and other wireless terminals.

The growing demand for mobile e-services, applications, and access to corporate databases is facilitating advances in wireless services and technologies. Consequently, the security of wireless protocols and systems, including the wireless application protocol (WAP), wireless local area networks (WLAN), and personal area networks (PAN), has emerged as an important issue when related to NS/EP communications transiting wireless networks and technologies.

The interoperability of wireless and wireline communications methods raises some network security and vulnerability issues. Specifically, end-to-end security for wireless networks and electronic transmissions involving WAP-enabled applications lags behind the levels of security found in more robust Internet standards. The WAP-related security problems stem from vulnerabilities in the WAP gateway model and translation methods.

WAP gateways are the software providing connectivity between the Internet and mobile networks. Industry experts predict WAP gateways for service providers will act as "hacker magnets" and provide insufficient security levels for Web transaction services.[11]

Wireless application Protocol

The potential threats to WLANs and PANs are unique to wireless technologies and are exacerbated by the connection between wireless and wireline networks.[12] WAP enables wireless and wireline networks to exchange information via a list of protocols and specifications. Mobile WAP devices attach to mobile networks via a modem to a dial-in server, which in turn provides content to the WAP device in Wireless Markup Language. All major mobile carriers in the United States offer wireless data services based on WAP. However, complex wireless protocol stacks, weak encryption, shared keys, users' confusion, and bandwidth and device restrictions may prompt vendors to take security

shortcuts with emerging mobile devices and services.[13]

The WAP standard uses its own protocol stack for security in lieu of the more robust common Internet security standard. Although the Internet standards and the wireless standards interoperate, they default to the less robust wireless security standard for wireless communications. In Internet wireline communications, the Secure Socket Layer (SSL) protocol encrypts data and public key infrastructure (PKI) can be used to authenticate users. For wireless transactions, WAP features the Wireless Transport Layer Security (WTLS) protocol, which is the wireless equivalent of SSL, and a similar wireless version of PKI. WAP transactions travel from a wireless device (using WTLS) to a carrier's WAP gateway and are converted to SSL before being transmitted to the other end user, database, or application. When this conversion to SSL takes place in the gateway, the encrypted information is initially converted to clear text. The encrypted information might contain important and proprietary information. Those with malicious intent can attempt to intercept the information while it is in clear text, posing risks to the viability and reliability of the transaction.

Government work with standards bodies would help to ensure consideration of NS/EP communications functional requirements during work addressing the security of the interoperation of wireless and wireline networks, and more specifically, activities addressing WAP.

Wireless Local Area Networks

A WLAN is a high-speed data network without wires, providing connectivity throughout a particular building or campus. Although these networks are cost-effective, convenient, and scalable, the security of WLANs is a serious concern. According to Gartner Group, by the end of 2002, 30 percent of enterprises will suffer serious security exposures because they have deployed WLANs without proper security.[14]

WLANs are vulnerable to well-known data network vulnerabilities, including DoS attacks. WLANs also introduce new vulnerabilities, including—

- **Client-to-Client Attacks**—which are possible because clients in WLANs can interface directly with each other without the need of access points. Therefore, each client needs to be protected against potential attacks from other directly connected clients.

- **Misconfiguration Attack**—which occurs because, by default, WLANs are shipped

from the factory in a low security mode (such as shipping WLANs with default passwords that are known to the hacker community). Systems administrators are expected to reconfigure the systems upon receiving them; otherwise, these new WLANs will remain at a high risk for attack.

WLANs use the 802.11b security standard, which includes the wired equivalent privacy (WEP) protocol. WEP employs the well-known Ron's Code 4 (commonly known as RC4) pseudo-random number generator algorithm, which uses a 40-bit key and can be decrypted in about 5 hours.[15] This security vulnerability allows an attacker to eavesdrop on and modify transmissions over WLANs. One new form of attack, "war driving," has become common because of the widespread deployment of unsecured WLANs. War driving occurs when attackers use hacking

software available on the Internet[16] and a WLAN access device, equipped with an external antenna and installed in a laptop computer, to scan the airways for unprotected 802.11b networks that employ minimal security measures (e.g., only the WEP standard) or have security mechanisms (e.g., WEP encryption) turned off.[17],[18] More robust forms of encryption, such as Virtual Private Networking utilizing the more robust encryption of IPSec, are available. Use of the built-in security features, such as WAP, would help to counter the success of WLAN hacking, while deployment of IPSec would render war-driving attacks virtually impossible.

Government departments and agencies using minimal security measures in any critical WLANs, such as those supporting NS/EP requirements, are subject to potential compromise (e.g., client-to-client attacks, misconfiguration attacks, and war driving). It would be beneficial for these departments and agencies to deploy WLANs with higher levels of security. Beyond this, non-mission-critical WLANs may become interconnected with mission-critical systems. Therefore, consideration should be given to deploying higher level security for all WLANs.

Personal Area Networks

PANs are similar in design to WLANs, although PANs cover a shorter range (usually 10 meters or less). The primary reason for the growing popularity of PANs is that they eliminate the need for short-distance hardwire connections, thus adding flexibility, speed, cost savings, and efficiency to organization networks.

PANs employ the InfraRed Data Association (IrDA) standard, which allows personal digital assistants (PDA) to send and receive applications from other devices. In the

future, we anticipate this technology may evolve to use other wireless spectra. Because it does not have any built-in security mechanisms, the IrDA standard can transfer potentially malicious code among PDAs. Users could then transport the viruses onto a home computer or an organization's network. PDAs, and consequently corporate networks, are becoming increasingly vulnerable to viruses through PDA synchronization. This occurs when PDA applications carrying malicious code are downloaded from the Internet and personal computers, and then the application is synchronized with a computer that is connected to a network. PDA security is a growing concern as Federal departments and agencies are using PDAs for security-related applications, including one-time password generation, storage of medical records, and confidential inventory tracking.[19]

The widespread deployment of PAN technology poses a growing threat. The Government could consider policies that would allow use of these devices while reducing their risk of compromise. Such policies could support—

- Centralized management and deployment of PAN technologies
- Centralized management of security measures for PANs
- Disallowing untracked, unmanaged devices from synchronizing with critical systems
- Installation and maintenance of agency-supplied security, backup, and auditing tools.

NS/EP implications

Physical, cyber, and control space vulnerabilities of the PN, including its wireless networks, can have enormous impacts on NS/EP services. Even localized physical outages of supporting communications infrastructure can disrupt NS/EP communications for specific organizations. Likewise, malicious cyber attacks have the potential, through direct means or collateral impact, to affect data communication capabilities critical to NS/EP. As critical infrastructures become more dependent on IP services, malicious attacks will target these systems more frequently and likely use more destructive payloads.

Malicious attacks like the Code Red, Sircam, and Nimda worms will continue to evolve and have a greater impact on the NGN. Such attacks will likely affect management and operations of packet networks because of insecure signaling and management protocols. They will also exploit the trust relationships between soft switches, access managers, and gateways. Similarly, inadequate packet network security procedures or standards will become increasingly troublesome as organizations supporting NS/EP activities become more reliant on IP technology and services for communication. For instance, packet network vulnerabilities, such as those illustrated by the Code Red worms, will affect the

reliability of voice over packet and voice over IP services.

Therefore, industry and Government must continue to work together to devise countermeasures and strategies to mitigate the impacts of physical and cyber attacks on critical infrastructures. Automated rather than manual responses to such attacks would expedite the capability to respond.

Countermeasures/ Mitigation Strategies

On the basis of our analysis, the NS/VATF concludes that the best strategies for countering vulnerabilities of the critical telecommunications infrastructure involve standards bodies support, Government contractual specification, and stakeholder awareness. The NS/VATF also reviewed the findings of the Legislative and Regulatory Task Force (LRTF) regarding NS/EP legal and regulatory implications of network convergence, including whether additional legal authority is required to ensure NS/EP services in the converging and NGN environments. The NS/VATF's comments on those findings are also included in this section.

Standards Support

Because of the prevalence and increasing impact of DoS and DDoS attacks on critical infrastructures, standards bodies are beginning to focus on cyber security as a topic of primary importance. Increased emphasis on Government participation in standards bodies and a coordinated Government approach to standards development are critical. This emphasis could include increased funding and resources for priority standards efforts such as the ETS.[20] The work on IPv6 deployment[21] and IPSec development, as well as the focus on ETS will continue to advance the capabilities presently available for NS/EP users.

This emphasis will yield the standards basis for vendor features and carrier products and services in support of NS/EP service requirements through commercial off-the-shelf procurements. Such efforts are essential to making NS/EP services commercially available in the NGN.

Government Contractual Specifications

As security standards are developed and become the state of the practice, Government can help establish the market by specifying those elements in contracts and purchase orders. This process would result in more commercial off-the-shelf products and services, which Government can then procure at reduced cost. Unique network security and other service assurance requirements above and beyond the state of the practice can also be specified in contracts. This further supports the recommendation to the President provided in the *Convergence Task Force Report*, June 2001.[22]

Stakeholder Awareness

Many categories of stakeholders are responsible for PN security. The interests of all stakeholders need to be taken into account when considering network security improvements. The Government would be an appropriate sponsor for much needed public debate among various stakeholders. Stakeholders include—

- End users
- Network providers
- Service providers
- Equipment providers
- Software providers
- Government
- Academia.

Stakeholders need to be educated on security mechanisms for information technology systems, networks, and computers. Efforts to educate individual information technology users about security issues may well serve as a deterrent while helping to increase the overall security of the PN.

A number of technologies and software-based best practices can help defend against the growing threat of cyber attacks, especially DDoS attacks. Similar to deployment of end-user security mechanisms, organizations can take steps to help ensure their networks are not compromised. Strong cyber security and response plans are some of the best practices for securing networks. Other best practices include implementation of—[23]

- Strong authentication and password policies

- Robust antivirus software on all computers, including, where possible, pushing updates to users, and providing positive reporting audits

- Automatic updates for operating systems and application software, including, where possible, pushing the latest patches to users, and providing positive reporting audits

- Intrusion detection systems and firewalls

– Firewall technology for all computers, with priority to those operated outside of the network firewalls (e.g., home and in-transit personal computers, especially those connected to broadband services such as digital subscriber lines and cable modems)

– Edge routers and firewalls configured to deny all unauthorized services and incoming traffic

- A provision to identify all devices and services in network and user equipment and the ability to disable those not required.

In conclusion, stakeholders must be diligent in configuring network infrastructures to mitigate vulnerabilities that can be exploited to launch attacks.

Legislation and Regulation

In response to a previous NSTAC tasking, the NSTAC's LRTF examined NS/EP legal and regulatory implications of network convergence. Specifically, the LRTF has considered the following questions—

- Is additional legal authority required to ensure NS/EP services in the converging and NGN environments?

- What is the proposed legal basis for NGN priority service (i.e., packet) obligations?

- Is authority available for wireless providers to provide NS/EP services and are new or revised legislation and/or executive orders required for NS/EP services in the converging and NGN environments?

- Are potential antitrust protections necessary for cooperation among service providers of NS/EP services in the NGN?

Based on the LRTF report, the NS/VATF concludes that the legal issues underlying the provisioning of NS/EP priority services to the Federal Government in an NGN environment are extremely complex and may require further study in response to any proposed legislation and/or regulation. Until the standards for packet-based services are established, including provisions for ETS, and the Government's requirements in the evolving environment are certain, new legislation or regulation is premature.

For more information, see Appendix E, *Legislative and Regulatory Task Force Report*.

conclusions

The NS/VATF reached the following conclusions:

- To date, the telecommunications infrastructure has not been a direct target of terrorism. Nonetheless, the infrastructure was an incidental victim of the events of September 11, 2001. In the future, the telecommunications infrastructure might be the target of attack. Given that eventuality, it may be necessary for the Federal Government to assist industry in protecting the Nation's critical communications assets. The Telecom-ISAC is the best forum to coordinate and prioritize Federal assistance to the telecommunications industry.

- Because of the changeable threat environment, another important goal is to increase efforts to mitigate impacts to NS/EP services. Reenergizing the TESP program and supporting the TSP program could aid this goal.

- Within each Government organization and private sector enterprise, stringent version control of hardware, software, and current patch releases must be maintained to ensure effective threat deterrence.

- Ensuring authenticated, secure communications where there is interaction of shared infrastructures (i.e., SS7) is critically important. Industry must ensure network perimeter security wherever control data transits nonprivate networks, through use of state-of-the-practice intrusion detection systems and signaling gateway firewalls. Essentially, the detection and deterrence capabilities of network edge equipment must be enhanced to minimize the negative impacts of distributed attacks.

- Industry and Government must cooperate to address control space vulnerabilities and implement subsequent remedial tools, including IPSec. Future work on IPv6 is also important for the provision of future NGN communications. It is particularly important that industry and Government work with relevant standards bodies to ensure NS/EP communications functional requirements are considered during their work on network convergence issues, including security of PSTN-IP network SS7 control traffic.

- A cross-industry security posture could help provide a foundation for containing the control space of the emerging PN. It is important for industry and Government to support the NSIE-led efforts in this area.

- Government work with standards bodies would help to ensure consideration of NS/EP communications functional requirements when addressing the security of the interoperation of wireless and wireline networks, and more specifically, activities addressing WAP.

- It would be beneficial for departments and agencies to deploy WLANs with higher levels of security. Beyond this, non-mission-critical WLANs may become

interconnected with mission-critical systems. Therefore, consideration should be given to deploying higher level security for all WLANs.

- Government policies should allow use of PAN devices while reducing their risk of compromise. Such policies could support—

– Centralized management and deployment of PAN technologies

– Centralized management of security measures for PANs

– Disallowing untracked, unmanaged devices from synchronizing with critical systems

– Installation and maintenance of agency-supplied security, backup, and auditing tools.

- Industry and Government must continue to work together to devise countermeasures and strategies that would mitigate the impacts of physical and cyber attacks on critical infrastructures such as the PN. Automated rather than manual responses to such attacks would expedite the capability to respond.

- Because of the prevalence and increasing impact of DoS and DDoS attacks on critical infrastructures, standards bodies are beginning to focus on cyber security as a topic of primary importance. Increased emphasis on Government participation in standards bodies and a coordinated Government-wide approach to standards development are critical. This emphasis could include increased funding and resources for priority standards efforts such as the ETS.

- As standards are developed and become the state of the practice, Government can help establish the market by specifying those elements in contracts and purchase orders. This process would result in more commercial off-the-shelf products and services, which the Government can then procure at reduced cost. Unique network security and other service assurance requirements above and beyond the state of the practice can also be specified in contracts. This further supports the recommendation to the President contained in the NSTAC *Convergence Task Force Report*, June 2001.

Recommendations 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,* and Executive Order 13231, *Critical Infrastructure Protection in the Information Age,* direct the appropriate departments and agencies, in coordination with industry to—

- Coordinate and prioritize through the Telecommunications Information Sharing and Analysis Center, Government assistance to industry to protect the Nation's critical communications assets and to mitigate the effects of an attack as it is occurring

- Encourage and adequately support the development and adoption of baseline standards and technologies, including Internet Protocol version 6, Internet Protocol Security, and the Emergency Telecommunications Service scheme to help bolster core security and reliability of the Next Generation Network

- Support the Network Security Information Exchanges' efforts to develop a cross-industry security posture that could help provide a foundation for containing the control space of the emerging public network

- Work with standards bodies to ensure consideration of NS/EP communications functional requirements while addressing the security of the interoperation of wireline and wireless networks, and more specifically, activities addressing the wireless application protocol

- Ensure that all wireless local area networks used by the Government meet the highest level of security standards available, with priority given to those supporting NS/EP missions

- Develop policies and procedures to support the use of personal area network devices while reducing their risk of compromise.

APPENDIX A

TASK FORCE MEMBERS AND OTHER PARTICIPANTS

taSK fORCE mEMBERS

SAIC	Mr. Hank Kluepfel, Chair
Verizon	Mr. James Bean, Vice-Chair
AT&T	Mr. Harry Underhill
BellSouth	Mr. Shawn Cochran
Boeing	Mr. Bob Steele
Cisco Systems	Mr. Charles Booth
CSC	Mr. Guy Copeland
EDS	Mr. Dale Fincke
Global Crossing	Mr. Hank Fischer
ITT	Mr. Joe Gancie
Lockheed Martin	Mr. Brian Dailey
Lucent	Mr. Karl Rauscher
Motorola	Mr. Henry Ott
Nortel Networks	Mr. Jack Edwards
Northrop Grumman	Mr. Scott Freber
Qwest	Mr. John Lofstedt
Raytheon	Mr. Tom O'Connell
Rockwell	Mr. Ken Kato
SBC	Ms. Rosemary Leffler
TRW	Mr. Sy Sherman
USTA	Mr. Paul Hart
WorldCom	Ms. Joan Grewe

OTHER PARTICIPANTS

Cisco Systems	Mr. Kevin Ziese
GWU	Mr. Jack Oslund
Telcordia	Mr. John Kimmins
WorldCom	Ms. Cristin Flynn
WorldCom	Mr. Kevin McMahon

GOVERNMENT PARTICIPANTS

DISA	Mr. Tom Dickinson
NCS	Mr. Harold Folts
NSC	Ms. Marjorie Gilbert
	Mr. Paul Kurtz

APPENDIX B

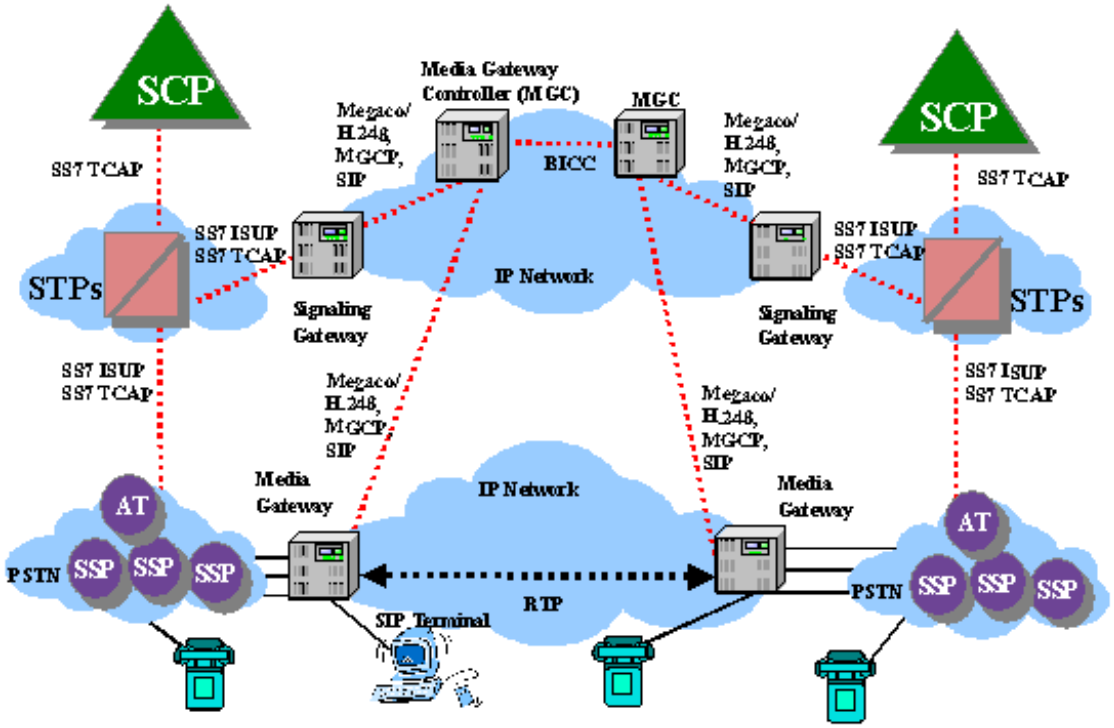
UNDERSTANDING NETWORK CONVERGENCE AND THE NEXT GENERATION NETWORK

Understanding Convergence and Interconnection of Emerging Networks

(Source: "NGN Convergence: Security Issues and Recommendations," Telcordia Technologies, October 2001).

Figure B-1 illustrates a typical public switched telephone network (PSTN) and next generation network (NGN) convergence architecture. Various combinations of user communications can occur. For example, users served by the PSTN can communicate with users served by the NGN. Users served by the NGN can communicate with users served by the PSTN. Users served by the PSTN can communicate with users served by the PSTN through an NGN. For multiparty calls, numerous other combinations are possible.

Figure B-1. Reference PSTN and NGN Convergence Architecture



In the reference architecture shown in Figure B-1, the PSTN consists of service switching

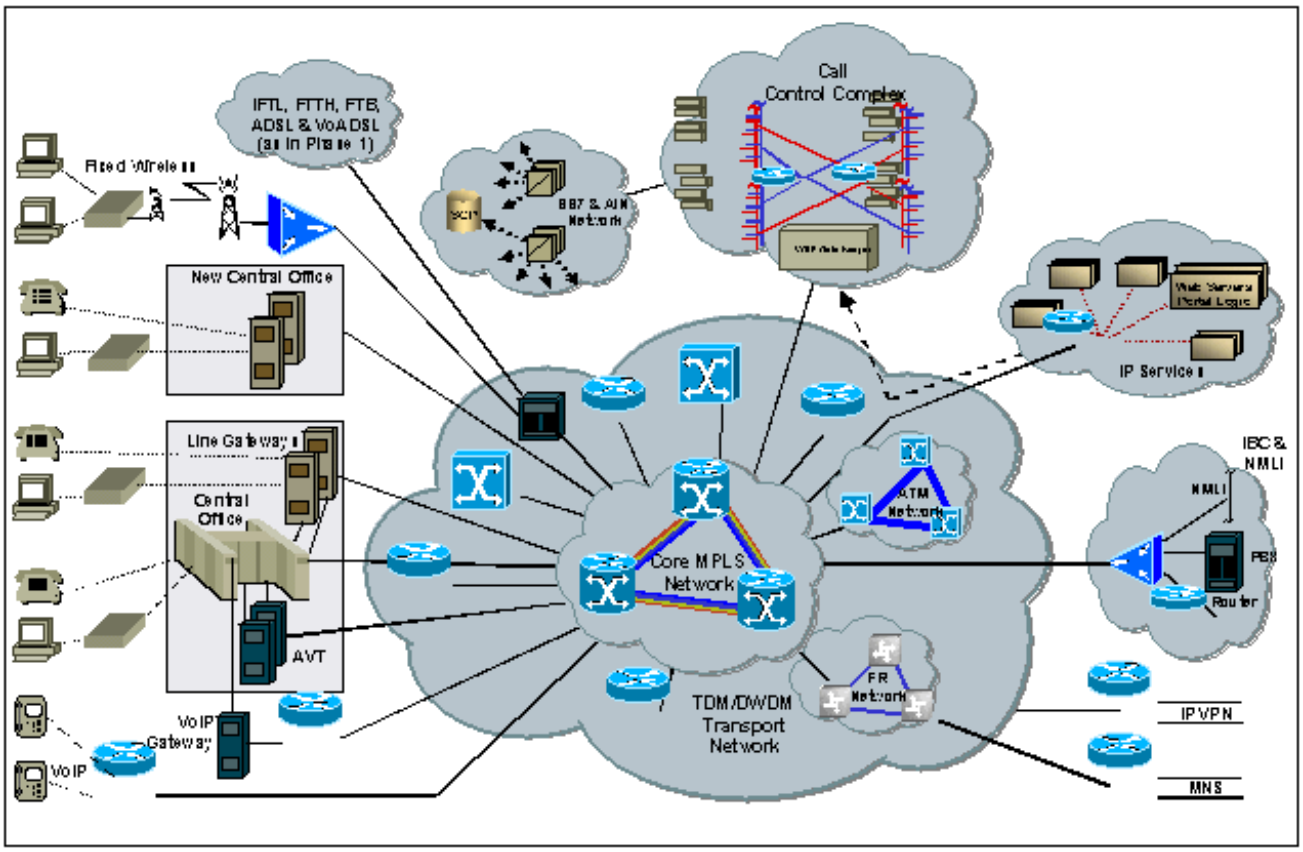
points (SSP), which may be local or tandem exchanges (i.e., switching systems), signaling transfer points (STP), and service control points (SCP). The NGN consists of media gateways, signaling gateways, media gateway controllers, and an Internet Protocol (IP)-based core network. In this reference architecture from a Session Initiation Protocol (SIP) perspective, signaling gateways could support the SIP gateway functionality, and media gateway controllers could support the SIP server functionality.

Understanding the Next Generation Network

(Source: NSTAC Convergence Task Force Report, May 2001)

As indicated in Figure B-2, the NGN will be a complex, diverse network. According to this depiction, the emerging NGN will unify multiple legacy and new services into a single backbone network consisting of IP running over an asynchronous transfer mode (ATM) network using multi protocol label switching (MPLS). ATM is a network technology that supports multimedia communications such as real-time voice and video as well as data. MPLS enables IP-ATM integration, traffic engineering, and establishment of virtual private networks. MPLS also provides tools to engineer quality of service (QoS) features into the network. This is important because in a converged PSTN-IP network environment, different services have different reliability, protection, and restoration (RPR) requirements, as well as different QoS requirements (e.g., throughput, latency, guaranteed delivery). Essentially, services crossing multiple networks must rely on cooperation at each network-to-network interface (NNI) to provide end-to-end RPR and QoS. MPLS enables the policy-based networking needed to achieve this. Policy-based networking uses a network management paradigm with centralized databases for rules to enable distributed policy enforcement at the network element level. Such a system would help simplify operations with uniform control, translate service-level policy to network control functions, and permit scalability.

Figure B-2. Sample Depiction of an NGN Architecture



APPENDIX C

THE EMERGENCY TELECOMMUNICATIONS SERVICE (ETS) IN EVOLVING NETWORKS

The Emergency Telecommunications Service in Evolving Networks February 4, 2002—Version 3.0

Abstract

This white paper presents the functional requirements, features, and objectives for the Emergency Telecommunications Service (ETS) in newly emerging telecommunication networks. The ETS is an extension of the International Emergency Preference Scheme (IEPS) of the International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) Recommendation E.106 and includes additional provisions for multimedia services through a packet-based telecommunications environment. Efforts are underway in the national standards bodies and international organizations to identify, establish, and apply a comprehensive family of ETS standards

for new packet-based networks.

1. Introduction

The purpose of the Emergency Telecommunications Service (ETS) is to facilitate emergency recovery operations for restoring the community infrastructure and for returning the population to normal living conditions after serious disasters and events, such as floods, earthquakes, hurricanes, and terrorist attacks. The ETS will be provided through shared resources from the public telecommunications infrastructure that is evolving from a basic circuit-switched configuration of today's conventional telephone networks to an Internet-based, packet-switched technology providing a richness of communication capabilities. The timely establishment of an effective ETS has been given significant urgency as a result of the September 11 terrorist attacks in the United States.

Many challenges and considerations need to be addressed in defining and establishing the functional capabilities for the ETS in the emerging packet-based telecommunications services. This paper presents an overview of the basic requirements, features, and concepts for ETS that packet-based telecommunication and third-generation (3G) mobile networks are capable of providing and that must receive attention during the process of the convergence of these technologies. Specific solutions are not offered, but this paper is intended to stimulate innovative thinking and productive discussion in industry standards bodies leading to development, establishment, and deployment of appropriate standards for the evolving telecommunications services.

Disasters situations can occur any time, any place unexpectedly. These events often significantly damage the community infrastructure and severely disrupt daily living. Recovery requires rapid response by local authorities, immediate reaction from utility service providers, and support from medical, construction, fire, and police resources. Effective communications are essential to facilitate the myriad activities for coordinating lifesaving activities concurrent with reestablishing control in the disaster area. Following a disaster, immediate response operations focus on saving lives, protecting property, and meeting basic human needs.

2. ETS Operational Requirements

A U.S. Government working group recently identified 14 basic functional requirements for the future ETS. These requirements are listed in the table below and represent the objectives that need to be fulfilled for national security and emergency preparedness (NS/EP) in the ETS.

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

m. Affordability	Services must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf technologies, services).
n. Reliability/Availability	Services must perform consistently and precisely according to their design requirements and specifications and must be usable with high confidence.

These 14 functional requirements are discussed in this white paper. Several of these are elaborated upon in more detail in Section 4 providing considerations for the 11 ETS features and objectives. The other requirements are addressed by text presenting the many concepts that are involved in the development of a comprehensive and effective ETS. The {x} in the text identifies the functional requirement in the above table that is being addressed in this paper.

Public telecommunication services are universally available, deployed by a massive infrastructure throughout most nations, except in the most remote and unpopulated regions. These critical telecommunications resources, therefore, must be depended on by the emergency responders for supporting the organization and coordination of initial and ongoing recovery activities. It is possible to realize readily these capabilities by leveraging the resources that are ubiquitous and most likely to be immediately available any place, any time {h}. This includes the use of wireless services as mobile networks expand their coverage {g}. Dedicated or special government telecommunications resources, on the other hand, do not generally have the immediate global reach to be responsive initially to disaster events.

Two recommendations of the ITU-T present the basic requirements for international emergency telecommunications. ITU-T Recommendation E.106, *Description of an International Emergency Preference Scheme (IEPS)* [1], applies to telephony services provided by the public switched telephone network (PSTN), integrated services digital network (ISDN), and public land mobile network (PLMN). ITU-T Draft Recommendation F.706, *Service Description for an International Emergency Multimedia Service (IEMS)* [2], applies to all modes of telecommunications service, including telephony, over the newly emerging telecommunication networks, including the packet-based Internet Protocol (IP) technology and 3G mobile networks. The ETS can be used both in national and international contexts and includes the provisions of the IEPS and the IEMS.

Conventional circuit-switched telecommunications services are rapidly evolving to a connectionless packet-switched technology. Wireless technology is also evolving toward the new 3G capabilities for seamless provisioning of services over and across the

heterogeneous fixed and mobile networks. A substantial transition period is under way as these technologies converge. As a result, there will be many critical issues of transition and interoperability to address {f}. The newly emerging technologies will provide greatly enhanced capabilities that can be leveraged and can benefit emergency recovery operations during serious disaster situations. The packet-based packet technology provides a very new environment that must be leveraged for providing effective and economical public telecommunications services for supporting ETS capabilities.

When a disaster event strikes, the public telecommunications infrastructure generally sustains damage, experiences excessive traffic loads, and is subject to external interference that may severely limit the ability for response and recovery activities to communicate. Therefore, special provisions to facilitate effective communications for the emergency activities are necessary. This includes priority establishment and processing of communications through the telecommunication resources that remain available {a}. ETS traffic needs to receive preferential use of the surviving capacity of the impacted network.

3. ETS Features and Objectives

A fully comprehensive ETS needs to have a richness of capabilities to support a variety of operational requirements for emergency recovery forces. The following is a list of specific features that could potentially facilitate communications for disaster recovery activities:

A. Selection of multimedia and telephony services {j} {k}

B. Rapid authentication of authorized ETS users {b}

C. Security protection of ETS traffic {b} {c}

D. Preferential access to telecommunications facilities {a}

E. Preferential establishment of ETS communications {a}

F. Preferential routing of ETS traffic {a}

G. Preferential use of remaining operational resources for ETS traffic {a}

H. Preferential completion of ETS traffic to destination {a}

I. Optional preemption of nonemergency traffic {a}

J. Allowable degradation of service quality for ETS traffic {l} {n}

K. Interchange of critical telecommunications service management information.

{d}{n}

Not all of these features may be immediately possible, practical, or available universally. The above list focuses on the basic capabilities that need to be addressed and developed. These capabilities could greatly facilitate effective and timely recovery operations during emergency events. This paper discusses these features in detail.

Many nations do not have any emergency capability today except for their public telecommunications infrastructure in its present state without any of the special features listed above. In the United States, the Government Emergency Telecommunications Service (GETS) supports emergency recovery operations. However, it only provides priority establishment and routing of telephone calls through the PSTN for specifically authorized users who expect to be involved in emergency recovery operations. GETS fulfills the basic functional requirements of ITU-T Recommendation E.106.

The ETS also has international aspects. Disaster situations are often regional and involve multiple nations {e}. In these cases, disaster recovery assets from multiple nations may be necessary to respond to one specific event. Also, in the increasingly "global" world, many nations often provide support for recovery operations for emergency disasters contained within the borders of another country. ETS traffic, therefore, needs to receive favorable treatment at international gateways and within national networks providing an ETS. {a}

The emergence of new telecommunications technologies and their application for telecommunication services in the evolving telecommunication networks provides great promise for the realization of an enhanced, comprehensive, and effective global ETS. ITU-T Draft Recommendation F.706 [2] presents requirements for multimedia services to support emergency operations. Not only will voice telephony services need to continue, the inclusion of broadband services like video broadcast and conferencing will also be beneficial {k}. In addition, narrowband capabilities such as instant messaging and presence as well as email would facilitate short, rapid command and control information interchange and would enhance recovery operations. This would be particularly useful during periods of limited bandwidth availability and as a last resort to communicate when conditions become most severe.

Currently, prominent international standards bodies are developing a new telecommunication infrastructure that is expected to be deployed over the next several years. It is imperative that the specifications of these networks include support for the functional requirements of a comprehensive ETS before equipment and systems are designed, manufactured, and deployed. None of these new specifications shall cause

change or impairment of operation of existing emergency capabilities or the basic packet-switched infrastructure. With the necessary capabilities built into the new telecommunications infrastructure, the ETS can then become readily available with a diversity of services for emergency response operations through execution of service level agreements (SLA) between service customers (SC) supporting recovery operations and the telecommunications service providers (SP). It will then be possible to offer the service more expediently and to avoid the expense of deploying special capabilities or retrofitting existing systems. The SC will then pay the appropriate tariffs for actual services received.{h}

The availability of the ETS for authorized users could also be specified in an SLA. The ETS could always be available for use at any time and at any place in a specific network. This would allow fast-response access immediately when the disaster strikes. Some networks, on the other hand, may only activate the ETS upon declaration of an emergency by the appropriate authority. This could cause a serious delay in the ability for response and recovery forces to communicate effectively. Some in-between capability could also be possible, where a basic preferential service would always be available and then enhanced features could be activated upon declaration of an emergency.

The transition to packet-based and 3G mobile services for new telecommunication services will involve a number of issues, one of which is to ensure orderly and transparent continuance of the basic E.106 emergency preference capabilities. During the convergence period, the different schemes for interworking between the two technologies must be considered. For example, voice calls from the telephone or mobile network may transit voice-over-IP links and then terminate in either the telephone network or directly in a packet-based network {f}. The European Telecommunications Standards Institute (ETSI) describes four different scenarios of interoperation [3]. Because of the variety in configurations, it is necessary to establish the interfaces for interworking between the signalling systems of today's telephone networks and the new call control and signalling protocols of evolving telecommunication networks. This needs to be accomplished without negatively impacting the fundamental operation or infrastructure of existing and future packet-based networks. As new networks with the basic emergency service priority capabilities come into being, it will be important to provide enhanced services by leveraging the new capabilities of the emerging packet-based networks.{k}

As indicated earlier, ubiquitous telecommunications resources that provide services to the general population provide the basis for readily available capabilities for an ETS.{h} Since public telecommunication resources are normally at hand, emergency operations

activities do not have to wait for deployment of special facilities. However, as emergency operations get under way, supplemental capabilities could also be of significant benefit, particularly when public telecommunication resources become seriously stressed and limited. Therefore, it would be desirable to have a telecommunications infrastructure that can be readily integrated with transportable, redeployable, and fully mobile facilities, such as personal communications service, cellular, satellite, and high frequency radio {f} {g}. Interoperability and interfaces among selected Government or private facilities, systems, and networks would be very beneficial {f}. It is also highly desirable that ETS resources be as robust as possible to support surviving users under a broad range of circumstances, including widespread damage during natural or man-made disasters {i}.

4. ETS Considerations

There are a number of important considerations that need to be studied to best use the connectionless packet technology for the ETS in the new telecommunication capabilities. The advantages and inherent characteristics of the packet-based technology need to be leveraged and not impeded. It will be necessary to define and establish the appropriate quality, availability, and reliability of service guidelines for the various modes of multimedia communications. There are many formidable challenges that need to be addressed in the fulfillment of the functional requirements that have been established in ITU-T Recommendations E.106 [1] and F.706 [2]. They serve as the principal objectives to meet in provisioning a truly comprehensive and effective ETS. More specific considerations in seeking the necessary mechanisms and solutions for ETS are—

A. Selection of multimedia and telephony services {k}—The basic service defined in ITU-T Recommendation E.106 [1] is telephony as provided by the PSTN, ISDN, and PLMN. The emergence of integrated voice/data services of evolving telecommunication and 3G mobile networks, based on packet switching technology, need to not only support telephony services but also provide a variety of enhanced modes of communication including instant messaging and presence, email, Web and database access, video, and teleconferencing. These additional services can also be used effectively for emergency communications. This will enable emergency recovery operations to have a comprehensive menu of supporting communication capabilities.

B. Rapid authentication of authorized ETS users {b}—The ETS is intended for use only by authorized users involved with emergency recovery operations. The appropriate authority of each nation or community would authorize these designated users. Upon initiation of an emergency communication request, an authentication

process needs to verify the user's identity to protect the telecommunication resources against excessive use and abuse during an emergency situation. In the United States, a personal identification number (PIN) similar to the application of credit card calling in the PSTN currently authenticates authorized GETS users. For the future ETS, it is desirable to establish an innovative method for a streamlined and rapid user authentication in the emerging telecommunication and 3G mobile networks. The passing of authentication as the ETS communication travels across networks also needs to be addressed.

C. Security protection of ETS traffic {b} {c}—Security is a major concern with the evolution of packet-based networks. In addition to the many basic security provisions already under consideration, ETS has additional security provisions that require special attention. Security protection is necessary to prevent unauthorized users from accessing scarce resources needed to support emergency operations. This includes such threats as spoofing, intrusion, and denial of service. In addition, the identity and location of certain authorized users of the ETS need protection.

D. Preferential access to telecommunications facilities {a}—There are a number of ways to access telecommunication resources for obtaining ETS capabilities. These include PSTN wire line, wireless, satellite, cable, digital subscriber line (DSL), and optical fiber. There will be a significant advantage for an emergency operations user to be able to obtain access to these various telecommunications services on a priority or preferential basis. This will enable more rapid initiation of emergency communications.

Today the PSTN service has no general provision for signalling priority access requests. However, specially marked lines or specifically provisioned "off-hook" services could provide preferential access, but that would only be by line and location, not per ETS request. There is currently no provision for conveying a priority dial tone or service initiation via general access from a conventional telephone instrument. Dial tone comes on a demand basis from a limited selection of ports, and heavy traffic conditions can delay access if demand consumes the supply of ports. Therefore, a provision for preferential access to services in packet-based telecommunication networks is a capability that requires consideration.

As with the PSTN dial-tone ports, cellular services have a limited number of channels in each cell to accept call initiation from an end device. When a disaster event occurs in a particular local area, floods of call attempts generally occur. This severely reduces the probability of access. Therefore, a priority access service for designated users or end devices is also needed for cellular services.

Appropriate technical mechanisms inherent in the infrastructure need to be applied to enable preferential access via the various methods for initiation of ETS

communications. It is imperative that authorized emergency operations have the ability to respond rapidly to disaster events in a timely and efficient manner.

E. Preferential establishment of ETS communications {a}—A communication may consist of a single unit of information transiting from source to destination or of a flow of information via a series of packets or stream of data. In technologies that support connection mode operation, an end-to-end path for the communication to transit is established upon entry of the address, or telephone number, of the destination terminal. In connectionless mode operation, individual packets may transit the network over different paths. When the total communication involves a series of packets, they are assembled and processed together at the destination.

Emergency communications must have a high degree of assurance for successfully reaching the destination, regardless of the networks they transit. Therefore, the ETS traffic needs to be uniquely identified and receive preferential treatment over non-emergency traffic. This provides a priority service for authorized communications in the ETS. In a PSTN, once a connection is established, the call effectively is "hard-wired" in the form of a circuit-switched connection and does not require continuance of preferential status. In a connectionless packet network environment, however, it is necessary to maintain the ETS identification for all respective packets. ETS identification also needs to be conveyed to each of the transit networks, regardless whether they support ETS. Telecommunication SPs must be able to identify and prioritize emergency communications according to their SLA with the SCs and other SPs.

F. Preferential routing of ETS traffic {a}—Routing of packets is a continuing process for an instance of communication until the session has reached completion. As indicated above, the priority status and identification of emergency communications must be maintained until session termination. If the path being followed becomes congested or fails, the network or application layer mechanisms could be applied to dynamically reroute ETS traffic through remaining operational resources. While additional delay may result from the rerouting process, ETS traffic will still have a higher probability of reaching its destination.

G. Preferential use of remaining operational resources for ETS traffic {a}—During disaster events, infrastructure damage and heavy traffic demand can severely limit public telecommunications. Therefore, ETS traffic needs to have preferential use of the appropriate amount of operational infrastructure required to effectively support recovery operations without impeding the inherent traffic flow throughout the connectionless packet network. To this end, a scheme of preferential treatment needs to be defined that will accommodate various types of priority services for authorized users as well as for general public emergency use (i.e.,

911/999/112 emergency calling service). The appropriate balance of traffic flow needs to be maintained to ensure support of emergency traffic while the remaining capacity can be used for nonemergency applications.

H. Preferential completion of ETS traffic to destination {a}—In addition to considering the issue of preferential establishment, routing, and maintaining an ETS communication, it is also necessary to establish provisions to facilitate completion of the emergency communication to the destination terminal. When an end terminal can handle multiple sessions, its inherent packet-multiplexing feature naturally allows the incoming ETS communication to be delivered. When the terminal device can only handle a single session, such as a cell phone, the user needs to receive an overriding indication of an incoming ETS communication. The destination could then suspend nonemergency communications to free bandwidth for the incoming emergency communication. If preemption were an option, nonemergency communications to the destination could be terminated. Should the destination have "call forwarding" initiated, the network should then continue to reroute and process the emergency communication with preferential treatment to the new destination.

I. Optional preemption of nonemergency traffic {a}—ITU-T draft Recommendation F.706 [2] identifies the process and concept of preemption of nonemergency traffic by ETS traffic. While the concept of preemption typically applies to circuit-oriented communications, its application in connectionless packet network services, if determined viable, needs to be studied and defined. The basic ETS provisions do not include the concept of preemption of nonemergency traffic to free bandwidth and resources for emergency traffic. The intent is to have ETS traffic receive basically preferential treatment. If the communication encounters congestion or a blockage, it should be rerouted if possible. Any nonemergency communication in progress is normally allowed to continue until completion. However, some nations or private networks may allow preemption of nonemergency traffic to enable processing of emergency communications. Therefore, in these cases, preemption may be allowed only as an option, which could be invoked as specifically prescribed by that authority.

J. Allowable degradation of service quality for ETS traffic {l} {n}—Various levels of quality of service (QoS) are defined for different applications and modes of operation. Each may have multiple classes from the very best QoS to lesser levels. The QoS for different ETS services would typically be designated as the best available to ensure clear clean communications and conveyance of important information. However, when the telecommunication resources are experiencing severe stress, an allowable degradation of QoS could be acceptable. This would occur only when resources have become unavailable to the point that the network cannot support non-emergency traffic and sufficient bandwidth and resources are

not available to support the normally acceptable QoS level for emergency traffic. Rather than lose the ability to communicate, emergency operations need to continue to convey critical information, even if with difficulty. Any possibility of getting information through is better than none at all. The ETS needs to continue operation when only "best effort" service is available. Therefore a special or supplemental class of QoS for ETS is necessary to define the conditions and terms for allowable degradation of service.

K. Interchange of critical telecommunications service management information {d} {n}—During emergency operations, interaction between the SCs and SPs through sharing of critical information related to availability and status of telecommunication resources would be beneficial. SCs could maintain knowledge of service availability and could provide reports to SPs of service problems and failures. SCs could also have a view of resource configurations supporting the operational needs at hand. SPs would be able to provide reports of status and availability of resources, failure points, recovery notices, and alerts of lost capabilities.

L. When the ETS is only activated during a declared emergency, the SC can directly notify the SP on-line to activate the ETS service for the area impacted. An effective service management interface and a simple data interchange mechanism are needed to provide this important capability.

5. Conclusions

The establishment of meaningful standards to make ETS a reality requires dedicated cooperation and collaboration among industry and Government. Initial ETS capabilities, as defined by ITU-T Recommendation E.106 [1] exist in some nations today and can be deployed in the basic telephone systems that are in place. The evolution of telecommunications technology to provide more effective, efficient, and economical {m} facilities in emerging packet-based networks provides both a challenge in transition and an opportunity to apply greatly enhanced capabilities for a national and an international ETS. Many of the ETS requirements addressed in this paper may already be satisfied without change or addition to existing standards. These capabilities need to be identified and their application to the ETS needs to be defined. Where capabilities for ETS do not exist, new standards or additions to existing specifications in the international standardization process need to be addressed. It is imperative that any specifications include support for the functional requirements of a comprehensive ETS before equipment and systems are designed, manufactured, and deployed. None of these new specifications shall cause change or impairment of operation of existing emergency capabilities or to the basic packet-switched infrastructure. ETS is multidimensional and includes many critical technical issues as well as policy, legal, regulatory, and

operational issues that need to be addressed. Close cooperation between Government and industry will lead to timely establishment or identification of meaningful standards and deployment of ETS capabilities in the evolving telecommunication and 3G mobile networks.

This document is intended to serve as a basis for discussions and development of innovative ideas in standards bodies. The material presented will be further refined as a result of continuing work toward identifying, establishing, and applying a family of comprehensive standards for national and international ETS. Please visit www.iepscheme.net and subscribe to the IEPS email list to track the progress of work.

6. References *(copies available from www.iepscheme.net)*

1. ITU-T, "Description of an International Emergency Preference Scheme," ITU-T Recommendation E.106, March 2000.

2. ITU-T, "Service Definition of an International Emergency Multimedia Service," ITU-T Draft Recommendation F.706, August 2001.

3. ETSI TR 101 300, V2.1.1, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues," October 1999.

Hal Folts, Senior Systems Engineer
Priority Services—Internet Team, Technology and Programs
National Communications System
foltsh@ncs.gov
(703) 607-6186

APPENDIX D

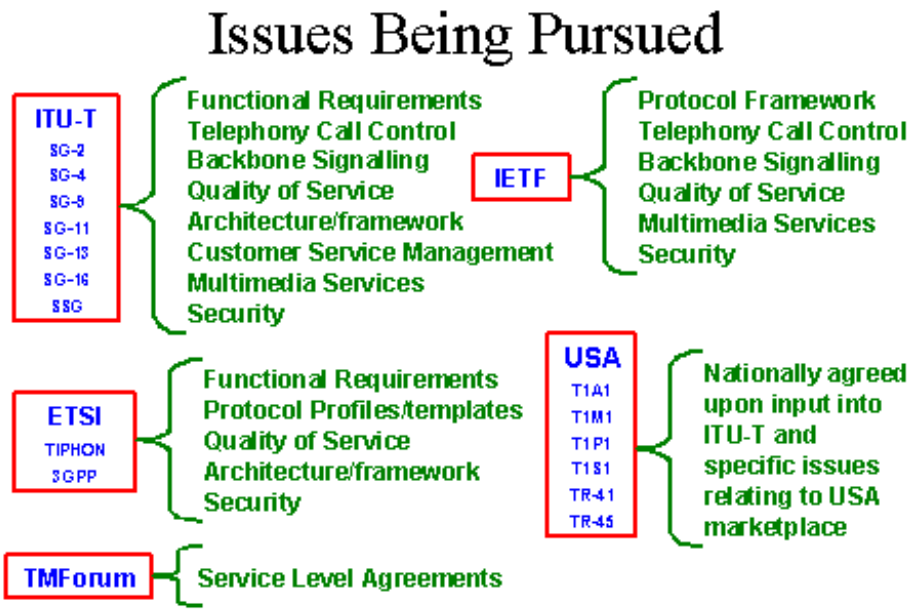
ISSUES FOR STANDARDS DEVELOPMENT BEING PURSUED FOR THE EMERGENCY TELECOMMUNICATIONS SERVICE

V1.0, February 4, 2002

Issues for Standards Development Being Pursued for the Emergency Telecommunications Service

1. Introduction

The Office of the Manager, National Communications System (OMNCS) Technology and Programs Division is pursuing the task of establishing a comprehensive family of standards for an Emergency Telecommunications Service (ETS) in Evolving Networks (EN). This effort is being worked on in cooperation with the telecommunications industry in major national and international standards bodies. This effort addresses the issues of mechanisms in the new protocols and signaling systems to support priority services for preferential handling of ETS communications. This is a multidimensional effort addressing myriad issues that will ensure the provision of a comprehensive and effective ETS in future networks. The issues for transition during a period of convergence from today's telecommunication services to an all packet-based infrastructure of the future are also being addressed. The figure below summarizes the standards activities and issues of focus that are being pursued.



2. Industry Standards Development Organization

2.1 International Telecommunication Union, Telecommunication Standardization Sector (ITU-T)

ITU-T—Seven study groups (SG) have been identified that address various issues related to development of effective and comprehensive standards for the ETS. Each SG has a different, but specific, focus of work. The areas of interest in each SG are—

2.1.1 Study Group 2—Operational aspects of service provision, networks, and performance. SG 2 deals with the following:

- Application of numbering, naming, and addressing plans for fixed and mobile services
- Routing and interworking plans for fixed and mobile networks
- Management and development of voice and nonvoice based telecommunication services
- Human factor issues in international telecommunication services
- Service quality of networks
- Network management
- Traffic engineering for personal communications
- Traffic engineering for SS No. 7- and Internet Protocol (IP) based signalling networks
- Traffic engineering for networks supporting IP services.

SG2 developed Recommendation E.106, *Description of an Emergency Preference Scheme.* This Recommendation applies to emergency services in the public switched telephone network (PSTN), integrated services digital network (ISDN), and public land mobile network (PLMN). SG 2 may also get involved in or be part of the coordination of work on other aspects of the ETS work. No specific contributions or proposals have been submitted at this time. NCS staff participates in this work

2.2.2 Study Group 4—Telecommunication Management, Including Telecommunication Management Network (TMN). SG4 deals with the spectrum of telecommunications management aspects. This is of specific interest to the ETS work in

the development of customer service management interface specification. This would be used by recovery operations activities to monitor the status, report service failures, and interchange critical management information that would facilitate effective communications support. Draft Recommendation Mets, *Network and Service Management Requirements for Information Interchange Across the TMN X-interface for the International Emergency Telecommunications Service (ETS)*, is under development to specify the operational requirements. Then work is needed to identify the appropriate interface protocol to be used and to define specific data elements that would be unique to ETS operations. This capability can also be adapted for application to support the Information Sharing and Analysis Center (Telecom-ISAC). NCS staff participates in this work.

2.2.3 Study Group 9—Integrated broadband cable networks and television and sound transmission. SG9 deals with the aspects of integrated voice, video, and data over cable networks. SG 9 has already developed a number of J-Series ITU recommendations that address services for cable networks. Most of these recommendations stem from the IPCablecom project, which focuses on standardizing time-critical interactive services using IP technology. The work of SG 9 and the resources available from cable networks could directly benefit ETS. Given the various issues and complexity of the new technical area of cable networks for ETS, both staff of the Institute of Telecommunication Sciences (ITS) and NCS are jointly participating in this work.

2.2.4 Study Group 11—Signalling requirements and protocols. SG11 deals with basic signalling systems for telecommunication networks. The critical issues here are getting an international code point established for ETS services in Signalling System Number Seven (SS7) and the Bearer Independent Call Control (BICC) specifications. In addition, an appropriate interface needs to be specified that will interface SS7 and BICC with the new packet-based networks that will be supporting telephony and multimedia services in the future. Contributions are being developed to provide specific proposals. This work is being supported by AG Communication Systems (AGCS) under an NCS contract with Science Applications International Corporation (SAIC).

2.2.5 Study Group 13—Multiprotocol and IP-based Networks and Their Internetworking. SG13 deals with a number of issues under the IP project that are associated with the ETS.

The ETS white paper, *Emergency Telecommunication Service in Next-Generation Networks,* was submitted to the Q1/13 work in frameworks and architecture. They prepared a draft Recommendation Y.roec (Recommendation on Emergency Communications), *Framework(s) on Network Requirements and Capabilities to Support*

Emergency Communications Over Evolving Circuit-Switched and Packet-Switched Networks. This draft incorporated the majority of the material in the white paper. The more general term "emergency communications" was used because SG13 does not deal with specific services. It can be considered that the ETS supports emergency communications. Other issues that will be pursued in this group will be interworking (Q5/13) and service performance (Q6/13). NCS staff participates in this work.

2.2.6 Study Group 16—Multimedia services, systems, and terminals. SG16 deals with all aspects of multimedia communications including IP-telephony. H.323 is the principal call control and signalling protocol, and H.248 specifies the traffic gateway. The first recommendation produced is draft F.706, *Functional Requirements for an International Emergency Multimedia Service to Support Critical Communications*. This recommendation should be approved at the full SG16 meeting in February 2002. Three additional recommendations are currently under development.

The first recommendation is the second Draft H.GEF.4 (to be H.460.4), Service Class designations for H.323 Calls. It provides the mechanism for identifying and processing ETS communications. It is hoped that the draft will start the approval process at the February 2002 meeting of SG16. Delta Systems, under NCS contract, has been supporting this issue and serves as editor of the recommendation.

The second recommendation is H.priority, Techniques, and Procedures for Controlling Service Priority. The session priority categorization specified may be used by service providers and operators to specify service class and in the context of different service types. This will allow a session (e.g., call) to be given preferential treatment during session setup and routing. NCS staff is supporting this issue.

The work for developing the third recommendation on security for the ETS was agreed upon and a new work item was added to Question G/16. Support through NCS contract with SAIC will now prepare a draft from this contribution, which was submitted to the meeting. The SAIC representative was appointed editor for this work.

2.2.7 Special Study Group (SSG)—SSG "International Mobile Telecommunications 2000 (IMT-2000) and Beyond." The SSG deals with the network aspects of the next generation of standards for wireless communication services. The SSG is working with the ITU Radio Standardization Sector (ITU-R), Working Group 8F, on development of a joint vision for IMT-2000 and Beyond. This work will include interworking, harmonization, and convergence requirements and aspects for IMT-2000 systems. ETS requirements have been introduced to the SSG for inclusion in the work. NCS staff participates in this work.

2.3 Internet Engineering Task Force (IETF)

The IETF is an international activity that develops standards and specifications applicable to the Internet. They primarily deal with very specific issues and do not concern themselves with systems, service, or architectural aspects. Several ETS-related contributions have been submitted in the form of Internet-Drafts (ID). There are currently four active IDs addressing ETS aspects. The first ID proposes a framework for various IETF protocols for call control and backbone signalling to support ETS communications. The second ID proposes how the IETF IP Security (IPSec) specification for security should be applied to ETS communications to support authentication and integrity of sessions. The third ID is the ETS white paper, *Emergency Telecommunications Service in Next-Generation Networks*. The fourth ID is proposed for an ETS class of traffic to be identified in the Real-Time Protocol (RTP). All four of the IDs will be processed as informational requests for comment (RFC), which is the term the IETF uses for formalized, agreed-upon documents. Issues of quality of service and multimedia specifications, including presence and instant messaging will be pursued for the ETS in the IETF Internet environment.

2.4 European Telecommunications Standards Institute (ETSI)

ETSI has opened some of its areas of work as international activities. One area is Project TIPHON (Telecommunication and Internet Protocol Harmonization over Networks) to deal with interworking issues during the period of convergence when the PSTN transitions to an IP-based packet infrastructure. The other is Project 3GPP (Third Generation Project Partnership) is dealing with development of the future wireless standards.

2.4.1 TIPHON—In the Project TIPHON work, the requirements for the ETS have been successfully introduced and adopted. TIPHON works in progressive stages called Releases. Release 3 has just been completed and includes identification of the basic provisions for the ETS in their technical specification 1008/1009, requirements, and 3016, protocol profiles. A major work item (WI) has been approved for the ETS issues in Release 4 and Release 5. The ETS WI calls for development of a two-part document: Part 1 specifies the requirements for a comprehensive and global, and Part 2 will be a detailed systems description of how the ETS requirements are being fulfilled by specific standards.

Work on Release 4 has now begun. Specific contributions ETS have been provided on ETS in ENs, ETS security, and ETS quality of service. The issue of protocol profiles and

templates for ETS will also be pursued in Release 4. NCS staff and an NCS contract with SAIC support this work.

2.4.2.3 GPP—The Project 3GPP work is a very intensive and extensive activity to develop a new family of standards for the next-generation wireless capabilities. The NCS successfully introduced the ETS requirements into a 3GPP work item. Work is progressing on a feasibility study. Upon completion of this work, it is anticipated that change requests to existing Global System for Mobile Communication (GSM) and 3G standards and work items will be initiated to satisfy ETS requirements. NCS staff participates in the 3GPP activity.

2.4.3 New Work—ETSI is also considering the establishment of a new technical committee on Next Generation Networks (NGN). It may absorb the work of TIPHON and have a more comprehensive work program to address myriad issues in NGNs (or EN).

2.5 USA Standards Activities

The primary participation in the USA standards activities is to reach a national consensus on the many issues that are being introduced into the international standards bodies. As this work is being done in partnership with the U.S. telecommunications industry, it is imperative that a common understanding of the issues is reached and participation in the international work is consistent.

2.5.1 T1—Telecommunications—is the North American body to support standardization in the telecommunications industry. This activity is sponsored by the Alliance for Telecommunications Industry Solutions (ATIS) and is accredited as an American National Standards Committee by the American National Standards Institute (ANSI). T1 has a number of subcommittees that address many issues for the ETS.

2.5.1.1 T1A1—Performance and Signal Processing. T1A1 deals with issues of security, network integrity, and quality of service. This subcommittee is processing the ETS white paper, *Emergency Telecommunications Service in Next Generation Networks*, as a technical report to serve as a basic reference for the ETS work in the various T1 subcommittees. They will also be addressing issues related to quality of service for ETS communications. T1A1 does not directly interface with the ITU-T. NCS staff does not regularly participate in this subcommittee.

2.5.1.2 T1M1—Internetwork Operations, Administration, Maintenance, and Provisioning (IOAM&P). T1M1 deals with issues related to management of the telecommunications

services and infrastructure. There is now a formal project established to address several ETS issues in their work. T1M1 is the U.S. interface with ITU-T SG 4. The first issue currently being addressed is the development of M.ets, Network and Service Management Requirements for Information Interchange Across the TMN X-interface for the International ETS. A new technical issue to be addressed by T1M1 is the Telecom-ISAC interface with the telecommunication service providers for interchanging and sharing of critical management information. A third issue will be the updating of the standard T1.211 on Telecommunications Service Priority (TSP) and its applicability in the EN service-oriented environment. The fourth issue addresses management controls during traffic congestion periods. The current standard T1.202 specifies that GETS traffic is exempt from management controls. A revision to this standard will be considered for applicability to new packet-based networks. NCS staff participates in this activity.

2.5.1.3 T1P1—Wireless/Mobile Services and Systems. T1P1 deals with the many issues associated with wireless telecommunication services. It provides the U.S. interface with the ITU-T SSG and 3GPP. Issues of priority access and call processing are addressed in this subcommittee. ETS requirements were socialized in T1P1 and were forwarded to both the ITU-T SSG and 3GPP. In addition, this group forwarded the requirements for information to GSM North America, a closed forum for North American wireless operators and their manufacturers. NCS staff participates in this activity.

2.5.1.4 T1S1—Services, Architectures, and Signaling. T1S1 deals with the PSTN signalling system issues and the interface with IP telephony services in the ENs. This subcommittee is the U.S. interface with the work in SG 11 and SG 13. NCS N2 staff and experts under NCS contract with AGCS through SAIC participate in this activity.

2.5.2 TIA—Telecommunication Industry Association (TIA)—is a leading association in the telecommunications and information technology industry. Two TIA technical standards groups in TIA, TR41 and TR45, are addressing issues related to the ETS. In the future, these TIA standards groups may merge their standards development with Telecommunications Committee T1 standards development activities.

2.5.2.1 TR-41—User Premises Telecommunications Equipment Requirements. TR-41 deals with standardizing network interfaces from a terminal equipment perspective. TR41's current standards development centers on two types of interfaces: interfaces to enterprise networks, and interfaces to users. A current TR41 industry standards project, IP Telephony Support for Emergency Calling Service (e.g., E911), is addressing requirements for an enterprise IP network to properly support emergency calling services. The identification of specific issues in TR41 to address ETS using the

resources of enterprise networks is still under development.

2.5.2.2 TR-45—Mobile and Personal Communications Public 800 Standards. TR-45 deals with the many issues associated with wireless communications. This activity interfaces with the international work on this subject. It also overlaps with the activities of T1P1. NCS staff participates in this activity.

2.6 TeleManagement Forum (TMForum)

The TMForum is a large industry consortium with a membership of approximately 250 organizations from more than 30 countries. The Forum specifically addresses implementation and interoperability issues of the operating support systems (OSS) for management operations of the telecommunications infrastructure. One Forum activity of significant interest to the ETS work is the development of an industry handbook for service level agreements (SLA). This handbook provides a mechanism to clearly address Quality of Service issues and certain responsibilities of both service providers and service customers with respect to "delivered services" and customer requirements in the new emerging telecommunications business environment. Edition 1 of the handbook was published in early 2001. Edition 2 is under development with provisions for the ETS as an "extension" of normal services to preclude any potential need for expensive service provider retrofitting. The services will then be obtained for supporting emergency recovery operations through the execution of specific SLAs for the ETS. NCS staff and support from NCS contract with Telcordia through SAIC participate in this activity.

3. Conclusions

The multidimensional effort addresses myriad issues in many industry activities to establish a comprehensive family of industry standards for an effective ETS. Over the past year considerable progress has been made. The basic groundwork has now been laid. However, there is still much to be done through effective use of limited resources and good cooperation with industry. The process of developing standards is one of consistent participation in the work, persistence to put forth and promote the issues, and patience for the details to be worked out and agreed upon through industry consensus.

APPENDIX E

LEGISLATIVE AND REGULATORY TASK FORCE REPORT

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

LEGISLATIVE AND REGULATORY TASK FORCE REPORT

Will the Current Legal and Regulatory Environment Ensure the Availability of National Security and Emergency Preparedness Services in the Converging and Next Generation Network Environments?

March 2002

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Convergence is a 3- to 5-year period of evolution in the public network (PN) during which traditional circuit-switched networks and Internet Protocol (IP) based data networks coexist and interoperate to enable end-to-end transmission of voice communications until packet-based networks subsume circuit-switched networks.[1] Currently, the national security and emergency preparedness (NS/EP) community depends on the priority treatment of voice calls and voice services within the PN to support NS/EP operations. Emerging next generation network (NGN)[2] technologies, such as IP packet-switched services, are also now essential to support NS/EP operations as well as advanced technologies, such as wireless, satellite, and broadband. It is important to examine the current policy environment to determine whether the legal and regulatory structure is adequate to ensure availability of NS/EP services in the converging and NGN environments, or if the current laws and regulations need to be revised. To that end, the President's National Security Telecommunications Advisory Committee's (NSTAC) Legislative and Regulatory Task Force (LRTF) examined these legal issues and has documented its analysis in this report.

In January 2001, NSTAC's Industry Executive Subcommittee (IES) tasked the Legislative and Regulatory Working Group (LRWG), which subsequently became the LRTF, to examine whether existing legal and regulatory authority will adequately ensure the availability of NS/EP services in the converging and NGN environments, and to identify and address related issues.
Specifically the IES recommended that four issues be addressed—

- Is additional legal authority required to ensure NS/EP services in the converging and NGN environments?

- What is the proposed legal basis for NGN priority service (i.e., packet) obligations?

- Is authority available for wireless providers to provide NS/EP services and are new or revised legislation and/or executive orders required for NS/EP services in the converging and NGN environments?

- Are potential antitrust protections necessary for cooperation among service providers of NS/EP services in the NGN?

The LRTF came to the following conclusions—

- Existing legal statutes ensure that NS/EP priority services can be provided over the circuit-switched network. Ambiguity arises, however, when these rules are applied to ensure NS/EP services in the converging and NGN environments. The terrorist attacks of September 11, 2001, have reiterated the value of NS/EP communications services.

- The Federal Communications Commission (FCC) is authorized in peacetime to allow priorities that are not "undue" or "unreasonable." This authority allows for NS/EP priority programs such as the Telecommunications Service Priority (TSP) System, the Government Emergency Telecommunications Service (GETS), the Special Routing Arrangement Service (SRAS), and the Priority Access Service (PAS).

- While GETS applies to voice NS/EP services, there are several initiatives under discussion, e.g., GovNet,[3] which would enhance IP packet NS/EP services. IP packet services are becoming increasingly essential to NS/EP operations.

- The TSP rules neither disallow their application to the converging and NGN

environments nor necessarily apply in these environments.

- The Telecommunications Act of 1996, which amended the Communications Act of 1934, introduced a differentiation between telecommunications and information services just as the two systems were merging. This creates uncertainty as to whether new technologies are within the FCC's regulatory purview and whether the FCC currently has authority over Internet Service Providers (ISP) and noncommon carriers.

- Rapid evolution in technology fosters ambiguity as to what type of services will be necessary for NS/EP operations in the NGN environment.

- The LRTF recognizes that many national and international standards bodies are considering what NS/EP related functions could—or should—be recommended for Internet-based NS/EP services.[4] The task force continues to monitor the work of those groups, specifically those focusing on priority packet-based services.

- Authority is available for wireless providers to provide NS/EP services based on the Wireless PAS, which allows the wireless community to offer such services voluntarily. However, the rules are tied too closely to technology and can become outdated very quickly.

- Ensuring interoperability among multiple wireless carriers using different standards in their networks is complicated and may require significant additional work to address the technical reliability and interoperability of these multiple networks. This is a goal that should be pursued.

- The LRTF has not identified specific antitrust issues at this time regarding the provision of NS/EP services in the NGN by service providers.

Until the standards for packet-based services are established, including provisions for the Emergency Telecommunications Service (ETS),[5] and the Government's requirements in the evolving environment are certain, legislation or regulation is premature. This creates difficulty in determining whether additional legal authorities will be necessary to ensure NS/EP services in the NGN. In the meantime, traditional methods for providing NS/EP services should not be abandoned. The LRTF has responded to its tasking to address convergence issues based on the standards and requirements that are currently available and can reexamine this issue when the standards and requirements are more clearly defined or if given additional taskings on the subject. This report serves as a framework for further analysis of the legal authority for NS/EP services in the converging and NGN environments.

1.0 introduction and CHARGE

The public network (PN), which includes any switching system or voice, data, or video transmission system used to provide communications services to the public, once consisted primarily of the narrowband, mature, public-switched telephone network (PSTN), including access to the Internet. The PN is now transforming from separate switched voice and packet data networks to an interconnected network. Eventually, the PN will become a unified next generation network (NGN).[24] This transition process, termed *convergence*, is a 3- to 5-year period of PN evolution during which traditional circuit-switched networks and Internet Protocol (IP) based data networks coexist and interoperate to enable end-to-end transmission of voice communications until packet-

based networks subsume circuit-switched networks.[25]

National security and emergency preparedness (NS/EP) services help ensure critical communications, and the terrorist attacks of September 11, 2001, have reiterated their importance. Currently, the NS/EP community depends on the priority treatment of voice calls and voice services within the PN to support NS/EP operations. Emerging NGN technologies, such as IP packet-switched services, are also now essential to support NS/EP operations as well as advanced technologies, such as wireless, satellite, and broadband. Projections also indicate that reliance on Internet-based services will continue to grow as the NGN evolves. As a result of newness of many technologies that support the Internet, questions have arisen about whether or when NGNs will be as reliable and predictable as their circuit-switched predecessors.[26] Therefore, the PSTN remains, and will remain, critical to the provisioning of priority NS/EP services until the technical uncertainties relative to the NGN are resolved.

Other National Security Telecommunications Advisory Committee (NSTAC) task forces have addressed and continue to examine the technical, security, and vulnerability aspects of convergence. For example, the NSTAC Convergence Task Force (CTF) addressed technical issues in its July 2001 report, and the Network Security/Vulnerability Assessment Task Force (NS/VATF) is currently addressing the technical issues related to convergence. It is important, however, to also examine the current policy environment to determine whether the legal and regulatory structure is adequate to ensure availability of NS/EP services in the converging and NGN environments, or if the current laws and regulations need to be revised. To that end, the NSTAC's Legislative and Regulatory Task Force (LRTF) examined these legal issues and has documented its analysis in this report.

1.1 Background

At the January 2001, meeting of the NSTAC's Widespread Outage Consequence Management Scoping Group (WOCMSG), the group recommended that the Legislative and Regulatory Working Group (LRWG), which subsequently became the LRTF, be tasked to address legal authorities related to NS/EP services in the converging and NGN environments. This recommendation was defined in the January 2001, "NSTAC IES Issue Evaluation Form of the WOCMSG." Acting on this recommendation, the IES tasked the LRWG to examine whether existing legal and regulatory authority will adequately ensure that NS/EP services will be available in the converging and NGN environments, and to identify and address related issues.

Specifically the IES recommended that four issues be addressed—

- Is additional legal authority required to ensure NS/EP services in the converging and NGN environments?

- What is the proposed legal basis for NGN priority service (i.e., packet) obligations?

- Is authority available for wireless providers to provide NS/EP services and are new or revised legislation and/or executive orders required for NS/EP services in the converging and NGN environments?

- Are potential antitrust protections necessary for cooperation among service providers of NS/EP services in the NGN?

This report presents the LRTF's response to these issues.

1.2 Approach

LRTF members, subject matter experts from their respective companies, and Government participants contributed to this effort. Annex A provides a list of task force members, Government, and other participants.

1.3 Scope of Study

The LRTF's jurisdiction in this tasking is to address only the legal and regulatory aspects of providing NS/EP services in the converging and NGN environments. As previously mentioned, the NSTAC's CTF and NS/VATF have addressed and continue to examine the technical, security, and vulnerability aspects of convergence. In addition, the Telecommunications Service Priority (TSP) Oversight Committee[27] is responsible for reviewing convergence issues specific to TSP, and it has reviewed the paper entitled, *Priorities in a Converged/Next Generation Network*, submitted by Office of the Manager, National Communications System (OMNCS) Counsel and attached as Annex B.

The LRTF has focused its analysis on the legal issues related to convergence, based on its tasking by the IES, and has centered its discussion around examining the four issues raised. The LRTF was not tasked to respond to issues raised by the Government's Convergence Interagency Working Group (IWG), which identified a need for the Government to review specific laws. In keeping with its focus, the LRTF refrained from reviewing specific laws; however, this report provides a brief background on the most relevant laws as a framework for discussion.

2.0 LEGAL ISSUES SURROUNDING CONVERGENCE

2.1 Overview of Current Legal and Regulatory Environment

Existing legal statutes ensure that NS/EP priority services can be provided over the circuit-switched network. Ambiguity arises, however, when these rules are applied to ensure NS/EP services in the converging and NGN environments. Executive Order 12472 of April 3, 1984, references several laws as authorities for assigning NS/EP preparedness telecommunications functions to various Government agencies. One of the primary authorities is the Communications Act of 1934, as amended (47 U.S.C. 151 et seq.), which provides for the regulation of interstate and foreign commerce in communication by wire and radio and gives the Federal Communications Commission (FCC) the authority to regulate such communication.

- Title II of the Act mandates that common carriers[28] not make:

  undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage.[29]

- However, Section 606 of the Act states that:

  during the continuance of a war in which the United States is engaged, the President is authorized, if he finds it necessary for the national defense and security, to direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier subject to this Act.[30]

Therefore, for the purpose of national security, the President is permitted to prescribe priorities for Government communications. Moreover, the FCC, which executes and enforces the provisions of the Act, is authorized in peacetime to allow priorities that are not "undue" or "unreasonable." This authority allows for NS/EP priority programs such as the TSP System, the Government Emergency Telecommunications Service (GETS), the Special Routing Arrangement Service (SRAS), and the Priority Access Service (PAS).

The FCC organization includes a Defense Commissioner, who has the specific duties of ensuring continuity of the Commission's NS/EP functions and of approving NS/EP plans and programs (including the provision of service by common carriers).[31] The rules

governing the FCC (47 C.F.R. § 1.925) provide that the FCC may waive specific provisions in its rules on its own motion or upon request.

As a result of this provision, the FCC, possibly at the recommendation of the defense commissioner, could waive its rules to better ensure NS/EP functions during a crisis.

The Telecommunications Act of 1996, which amended the Communications Act of 1934, differentiates between telecommunications services and information services. This distinction creates uncertainty as to whether the FCC currently has authority over Internet Service Providers (ISP) and noncommon carriers as well as whether new technologies are within the FCC's regulatory purview.

The TSP Report and Order, which establishes the TSP System, allows telecommunications service vendors to provide priority treatment to NS/EP telecommunications services and ensures that such vendors are not violating Title II, Section 202 of the Communications Act of 1934 when doing so.[32] The TSP System operates primarily within the circuit switched network environment; therefore, it is unclear whether the TSP rules are sufficient to provide NS/EP services in the converging environment and eventually in the NGN. The TSP System is explored in depth in the following discussion and in Annex B.

2.2 Issues Addressed

The LRTF considered four legal issues regarding NS/EP services in the converging and NGN environments. This section summarizes the LRTF's initial analysis of these issues.

2.2.1 Is Additional Legal Authority Required To Ensure NS/EP Services in the Converging and NGN Environments?

The current rules and other procedures provide sufficient legal authority for NS/EP services. The TSP Report and Order, for example, allows for priority service in the traditional network environment. A bit of background is necessary, however, to understand certain challenges that exist when the TSP Order is applied to advanced services provided by ISPs. When the TSP Report and Order was adopted in 1988, the FCC envisioned evolution of telecommunications technology; therefore, it made the rules flexible by allowing carriers and users to "determine jointly the feasibility and availability of services that can be restored under a TSP priority."[33] The TSP rules neither disallow their application to the converging and NGN environments, nor do they necessarily apply in this environment. This ambiguity arises because TSP traditionally

has been applied to physically identifiable circuits and equipment. However, priority treatment of packet-switched transmissions, characteristic of the converging and NGN environments, is very different from that of circuit-switched transmissions. Packet-switched transmissions are highly distributed throughout the network, and as they travel through the network "cloud," they are physically identifiable only at each end piece. While TSP could apply to services that use the network cloud for transmission, such as the case with frame relay,[34] priority treatment within the network cloud is difficult under the methods envisioned in the TSP rules. This creates uncertainty as to whether the rules can be, or practically need to be, applied to the converging and NGN environments. Also, the current TSP rules mandate only that common carriers provide TSP services.[35] Thus, these rules do not provide the FCC with the authority to enforce them for noncommon carriers, such as ISPs. However, those noncommon carriers that elect to participate in the TSP program may consent to be bound by the TSP priority requirements. Uncertainty exists when considering to what degree the Government could require noncommon carriers to provide advanced services for NS/EP purposes if those carriers have not consented to be bound.

The Telecommunications Act of 1996 created further uncertainty because it introduced a differentiation between telecommunications and information services just as the two systems were merging. The 1996 Act also clearly regulates common carriers but is ambiguous as to its authority over the noncommon carriers that provide information services. This differentiation has clouded whether new rules will be needed. Moreover, the concept of applying additional regulations, particularly to noncommon carriers, is highly contentious.

Adding to the uncertainty is the rapid evolution in technology, which is characteristic of the converging network. This evolution fosters ambiguity as to what type of services will be necessary for NS/EP operations in the NGN environment. At least three possibilities exist—

- The Government may eventually find that a priority treatment for packet services will be necessary.

- The Government may find that priority treatment for packet services will not be necessary because the NGN design and implementation will provide sufficient capacity and redundancies to allow the NS/EP community to rely on the network itself to ensure NS/EP services.

- The Government and other users of NS/EP services may prefer to ensure NS/EP

communications by implementing a completely new program. While GETS applies to voice NS/EP services, there are several initiatives under discussion, e.g., GovNet,[36] which would enhance IP packet NS/EP services.

Because the NGN characteristics are still evolving and the Government's requirements in the evolving environment are uncertain, it is premature and inappropriate at this time to determine whether additional legal authorities will be necessary to ensure NS/EP services in the NGN.

2.2.2 What Is the Proposed Legal basis for NGN Priority Service (i.e., packet) Obligations?

As mentioned previously, the current rules provide legal authority to allow priority treatment, but as telecommunications and information services merge, the practical application of priority over packet-based services in the NGN becomes speculative.

The TSP rules are flexible because they mandate that "the NS/EP TSP System may apply, at the discretion of and upon special arrangements by the NS/EP TSP System users involved, to authorize priority treatment …to Government or non-common carrier services."[37] The Government can, therefore, contract for services, especially for noncommon carrier services with an ISP. Provisioning services via contracts may help to ensure availability of NS/EP services in the NGN, but commercial contracts may not guarantee priority NS/EP services, unless those service level agreements (SLA) in contracts provide for an allowable degradation in quality of service for qualified NS/EP users. Although SLAs require a user to pay more for higher service, this arrangement offers no guarantee that service providers will act in the public's best interest and give priority to NS/EP contracts over those between service providers and favored commercial customers. The TSP rules also allow common carriers to preempt services to provide NS/EP priority services without exposure to liability regarding Section 202 of the Communications Act of 1934.[38]

Conversely, while the rules are flexible, they are not directly applicable to NGN services that exist in the network cloud, as described in Section 2.2.1. Also, within the TSP Order, "carriers are not required to include services under TSP that they cannot provide."[39] It might not be economically or technically feasible for the Government to assign priority to packets associated with NS/EP services and under the TSP rules, and it is not necessary to provide end-to-end priority service delivery. Technology and standards are still evolving; it is apparently not yet feasible to tag individual packet services for end-to-end priority treatment. This is because each domain that the packet

travels through may classify and treat the packet differently, making completely reliable end-to-end priority routing nearly impossible. Until interdomain quality of service is achieved, end-to-end packet priority will not be completely feasible.[40] (See "RFC 3086: Definition of Differentiated Services Per Domain Behaviors and Rules for Their Specification," April 2001,[41] and "RFC 2474: Definition of the Differentiated Services Field [DS Field] in the IPv4 and IPv6 Headers," December 1998[42] for additional details on the technical background). Under the existing TSP rules, if the providers cannot feasibly provide such services, the Government cannot mandate them to do so. Even if the technical difficulties can be overcome, the costs to engineer and implement such an end-to-end capability and priority through the cloud will have to be considered as they may be excessive.

The LRTF recognizes that many national and international standards bodies, including the Internet Engineering Task Force, T1M1[43], and the International Telecommunication Union, are considering what NS/EP-related functions could—or should—be recommended for Internet-based NS/EP services. Establishing these functional requirements could then shape the standards for packet-based services that help support NS/EP services in the converged and NGN environments.[44] In the national standards bodies and international organizations, efforts are under way to identify, establish, and apply a comprehensive family of ETS standards for new packet-based networks.[45] The task force continues to monitor the work of those groups, specifically those focusing on priority packet-based services. Until the functional requirements for packet-based services are developed and are translated into fully established standards, legislation or regulation is premature. In the meantime, traditional methods for providing NS/EP services should not be abandoned because as originally conceived, TSP remains relevant during convergence because restoration assignments can still be applied to identifiable segments of the PN.[46]

In light of these factors, the LRTF concludes that it is uncertain whether there is sufficient legal basis to ensure NS/EP priority services in an NGN environment.

2.2.3 Is Authority Available for Wireless Providers To Provide NS/EP Services and Are New or Revised Legislation and/or Executive Orders Required for NS/EP Services in the Converging and NGN Environments?

The President's NSTAC issued a report in 1995 that addressed the issue of priority access for cellular services and recommended that a CPAS be established. As a result, President Clinton tasked the National Communications System (NCS) to explore this issue and suggest a course of action for implementing the new access service. Following the

recommendations from the NCS to implement a cellular priority access service, the FCC issued a Report and Order that established the Wireless PAS on July 13, 2000. This report established the guidelines and requirements for implementation for carriers if they voluntarily provided NS/EP services for wireless customers. The FCC did not mandate provision of this service. Although PAS allowed wireless carriers to provide priority treatment of wireless calls for NS/EP users, it did not guarantee reliability of the wireless network.

As a direct result of the September 11, 2001, terrorist attacks in the United States, the NCS determined that priority wireless services were needed immediately. Recently, the NCS entered into negotiations with wireless providers to grant Federal officials wireless priority in Washington, DC, and New York City, New York, during times of national emergencies. Salt Lake City, Utah, would have also received wireless priority access because it hosted the Winter Olympics in February 2002. The FCC would need to grant a waiver of the existing priority access rules it had passed just last year because those rules were already technically obsolete. Thus, while the LRTF concludes that authority is available for wireless providers to provide NS/EP services based on the FCC's recent Report and Order, which allows the wireless community to offer such services voluntarily, it also concludes the rules are tied too closely to technology and can become outdated very quickly.

The task force notes that telecommunications technology is evolving so rapidly that it is not only very difficult for a governing body to adopt orders and implement rules for NS/EP services in this environment but also probably inappropriate to tie rule making to technology rather than indicate the objective and specify time frames for compliance. Further, it is extremely difficult to ensure that NS/EP wireless services will be available during an emergency situation or crisis because several wireless standards exist in the United States. Ensuring interoperability among multiple wireless carriers using different standards in their networks is complicated and may require significant additional work to address the technical reliability and interoperability of these multiple networks. This is a goal that should be pursued.

2.2.4 Are Potential Antitrust Protections Necessary for Cooperation Among Service Providers of NS/EP Services in the NGN?

The antitrust laws are a collection of Federal and State statutes that have been enacted and interpreted in many court decisions over the past 90 years. The essential objective of the antitrust laws is to prohibit actions that prevent or unfairly restrict competition in the marketplace. The principal Federal antitrust laws are the Sherman Act, the Clayton Act,

the Robinson-Patman Act, and the Federal Trade Commission Act. The antitrust laws were adopted to protect markets and prevent restriction of access to services. The FCC has established a precedence for traditional common carriers to provide priority provisioning restoration of NS/EP services. However, as indicated above, these rules are not mandatory for the noncommon carriers, such as the ISPs. Given that the ISPs voluntarily undertake to provide information services on a priority basis to the Federal Government, there may be some concern that they will expose themselves to claims of violating the antitrust laws.[47] Though this may be true, the LRTF has not identified specific antitrust issues at this time regarding the provision of NS/EP services in the evolving environment by service providers.

3.0 conclusions

The LRTF concludes that the legal issues underlying the provisioning of NS/EP priority services to the Federal Government in an NGN environment are extremely complex and require further study. Whether the existing rules and procedures remain applicable to NGN services is extremely ambiguous. This uncertainty stems from the fluctuating nature of the transition from the PN to the NGN and the as as-yet undefined Government requirements for ensuring NS/EP services in the NGN. Although such ambiguity poses potential problems, it can also be beneficial because it can allow for flexibility of interpretation within the existing rules, thus enabling priority services to apply to the more advanced technologies in the converging and NGN environments. A certain degree of ambiguity, therefore, can be desirable until the evolving technology of the converging and the NGN environments can be defined with greater precision. On the other hand, uncertainty poses the risk that NS/EP services cannot be guaranteed to authorized NS/EP users. Additional legal authority may be necessary to minimize the ambiguity. In sum, the LRTF concludes that until the standards for packet-based services are fully established, it is premature to determine what legal authority will be necessary to support future NS/EP functions. The LRTF has responded to its tasking to address convergence issues based on the standards and requirements that are available and can reexamine this issue when the standards and requirements are more clearly defined or if given additional taskings on the subject. This report serves as a framework for further analysis of the legal authority for NS/EP services in the converging and NGN environments.

ANNEX A

Task Force Members, Government, and Other Participants

TASK FORCE MEMBERS

TRW	Mr. Tim Nagle, Chair
Telcordia Technologies	Ms. Louise Tucker, Vice-Chair
AT&T	Mr. Harry Underhill
BellSouth	Mr. Shawn Cochran
Boeing	Mr. Robert Steele
CSC	Mr. Guy Copeland
EDS	Mr. Dale Fincke
Global Crossing	Ms. Renee Bennett
Hughes Electronics	Ms. Jennifer Rougeau
Lockheed Martin	Mr. Christopher Myers
Qwest	Mr. James Payne
Raytheon	Mr. Thomas O'Connell
Rockwell Collins	Mr. Ken Kato
SBC	Ms. Rosemary Leffler
Unisys	Mr. Dan Wiener
USTA	Mr. Fred Tompkins
Verizon Communications	Mr. Lowell Thomas
WorldCom	Ms. Cristin Flynn

OTHER PARTICIPANTS

CSC	Mr. Daryl Savage
GWU	Dr. Jack Oslund
Qwest	Ms. Jane Kunka
Qwest	Mr. Jon Lofstedt
Qwest	Mr. Tom Snee
SAIC	Mr. Hank Kluepfel
Verizon Communications	Ms. Ernie Gormsen

GOVERNMENT PARTICIPANTS

DISA Counsel	LtCol Keith Alich
NCS Counsel	Mr. Paul Schwedler
OMNCS	Col Dave Crafton

ANNEX B

"Priorities in a Converged/Next Generation Network" Submitted by OMNCS Counsel

Priorities in a Converged/Next Generation Network

Issue:

Do current Federal Communications Commission (FCC) rules and regulations regarding priorities afforded national security and emergency preparedness (NS/EP) customers remain valid and relevant in a converged or next generation network?[48]

Conclusion:

Changes in network technology (such as packet switching) do not affect the legal basis of the rules for Telecommunications Service Priority (TSP) or the basis for the Government Emergency Telecommunications Service (GETS). While the rules remain legally effective, their relevance in a converged/next generation network is questionable because: 1. The rules do not require traditional carriers to provide a service the carrier has no technical ability to provide and 2. The FCC regulatory status of nontraditional service providers (such as Internet Service Providers[ISP]) is unclear. However, if technically feasible, participation in TSP on a voluntary basis by ISPs is not precluded.

Discussion:

The Communications Act of 1934, as amended, precludes common carriers from affording any unreasonable or unjust priority to customers.[49] Common carriers have therefore been understandably reluctant to provide services to customers if those services could be construed as illegal priorities or preferences. Before carriers would agree to provide priority types of services to Government customers, the FCC was asked to determine if the service contemplated would be construed as a violation of the Communications Act. Only after a Commission determination of "no violation," was the service offered.

In previous years, two types of priorities had been "blessed" by the Commission. Both have been replaced. *Precedence System for Public Correspondence Services Provided by the Communications Common Carriers*, 34 Fed. Reg. 17292 (1969) and *Priority System for the Restoration of Common Carrier Provided Intercity Private Line Services*, 77 FCC 2d 114, 81 FCC 2d 441 (1980). The Precedence System was based on manual operator intervention to ensure priority treatment in the public-switched network (PSN) on a call-by-call basis. The Restoration Priority System established a uniform system of priorities for the restoration, during emergency situations, of vital intercity private line telecommunications services provided by common carriers. The Restoration Priority

System was replaced by the TSP System. GETS replaced the Precedence System.

Telecommunications Service Priority:

In 1987, the National Communications System (NCS) filed a petition for rulemaking at the Commission seeking establishment of the TSP system.[50] The Petition stated that the existing Restoration Priority System did not apply to the provisioning of new service; that it applied only to intercity private lines, excluding both public switched services and private lines, which were not "intercity", that its administration and management were flawed, and finally that:

> "… the recent, vast changes in the structure of the telecommunications industry mean that the fundamental premises on which the Restoration Priority System was based no longer apply. For example, the competitive environment is leading to significant technological innovation, with many communications carrier's networks facilities evolving to all-digital transmission, signaling and switching. In this environment, communication services will be virtual and have no separately identifiable physical appearance in switching and transmission facilities and equipment. Thus, it will no longer be feasible to identify physically the specific circuits in a carrier's office and associate them with specific restoration priorities, as has been done for intercity private line services within the Restoration Priority System. **A mechanism to assign priorities to services and even to users rather than only to dedicated circuits is necessary and the NSEP TSP system establishes such a mechanism.**" (Petition, page 13, emphasis added.)

As the rulemaking proceeded, comments were received pointing out the difficulty of applying the rules to the switched PSN. In its Order adopting the TSP rules, the Commission stated:

> "TSP is intended to offer a system by which carriers are presumed not to be engaged in the provision of unreasonable preferences in violation of Title II of the Act if they prioritize services to users in accordance with TSP requirements and procedures. Carriers are not required to include services under TSP that they cannot provide. As a general rule, therefore, we will not limit the applicability of the TSP system to any specific service. The general PSN, however, as generally agreed upon by the commenting parties, is not technically amenable to restoration because subscribers' PSN services are not identifiable within the switching and transport system hierarchy…**We believe the most efficient means for assuring optimal flexibility and response to emergencies requiring restoration of telecommunications services is to rely, to the extent reasonably possible, upon users and carriers to**

> **determine jointly the feasibility and availability of services that can be restored under a TSP priority."** [51]

The notion that agreements could in part define the scope of TSP services found its way into the rules in the TSP Order. The FCC stated that the TSP system might apply at the discretion of and upon special arrangement with the TSP users involved to include Government or noncommon carrier provided services, which are not connected to common carrier provided services.[52]

Result: The FCC foresaw that new technology might make it impossible to track circuits through the network and therefore made the TSP rules applicable to services, but only to the extent providers could technically provide TSP. Noncommon carriers (information services providers?) are not precluded from providing TSP.

Government Emergency Telecommunications Service (GETS):

The NCS TSP Petition also asked the Commission to revoke the call-by-call Precedence System. Dependent on operator intervention, it was obsolete in an era of automatic switching. The Commission granted the NCS request in the TSP Report and Order.

GETS is provided via Government contract with selected interexchange and local exchange carriers. Like the old Precedence System, it provides call-by-call priorities over the PSN in times of emergencies.

In November 1993, the NCS asked the Commission for an opinion as to the legality of this priority system. The Commission responded in August 1995.[53] By that time, GETS was already being provided pursuant to filed tariffs. The Commissions response stated—

> "As described above, call-by-call priority is a feature of the federally managed GETS program. Lawful tariffs implementing that service have gone into effect; thus, it appears that the request for declaratory ruling filed on November 29, 1993 is moot."

In other words, if the service is the subject of a lawful tariff, it is legal. GETS and some other services have subsequently been "detariffed," but the act of detariffing should not make illegal a service that was legal under tariff. NS/EP-related call-by-call priorities over the PSN do not violate the Communications Act's prohibitions on unreasonable priorities and preferences. Packet switching is a technology not specifically addressed in the FCC's GETS letter, but it is unlikely the technology used in the PSN would make a legal difference.

Converged/Next Generation Network:[54]

As new information services technologies converge with traditional telecommunications services to become the next generation network, regulatory authority becomes less clear. The Telecommunications Act of 1996 distinguishes information services (e.g., internet services) from telecommunications services. It is uncertain to what extent rules written for and applied to traditional carriers are applicable to these new providers. However, even if legally applicable, the technical ability to provide NS/EP priorities must also exist before the rules have real meaning.

---

[1] Mr. Clarke has subsequently been designated as the President's National Security Advisor for Cyberspace Security by the President's Executive Order 13231.

[2] Executive Order 13231; Critical Infrastructure Protection in the Information Age.

[3] Stephanie Mehta, "Telco on the Frontline," October 15, 2001, *FORTUNE Magazine*, http://www.fortune.com/indexw.jhtml?channel=artcol.jhtml&doc_id=204468.

[4] The importance of physical security was first discussed in the August 1985, *NSTAC Commercial Network Survivability Task Force Report*, NSTAC V Briefing, October 9, 1985.

[5] Critical Infrastructure Protection R&D Interagency Working Group, *Report of the Federal Agenda in Critical Infrastructure Protection Research and Development, Research Vision, Objectives and Programs,* January 2001.

[6] Kevin J. Houle and George M. Weaver, *Trends in Denial of Service Attack Technology*, CERT Coordination Center, October 2001.

[7] Sam Costello, "Nimda Work Slows," *The Industry Standard*, September 19, 2001, http://www.thestandard.com/article/0,1902,29023,00.html.

[8] GAO Report, *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks*, September 26, 2001.

[9] Houle and Weaver, op cit.

[10] *Convergence Task Force Report*, June 2001, pp. 6–7.

[11] "WAP gateways will be 'hacker magnets,'" John Leyden, vnunet Web site (www.vnunet.com), accessed January 29, 2002.

[12] WAP Forum Web site (www.wapforum.org) accessed November 22, 2001.

[13] Leyden, op cit.

[14] "Firewalls Bypassed in Wireless LANs," http://biz.yahoo.com/bw/010809/2118.html, Yahoo.com, August 9, 2001.

[15] Princy C. Mehta, "Wired Equivalent Privacy Vulnerability," http://www.sans.org/infosecFAQ/wireless/equiv.htm, SANS Organization, April 4, 2001.

[16] A variety of WLAN auditing tools that include hacking tools are freely available on the Internet, e.g., http://www.netstumbler.com/download.php?op=viewdownload&cid=1&orderby=hitsD.

[17] Kevin Poulsen, "War Driving by the Bay," *Security Focus*, April 12, 2001, http://www.securityfocus.com/news/192.

[18] Frank Keeney, "Vacation War Driving: Making 802.11b Wireless Access Point Mapping Fun for the Whole Family," *Pasadena Networks LLC*, http://www.pasadena.net/vacation/.

[19] "PDAs Increasingly Vulnerable to Hackers;" *Reuters*, August 16, 2001.

[20] Please see Appendix B, *Understanding Network Convergence and the Next Generation Network*, and Appendix C, *The Emergency Telecommunications Service (ETS) in Evolving Networks*.

[21] The European Union recently undertook the IPv6 Internet Initiative (6INIT) project. The project's objective is to promote the introduction of IPv6 multimedia and security services in Europe. It will establish guidelines on how to set up an operational platform providing end-users with native IPv6 access points and native IPv6 services. Such guidelines could be used to support IPv6 rollout in the United States. "6INIT Project Information," 6INIT, http://www.6init.org/.

[22] p. ES-4.

[23] Some best practices information was culled from sources that include Michael Vatis, *Cyber Attacks During the War on Terrorism*, Institute for Security Technology Studies at Dartmouth College, September 22, 2001; Paul A. Zocco, *Ten Days to Network Security*, SANS Institute, August 6, 2001, http://www.sans.org/infosecFAQ/securitybasics/10days.htm.

1 Definition from *NSTAC Convergence Task (CTF) Force Report*, June 2001.

2 The NGN is a public, broadband, diverse, and scalable packet-based network evolving from the public switched telephone network (PSTN), advanced intelligent network (AIN), and Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence. *NSTAC CTF Report*, June 2001.

[3] GovNet is a project currently being proposed by the Government, which would create a network specifically used for Government communications.

[4] NSTAC discussed functional requirement in the *NS/VATF Report*, March 2002, and in "NS/EP Communications Functional Requirements," *The Information Technology Progress Impact Task Force Report on Convergence*, May 2000, Table 1.

[5] The ETS is an extension of the International Emergency Preference Scheme (IEPS) of the ITU-T Recommendation E.106 [1] and includes additional provisions for multimedia services through a packet-based telecommunications environment. Internet Engineering Task Force, *Emergency Telecommunications Service in Evolving Networks*, December 2, 2001.

[24] The NGN is a public, broadband, diverse, and scalable packet-based network evolving from the PSTN, advanced intelligent network (AIN), and Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence. *NSTAC CTF Report*, June 2001.

[25] Definitions from *NSTAC CTF Report*, June 2001.

[26] *The NSTAC Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies*, June 1999, Page 66, stated that "end-to-end NS/EP services cannot currently be offered via the public Internet. A number of factors (e.g., lack of NS/EP demand, market factors, and lack of regulatory mandates) make it unlikely that the same type of NS/EP services available in the public-switched network (PSN) will be available over the Internet for the foreseeable future."

[27] The TSP Oversight Committee was established to identify and review any systemic problems developing in the TSP System and to provide advice and assistance to the Manager of the NCS when problems arise.

[28] The term "common carrier" or "carrier" means any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this Act. Communications Act of 1934, as amended, §. 3 [47 U.S.C. 153].

[29] Communications Act of 1934, § 202 [47 U.S.C. 202].

[30] Communications Act of 1934, § 706 [47 U.S.C. 606].

[31] FCC rules, Defense and Emergency Preparedness Functions [47 C.F.R. 0.181–0.186].

[32] *TSP Report and Order*, 3 FCC Rcd 6650 (1988).

[33] *TSP Report and Order*, paragraph 25.

[34] In the case of frame relay, TSP is provided on the physically identifiable portions of the circuit. If problems occur with the equipment within the cloud, that equipment is replaced or the permanent virtual circuit is rerouted.

[35] *NSTAC CTF Report*, June 2001, page 14.

[36] GovNet is a project currently being proposed by the Government, which would create a network specifically used for Government communications.

[37] *TSP Report and Order*, Appendix A, paragraph 4, section (c)(1).

[38] It is clear that noncommon carriers, (e.g., ISPs), have the ability to opt-in to the TSP program. However, ISPs may be exposed to liability by other commercial customers in the event the service of those customers is degraded to provide TSP services to an authorized entity. ISPs will have to consider this issue to deal with the provision of TSP services in the NGN.

[39] *TSP Report and Order*, paragraph 24.

[40] The Internet Society, *Definition of Differentiated Services Per Domain Behaviors and Rules for Their Specification*, RFC 3086 (April 2001), paragraph 1.

[41] http://www.faqs.org/rfcs/rfc3086.html.

[42] http://www.faqs.org/rfcs/rfc2474.html.

[43] T1is a leading telecommunications network standards developer and refers to the Technical Committee and M1 is one of its six subcommittees and focuses on Internetwork Operations, Administration, Maintenance, & Provisioning. "T1 Mission/Vision Scope," http://www.t1.org/html/mission.htm#mission.

[44] NSTAC discussed functional requirement in the *NS/VATF Report*, March 2002, and in "NS/EP Communications Functional Requirements," *The Information Technology Progress Impact Task Force Report on Convergence*, May 2000, Table 1.

[45] The ETS is an extension of the International Emergency Preference Scheme (IEPS) of the ITU-T Recommendation E.106 [1] and includes additional provisions for multimedia services through a packet-based telecommunications environment. Internet Engineering Task Force, *Emergency Telecommunications Service in Evolving Networks*, December 2, 2001.

[46] *NSTAC Information Technology Progress Impact Task Force Report on Convergence*, May 2000, page 20.

[47] Noncommon carriers, along with common carriers, also participate in a forum called the Network Reliability and Interoperability Council (NRIC), which provides recommendations to the FCC and to the telecommunications industry that, when implemented, will ensure optimal reliability and interoperability of public telecommunications networks. There have been no antitrust concerns as a result of this recommendation-making collaboration between service providers for the FCC.

[48] *NSTAC's Information Technology Progress Impact Task Force Report on Convergence (ITPI Report)*, Section 2.0, lists 12 NS/EP Communications Functional Requirements. "Enhanced Priority Treatment" appears to be the only functional requirement posing a potential legal issue.

[49] 47 U.S.C. 202(a)

[50] *Petition for Rulemaking re National Security Emergency Preparedness Telecommunications Service Priority System*, April 1, 1987 ("Petition").

[51] *NSEP TSP Report and Order*, 3 FCC Rcd 6650 (1988), at pars. 24 and 25 (emphasis added).

[52] 47 CFR Part 64, Appendix A, Par. 4 c (Other Services)

[53] Letter to Carl Smith, Office of the Manager, National Communications System, from James R. Keegan, Chief, Domestic Facilities Division, Common Carrier Bureau, Federal Communications Commission, August 30, 1995.

[54] According to *the NSTAC's Information Technology Progress Impact Task Force Report on Convergence*, convergence "indicates a process over a 3-to-5 year period of Next Generation Network evolution during which traditional circuit-switched networks and IPO-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. It is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence."