Chicago, Illinois - USA
29 May – 2 June 2006

SOURCE : NSTAC (submitted by TIA)

TITLE : President's National Security Telecommunications Advisory Committee (NSTAC) Next-Generation Networks Task Force Report –Appendices

AGENDA ITEM : GTSC item 5.0

DOCUMENT FOR :

Decision	
Discussion	
Information	**x**

1 DECISION/ACTION REQUESTED

N/A

2 REFERENCES

Published by Consumers International in December 2005

3 RATIONALE

Web shot of the CI page where it can be downloaded as PDF or DOC (and a Japanese version too).

4 CONSEQUENCES AND IMPLICATIONS

(The implications for (including human resources) should be set out in this section).

5 ISSUES FOR DISCUSSION

(This section should, as necessary, contain additional argumentation).

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NEXT GENERATION NETWORKS TASK FORCE

Appendices

March 28, 2006

APPENDIX A

PARTICIPANT LIST:
TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER WORKING GROUP PARTICIPANTS

A PARTICIPANT LIST

TASK FORCE MEMBERS

Microsoft	Mr. Phil Reitinger, Chair
BellSouth	Mr. David Barron, Vice Chair
Bank of America	Mr. Roger Callahan
BellSouth	Ms. Cristin Flynn Goodwin
Boeing	Mr. Bob Steele
Cingular Wireless	Mr. Brian Daly
Computer Sciences Corporation	Mr. Guy Copeland
Lockheed Martin	Dr. Al Dayton
Lucent Technologies Bell Labs	Mr. Karl Rauscher
Motorola	Mr. Michael Alagna
Nortel Networks	Dr. Jack Edwards
Northrop Grumman	Mr. Dennis McCallam
Qwest	Mr. Jon Lofstedt
Raytheon	Mr. Frank Newell
SAIC	Mr. Hank Kluepfel
SBC	Ms. Rosemary Leffler
Sprint Nextel	Mr. John Stogoski
Telcordia	Ms. Louise Tucker
Unisys	Mr. Mike Gibbons
United States Telecom Association	Mr. Tom Soroka
VeriSign	Mr. Michael Aisenberg
Verizon	Mr. James Bean

OTHER WORKING GROUP PARTICIPANTS

ATIS	Mr. Tim Jeffries
BellSouth	Mr. Bryan Garrett
BellSouth	Ms. Pamela Gurule
Cingular Wireless	Mr. Brian Daly
Cingular Wireless	Mr. Peter Musgrove
Cingular Wireless	Mr. DeWayne Sennett
Cisco	Ms. Robin Roberts
Cisco	Mr. Chip Sharp
Cox Communications	Mr. Mark Adams
Cox Communications	Mr. Larry Dexter
Cox Communications	Mr. Craig Howell
Cox Communications	Mr. Scott Smith
George Washington University	Dr. Jack Oslund
Global Crossing	Mr. David Cooper
Hewlett-Packard	Mr. Joe Connor
Hewlett-Packard	Mr. Stephen Squires
Intel	Mr. Ryan Ware
Juniper	Mr. Ron Bonica
Lockheed Martin	Dr. Kate Cherry

Lockheed Martin	Mr. Joe Cramer
Lockheed Martin	Mr. Chris Nolan
Lucent Technologies	Mr. Tom Anderson
Lucent Technologies	Ms. Cheryl Blum
Lucent Technologies	Mr. Glenn Evans
Lucent Technologies	Mr. Brent Greene
Lucent Technologies	Mr. Bob Thornberry
Lucent Technologies	Dr. Zhibi Wang
Lucent Technologies Bell Labs	Mr. Stuart Goldman
Lucent Technologies Bell Labs	Mr. Eric Grosse
Lucent Technologies Bell Labs	Dr. Alan Jeffrey
Lucent Technologies Bell Labs	Mr. Rick Krock
Lucent Technologies Bell Labs	Mr. Ted Lach
Lucent Technologies Bell Labs	Dr. Anil Macwan
Lucent Technologies Bell Labs	Mr. Jim Runyon
Lucent Technologies Bell Labs	Mr. David Shinberg
Lucent Technologies Bell Labs	Mr. Rao Vasireddy
Microsoft	Mr. Khaja Ahmed
Microsoft	Mr. Jerry Cochran
Microsoft	Mr. Shawn Hernan
Microsoft	Mr. Ted Tanner
Microsoft	Mr. Paul Nicholas
Microsoft	Mr. Henry Sanders
Microsoft	Mr. Sanjay Kaniyar
Motorola	Mr. Mike Berta
Motorola	Mr. Tom Gaynor
Motorola	Mr. Jim Goldstein
Motorola	Mr. Don Dautel
Motorola	Mr. Ben LaPointe
Motorola	Mr. Chip Wood
Pennsylvania State University	Dr. Tom La Porta
PriceWaterhouseCoopers	Mr. Jim Craft
Qwest	Mr. Curtis Ashton
Raytheon	Mr. Sean Anderson
Rutgers University	Dr. Michael Tortorella
Spectrasite	Mr. Ted Abrams
Sprint Nextel	Mr. Chase Cotton
Sprint Nextel	Ms. Allison Growney
Sprint Nextel	Mr. Keecheon Kim
Telcordia	Mr. Arun Handa
Telcordia	Mr. Bob Lesnewich
Telecommunication Industry Association	Mr. David Thompson
United Telecommunications Council	Ms. Prudence Parks
University of California at Berkeley	Dr. Shannon Lake
VeriSign	Mr. Tony Rutkowski
Verizon	Mr. Tim Beaird

Verizon	Mr. Bruce Fleming
Verizon	Mr. Stuart Jacobs

GOVERNMENT PERSONNEL

Department of Defense	Mr. Scott Swartz
Department of Homeland Security	Mr. Daniel Ahr
Department of Homeland Security	Mr. David Delaney
Department of Homeland Security	Mr. Alan Gallagher
Department of Homeland Security	Mr. Rick Lichtenfels
Federal Reserve Board	Mr. Chuck Madine
General Services Administration	Mr. Doug Covert
National Communications System	Mr. Gary Amato
National Communications System	Mr. Steve Carty
National Communications System	Mr. Tom Falvey
National Communications System	Ms. Mai Tai Galloway
National Communications System	Mr. John Graves
National Communications System	Mr. Lou Morrison
National Communications System	Ms. DeJuan Price
National Communications System	Ms. Carol-Lyn Taylor
United States Northern Command	Capt. Eric Koenig
United States Northern Command	Mr. Dan Zink

APPENDIX B

ACRONYM LIST

B ACRONYM LIST

ASPR	Agreements, Standards, Policies and Recommendations
ATIS	Alliance for Telecommunications Industry Solutions
BGP	Border Gateway Protocol
COP	Committee of Principals
CRISP	Cross Registry Information Service Protocol
DCS	Digital Control Systems
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNS	Domain Name System
DOD	Department of Defense
DOS	Denial of Service
ETS	Emergency Telecommunications Service
FCC	Federal Communications Commission
FICC	Federal Identity Credentialing Committee
GETS	Government Emergency Telecommunication Service
GIG	Global Information Grid
GSA	General Services Administration
IAIP	Information Analysis and Infrastructure Protection
IDS	Intrusion Detection System
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
INEEL	Idaho National Laboratory
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRIS	Internet Registry Information Service
ISP	Internet Service Provider
IT	Information Technology
NCS	National Communications System
NDAC	Network Design and Analysis Capability
NGN	Next Generation Networks
NGNTF	Next Generation Networks Task Force
NIST	National Institute of Standards and Technology
NRIC	Network Reliability and Interoperability Council
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTRWG	Near Term Recommendations Working Group
OASIS	Organization for the Advancement of Structured Information Standards
OIC	Office of Interoperability and Compatibility

OSTP	Office of Science and Technology Policy
PCS	Process Control System
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RFC	Request for Comment
SCADA	Supervisory Control and Data Acquisition
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transaction Layer Security
VPN	Virtual Private Network
WPS	Wireless Priority Service
XML	Extensible Mark-Up Language

APPENDIX C

NGN DEFINITIONS

C NGN DEFINITIONS

As used in this paper:

Applications: software or hardware entities that provide specific, valuable functions or services to users.[1]

Services: functions provided by software or hardware entities built on top of the transport networks to deliver user-visible services such as fixed telephone services, mobile telephone services, and Internet services.[2]

Transport networks: facilities that carry user information and network management/ control information between different endpoints.

[1] See Computer User High Technology Dictionary (defining "Application" as "[a] program that helps the user accomplish a specific task; for example, a word processing program, a spreadsheet program, or an File Transfer Protocol (FTP) client. Application programs should be distinguished from system programs, which control the computer and run those application programs, and utilities, which are small assistance programs.")

[2] ATIS divides services into **Transport Services**, involving the transport of packets, and **Application Services**, which include remote delivery of functions by applications to users (e.g., network storage). ATIS Next Generation Network Framework, Part I: NGN Definitions, Requirements, and Architecture, p. 19-20 (Nov. 2004) (hereinafter ATIS NGN Paper Part I). Some might add **Infrastructure Services**, which provide the platform for transport and applications, to this list.

APPENDIX D

SUMMARY OF ANALYSIS FRAMEWORK

D SUMMARY OF ANALYSIS FRAMEWORK

D.1 Working Group Processes

At the President's National Security Telecommunications Advisory Committee (NSTAC) XXVII Meeting held on May 19, 2004, the NSTAC Principals requested that a task force be created to address how the Government can continue to best meet national security and emergency preparedness (NS/EP) telecommunications requirements and address emerging threats in the evolving NGN environment. Subsequently, the Next Generation Networks Task Force (NGNTF) was created to:

1) Agree upon a high-level description of the NGN's expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely;
2) Identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and accountability among network participants and network layers will work; and
3) Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements.

As a first step, the NGNTF assembled a group of subject matter experts (SME) and Government stakeholders to discuss NGN issues in August 2004. As a result of the meeting, working groups were created to address the following five areas: (1) a description of the NGN; (2) NGN service scenarios and user requirements; (3) end-to-end services provisioning; (4) NGN threats and vulnerabilities; and (5) incident management on the NGN. A sixth working group was formed to address actions that could be taken immediately to preserve or enhance NS/EP communications for the future.

The Near-Term Recommendations Working Group (NTRWG): The NTRWG examined near-term opportunities for which existing technology could be leveraged to improve the security and availability of NS/EP communications on converging networks. The NTRWG also investigated areas where Government involvement was needed in the near term due to the immediacy of events — such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs. Based on the NTRWG's analysis of near-term challenges and opportunities, the NSTAC made several recommendations to the President in March 2005.

The NGN Description Working Group: This group was formed to provide a high-level description of the NGN. The description reflects the vision of different communities and addresses what is known, what is unknown, and what the market may determine regarding the network.

The Scenarios and User Requirements Working Group (SURWG): The SURWG examined existing descriptions of NS/EP functional requirements to develop recommendations for

Government stakeholders regarding how these functional requirements should be amended or supplemented based on the scenarios. To accomplish its analysis, the working group developed scenarios in five areas: Continuity of Government, critical Government networks, industry and critical infrastructure, public safety, and general users. After identifying NS/EP user requirements that apply within an NGN environment for each scenario class, the working group then considered how these requirements will differ from those of traditional communications networks and what this will mean for network users.

The work of the SURWG served as the foundation for the work of the NGNTF's End-to-End Services Working Group and the Vulnerabilities and Threat Modeling Working Group. Together their work provided key insights into how next generation NS/EP services can be more resilient and maintain high quality, on-demand, seamless accessibility.

The End-to-End Services Working Group (ESWG): The ESWG examined the end-to-end services aspects of the evolving NGN and the implications to those performing NS/EP functions. The working group tasks included describing how end-to-end services would be provisioned and explaining how the interfaces and accountability among network participants and network layers would work. Building upon the work of the SURWG, the ESWG identified specific areas that Government, industry, and user community stakeholders and decision-makers must address, which will impact availability of those end-to-end services that the NS/EP communities require at times of crisis.

The Vulnerabilities and Threat Modeling Working Group (VTMWG): The VTMWG examined relevant threats and vulnerabilities from an NS/EP perspective, using the SURWG scenarios among others. The VTMWG examined vulnerabilities of NGNs from an NS/EP perspective; examined relevant threats associated with the SURWG scenarios from an NS/EP perspective; and identified how responsibilities for responding to or mitigating these threats have shifted. Emphasis was placed on confidentiality, integrity, availability, and authentication of communications.

The Incident Management Working Group (IMWG): The IMWG was formed to respond to NGN incident management issues raised at the August 2004 SME Meeting, including response time needed to thwart cyber attacks, the increase of nontraditional service providers in the NGN environment, and a need for improved information-sharing incentives, among other issues. In August 2005, the IMWG hosted a SME Meeting on Incident Management in the NGN, which was attended by about 100 incident managers from the communications and information technology industry as well as the Federal Government. The 2005 SME Meeting Proceedings are published separately.

D.2 Subject Matter Expert Meetings

August 4 -5, 2004: The NGNTF held its first SME Meeting on August 4-5, 2004, at Computer Sciences Corporation (CSC) in Falls Church, Virginia. The primary objectives of the meeting was to facilitate a better understanding of the key technical and policy issues surrounding the evolution of the current telecommunications network to NGNs and to develop the NGNTF's work plan for addressing the issue. The NGNTF used the input from this meeting to develop its

key objectives for the task force, including an effort to develop near term recommendations. The SME meeting focused on several critical areas including: Priority and Alternatives for NS/EP Communications; Cyber Security; End-to-End Services; and Wireless and Incident Management. The NGNTF's working groups — Description, Scenarios and User Requirements, End-to-End Services, Vulnerabilities and Threat Modeling, and Incident Management — were formed as a result of the findings from the meeting.

August 30, 2005: The NGNTF held a second SME Meeting with the National Coordinating Center (NCC) Task Force (NCCTF) on August 30, 2005, also at CSC in Falls Church, Virginia. The purpose of the meeting, "Incident Management in Next Generation Networks," was to further explore the findings from the Incident Management breakout group at the first NGNTF SME Meeting and to receive feedback on potential incident management recommendations for the NGNTF final report. A further objective of the meeting was to validate findings from three of the NGNTF subgroups: the SURWG, the ESWG, and the VTMWG.

D.3 Scenarios

The NGNTF created and charged the SURWG to develop scenarios for NS/EP communications on the NGN. The SURWG examined existing descriptions of NS/EP functional requirements to develop recommendations for Government stakeholders on amendments or supplements to these functional requirements based on the scenarios. To accomplish their analysis, the working group developed five scenarios:

- *Continuity of Government*. Focused on the needs and functional requirements for maintaining the systems and networks critical to the ongoing functioning of Government during incidents of national significance.

- *Critical Government networks*. Focused on the needs and functional requirements of a network key to the continuity of the U.S. economy, *Fedwire*.

- *Industry and critical infrastructure*. Focused on the needs and requirements for maintaining the functionality of Supervisory Control and Data Acquisition (SCADA) systems supporting U.S. critical infrastructures.

- *Public safety*. Focused on the needs and functional requirements of first responders and other public safety organizations, such as hospitals, during an NS/EP event.

- *General users.* Focused on the needs and functional requirements of the general civilian user during incidents of national significance and how these might compete, or in some cases interfere, with NS/EP communications needs. A further emphasis is on the NS/EP user that must access NS/EP communications services from a general civilian device or location (e.g., home Voice over Internet Protocol [VoIP] service; Internet access over a wireless handheld from a public hotspot).

After identifying NS/EP user requirements for each scenario class that apply within an NGN environment, the working group then considered how these requirements would differ from those of traditional communications networks and what this would mean for network users. The work of the SURWG served as the foundation for the work of the NGNTF's ESWG and the VTMWG.

APPENDIX E

FEDERAL FUNCTIONAL REQUIREMENTS

E FEDERAL FUNCTIONAL REQUIREMENTS

The President's National Security Telecommunications Advisory Committee's *Convergence Task Force Report*, 2001, determined that the following functions were necessary for the Federal Government to effectively make use of Next Generation Networks (NGN). Concepts such as "scalability" or "secure networks" do not go far enough in describing what technologies, services, and applications will be needed to support the Government's national security and emergency preparedness (NS/EP) mission going forward. As will be discussed in greater detail below, and throughout the scenarios to follow, the functional requirements are not applicable to all networks, systems, and users. However, Federal agencies may pick and choose the NGN NS/EP services needed to support a mission, based on the particular environment.

The fourteen Federal functional requirements are as follows:

Enhanced Priority Treatment
Secure Networks
Ubiquitous Coverage
International Connectivity
Interoperable
Scalable Bandwidth
Mobility
Broadband Service
Reliability/Availability
Restorability
Survivability/Endurability
Non-traceability
Affordability
Voice-Band Service

APPENDIX F

END-TO-END SERVICES ISSUES

F END-TO-END SERVICES ISSUES

F.1 Background

This Appendix provides additional background (developed by the End-to-End Services Working Group) on end-to-end services relevant to the conclusions and recommendations of the Next Generation Networks Task Force (NGNTF), which are contained in the main body of the Report.

F.1.1 End-to-End Services

A variety of new feature-rich services, extending beyond those available today, will emerge as the NGN develops. New expanded and highly integrated services, including video, geo-location and navigation aids, peer-to-peer communications and a plethora of other new and "smart" multimedia, interactive programming and data-intensive information services will become commonplace and ubiquitous. The strong emergence of standards-based technology for web services within service-oriented architectures (SOAs) will increase information technology adaptability and efficiency for a broad range of user and network applications. Greater wireless-based capabilities will allow access to information and services without the familiar wire tethers of our legacy telecommunications world. Nomadic capabilities will also blur the line between a location-based telephone and a mobile terminal, and location or numbering constraints.

Individuals with national security and emergency preparedness (NS/EP) roles and mission functions have a critical need to understand how the NGN service environment impacts their ability to execute those functions, and how their needs for assured services and availability will be satisfied by the NGN under a range of operational conditions; namely, routine day-to-day activities all the way to highly stressful crisis conditions.

It is critical for user communities to understand how to plan, implement, and accomplish their NS/EP missions through effective use of the evolving NGN environment. A question repeatedly asked by members of these communities: "what NS/EP required functions will be provided inherently by the NGN and what functions will NS/EP users need to provide?"

The NGN infrastructure will integrate a number of common network and information services, including messaging, discovery, collaboration, storage, numbering, and security. A plethora of custom application-oriented services for various affinity groups will also exist. For the various NS/EP communities of users, it is most important that those NGN capabilities and services used for critical mission functions be well-defined, understood, available and reliable.

Over time, it is anticipated that market force mechanisms will satisfy those NS/EP community requirements that have broad application within the NGN. As they are today and have historically existed, the most critical and often more narrowly required NS/EP community's needs may have to be addressed through alternative support mechanisms. Recent events and disasters have highlighted the importance of this community, including first responders, be given the support they need.

In order for the NGN to broadly meet essential NS/EP community requirements in a consistent, continuous and reliable manner from end to end, a 'common operational criteria' must be defined and adopted by entities supplying network access, transport and infrastructure services for this community.

F.1.2 The NGN: A Work in Progress

A fully capable NGN, as envisioned by both infrastructure and service-oriented professionals, readily supports current and forecast user requirements with highly available and robust connectivity. As the NGN itself is in an early implementation stage, actual access, transport, and service availability today may not fully support anticipated NS/EP user requirements. In addition, as the NGN is a local, regional, national, and global service environment, uniform and consistent support of broad NS/EP user requirements across extended geographical distances is a most challenging design goal.

F.1.3 The NGN: A Highly Complex Service Environment

Complex enterprise service environments, such as the NGN, are composed of multiple disparate networks, network management systems and data operations centers, integrated both logically and physically to support myriad applications for a diverse user community of interest. In an NS/EP context, daily operational complexity is significantly increased as a result of the emergence of often unforeseen and highly variable challenges, including real-time bandwidth allocation to support routine and surge data traffic, rapid user authentication and resource prioritization, transparent control of inter-network data and signaling information, and seamless management of critical and real-time end-to-end services, all supported within a compliant heterogeneous operational framework.

Although heterogeneous by design, the NGN shares common logical and physical components, such as:

- Routing and switching network elements,
- Network element operating systems,
- Network management platforms,
- Basic application services present on each network,
- Desktops and/or workstations in a distributed architecture, and
- Internal and external network routing protocols.

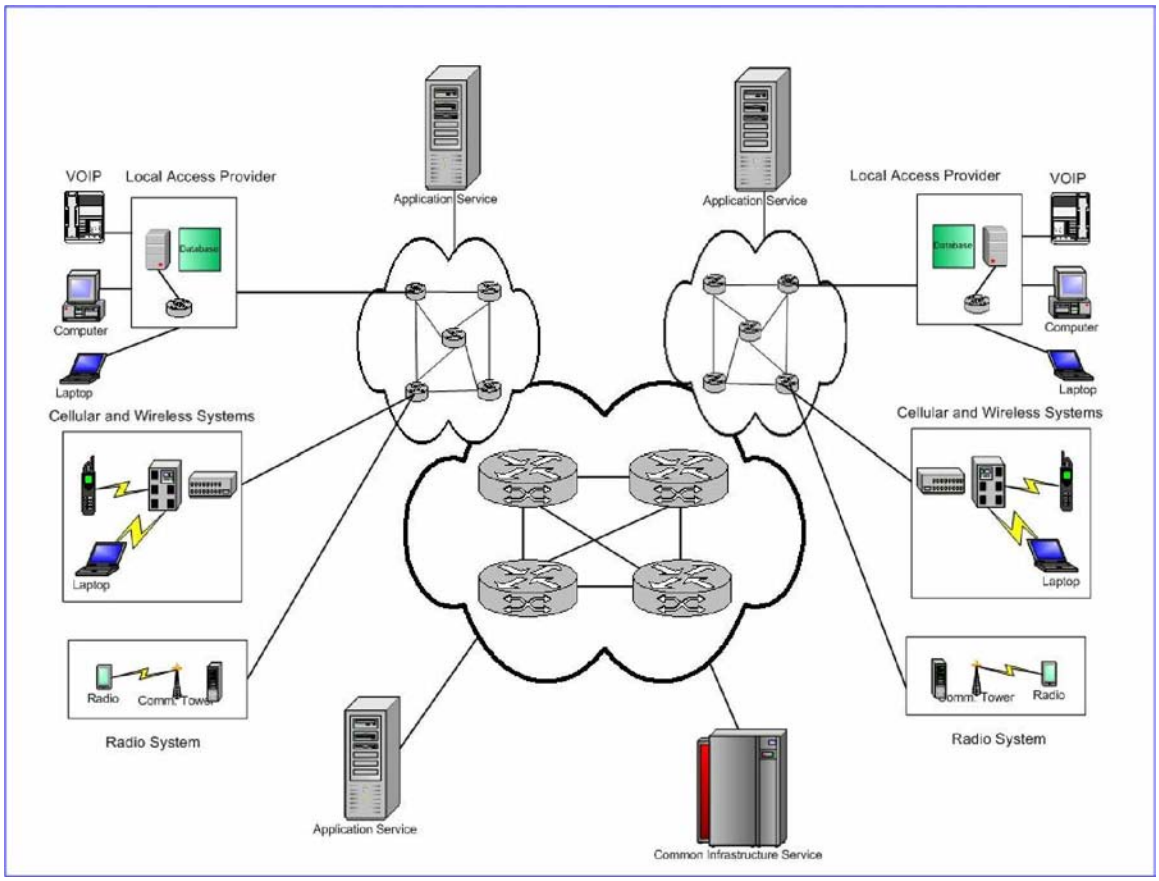
F.1.4 The NGN is Composed of Multiple, Interconnected Networks

NS/EP service availability in a dedicated, ad hoc, and/or geographically dispersed environment is enabled through dynamic, adaptive and resilient management of data traffic transported across interconnected user, management and control planes. Inter-network service connectivity considerations for NS/EP applications include, but are not limited to:

- Interior routing protocol(s) to exterior routing protocol(s) conversion
- Translation or encapsulation of mixed network management traffic
- Network topology hiding, protection and isolation (Firewall) activities between connected networks
- Design of data collectors for performance, fault, and accounting information
- Dynamic network element configuration across an interconnected environment
- Definition, dissemination and enforcement of end-to-end security policy, and
- Definition and dissemination of network management policies and standard operating procedures for use in defined NS/EP contingencies and scenarios.

Figure F-1, shown below, illustrates a notional depiction of the NGN. Note that public safety networks may be markedly different from this more commercially-oriented NGN diagram, however many of the basic concepts and NS/EP needs are the same, or even more demanding given the user class.

F-1. Notional Depiction of a Commercially Oriented NGN



F.1.5 Gaining Consensus for a Uniform NGN Logical and Physical Design Is a Critical Success Factor

The NGN is designed to support NS/EP scenarios in a localized, metropolitan, regional, national and international context. Success of the NGN, from an architectural and services perspective, is based on stakeholder understanding and acceptance of its capabilities to support well-defined user requirements. Therefore, implementation of the NGN requires designing and developing a scalable, high-availability network architecture capable of supporting current and anticipated user requirements, with realistic levels of service defined. Development of this network architecture includes identifying and resolving issues in the current operational environment that impede achieving that end-state goal. Such issues include optimization of network management capabilities; development, acceptance and the dissemination of operational procedures and practices; and, effective end-to-end mechanisms to rapidly isolate and resolve any network instabilities that impact availability and performance across the NGN.

The NGN NS/EP common operational criteria must address and incorporate these essential elements:

- Identification, authorization and authentication of the NS/EP user — namely, a person, communication device or network — trying to access local telecommunications services
- Priority access during times of contention and agreements on how priority transport of packets across multiple networks will be serviced consistent with a user's NS/EP authorizations and required class of service
- Practices and controls to manage security to provide required operational integrity.
- Mechanisms and agreements for managing and coordinating incident response when events are materially affecting the normal servicing of NS/EP users
- Best practices for participants, who are supporting and supplying services for NS/EP users of the NGN
- Defined classes of service that are supported by all network participants within the NGN

Addressing these needs will be a challenge of extraordinary significance and will require unprecedented leadership and collaboration among the public and private sectors.

F.1.6 Fundamental NGN Services Availability Issues

An NGN designed to support NS/EP applications and services for commercial, civil, and Government organizations, focuses on enabling a high-availability, secure and interoperable environment for local, regional and national user connectivity. Based on a logical framework, the NGN emphasizes high availability in a resilient, high bandwidth transport backbone as a principal characteristic. From a security perspective, the NGN is concerned with authentication of users attempting to access the network, uniform enforcement of security policy through user tracking and auditing, and network resources authorization. Interoperability of diverse network elements, protocols and operating systems in a geographically dispersed operational environment is a significant issue; therefore, managing it effectively is critical to the viability and resiliency of ongoing NS/EP applications and services support in the future.

F.2 Key and Unique NGN NS/EP Issues

NS/EP requirements on the NGN (*see Report, Section 4*) can be described in terms of three top-level fundamental and critical functional requirements: (1) access to the NGN; (2) transport of information within the NGN; and (3) availability of infrastructure and application-level services. Assurance of access, transport and services availability for NS/EP functions enable the required state of readiness and ability to respond to and manage any local, national, or international event or crisis that causes injury or harm to the general population, damage to or loss of property, or degradation of the NS/EP operational posture anywhere within the United States. However, the fundamental requirements of access, transport, and availability of services must be provided in a manner that *assures* NS/EP communities receive an appropriate level of service priority among potentially competing users and activities.

F.2.1 Local Access Requirement

In an NGN context, local access is defined as:

- Physical access and connectivity to communications, and
- A local end point connection and the destination end point connection (for human or machine network users as physical and logical entities).

Local access, transport and user services are the three constituent partitions of any network environment. Depending upon context, any of these three may be physical, logical or both concurrently. Local access is the partition that connects people and communications devices, identified as machines, with network resources. Networks connect together at the transport partition, and also use network resources. Therefore, a user community includes people, communications devices, and other networks. People and communications devices are connected locally and remotely to a network at local access, while networks connect at the transport partition.

Within the NGN it is essential that:

1) A network user is defined as an individual, a communications device (machine), or another network, as all three may request network access and resources from one or more sub-networks within the NGN.

2) Mandatory authentication is required for a valid user and authorization for resources in appropriate cases such as where the user could affect the NGN itself, and for all user requests at the local access partition and transport partition.

Establishing local access priority requires:

- Authentication of the user,
- Authorization of network resources,
- Identification of entities authorized (e.g., devices and human users),

- Establishment of information assurance and integrity, and
- Adherence to industry-accepted technical standards.

Priority is not an issue when all authenticated users have unrestricted access to network resources. Additionally, priority is typically not an issue in the transport partition, especially in the network backbone. However, priority is potentially an issue at local access due to contention for finite network resources available. Resources may be physical and logical, including physical switch ports, logical circuits, bandwidth, connection time limits, and end-to-end resource reservation constraints. Priority access, therefore, is based on the presence of contention for physical and logical resources within a network.

For the foreseeable future, NGN evolution will be as an overlay — composed of multiple physical networks bound together logically by common operational criteria and an overarching security policy. Each individual network's internal operational policy is based on supporting its own user community of interest first, and then supporting directly connected adjacent networks. However, common operational criteria, agreed upon by networks bound by cooperation in an NGN context; provide a framework for supporting NS/EP activities that extend beyond a local network level. In an NGN supporting NS/EP activities, common operational criteria for adjacent networks may supplant local network policy.

Priority resource requests for individuals or communications devices received from external networks are serviced in accordance with the common operational criteria for connected networks in an NS/EP context. When there is sufficient bandwidth and network connectivity to support all requests, there is no contention and priority is not considered. However, when contention for network resources occurs, networks will address resource requests either on a priority or first-come, first-served basis.

In a first-come, first-served context, all resource requests are of equal priority. New requests for network resources are denied in favor of maintaining already established connections once congestion or connectivity thresholds are met. When priority is considered, networks will actively arbitrate resource requests through enforcement of connection time limits; or by clearing lower priority connections randomly (informal call clearing); or via a weighted queue mechanism (formal call clearing) to accommodate higher priority requests. Determination of priority may be based on type of authenticated user, device or network, network resources requested, and type of service indicated in network protocol headers or end-to-end flow labels.

Within the NGN it is essential that:

1) A common operational criteria is defined and agreed upon by participating networks in an NGN context, to provide a framework for supporting NS/EP activities that extend beyond a single local network. Criteria focuses on authentication, authorization, contention, and priority issues across constituent networks in an NGN framework.

2) Priority management is implemented uniformly across the NGN, based on user, device or network authentication, network resources authorization, and class of service requested at the local access or transport partitions.

3) Priority is defined here as contention for network access, resources and services, but not for access to applications.

F.2.2 Establishing Priority Among Networks

Within an evolving NGN, multiple discrete networks are integrated as required to support NS/EP activities. Communication between two parties may originate in a network of a certain type and go through one or more different networks. Priority is defined and enforced differently by individual entities within the NGN, thus end-to-end priority determination is based on a concatenation of multiple local network policies that respond differently to NS/EP events. The mechanism for evaluating and handling priority of the packet/message/circuit may be different than the one used in the network of origin. Defining and enforcing end-to-end priority is a challenge for network designers and operations personnel alike due to the dynamic nature of the NGN, and the scope, severity and duration of potential NS/EP events. Defining common operational criteria across the NGN is a preferred mechanism to ensure uniformity of priority definition and support end-to-end. This will eventually necessitate agreements at both a business and policy level as well as at the technical levels. This will require definitions of equivalencies and shared semantics for various levels of priority between different types of networks. An appropriately articulated minimal acceptable service threshold of metrics or capabilities by the U.S. Government would benefit those with NS/EP requirements as developers engineer capabilities within the NGN. Further, suitable standard bodies will need to develop the protocols for translating required priority mappings.

Network-to-network connectivity typically occurs at the transport partition. However, under conditions of contention at either the local access or transport partition, user priority becomes the key criterion for permitting access to network resources after successful authentication and authorization occurs. In an NGN, end-to-end contention is a measure of the availability of resources across multiple constituent networks. Common operational criteria define and enforce priority uniformly for any and all users requesting network resources at either the local access or transport partitions. Participating networks in an NGN are required to successfully demonstrate the capability to support specified common operational criteria, such as assigning user priority and policy enforcement. This proof of performance and enforcement is normally defined and demonstrated prior to any actual NS/EP event.

Within the NGN it is essential that:

1) A common operational criteria across the NGN is defined as a standard mechanism to ensure uniformity of priority definition and support end-to-end.

2) Mutual service level guarantees are developed that encode a set of common operating rules that all registered networks agree to follow;

3) The capability to support common operational criteria is demonstrated, such as assignment of user priority and enforcement of NGN policy end-to-end, prior to an actual

NS/EP event; recognizing that processes should be in place for ad-hoc or unanticipated support.

F.2.3 Contention for Resources.

This issue is critical and highly complex, incorporating a number of intangible concepts such as contention/congestion, the "value" of users and resources, and decision-making in response to all types of NS/EP scenarios. Therefore, clarification is written in detail to propose a tangible approach to assessing and managing the interaction of contention, arbitration and precedence — which clearly complement or oppose each other, based upon event specifics.

For the foreseeable future, the NGN will be based on an overlay of individually connected networks, brought together physically and logically to support a myriad of NS/EP activities. Policies for handling contention for resources on an individual network or across multiple networks require definition and enforcement of common operational criteria. Such criteria provide a uniform mechanism for dealing with arbitration, priority treatment/pre-emption and precedence within a single network or across an expansive NGN.

User authentication and network resource authorization are two key criteria for access to network services whether or not contention is present. Precedence becomes a third key criterion when contention is present. Requests for classes of service, therefore, are based on considering these three criteria – authentication, authorization, and precedence, in combination. Common operational criteria define classes of service available or supported based upon accepted definitions of the three key criteria for an individual network, or multiple networks in the NGN.

An example representative framework supporting common operational criteria is presented below in Figure F-2. The critical elements of this framework: a) user authentication types, b) network service authorization levels, and c) resource precedence states, are combined to define specific classes of service (CoS) offered. Traffic management schemes employing traditional network queuing techniques can support these classes of service by ensuring equitable access and arbitration, or priority, as appropriate.

User authentication types, identifying essential and non-essential entities requesting access to the network at either the local access or transport partition, include:

- Support — Non-critical, sustaining, and administrative individual or network entity
- Essential — First responders, and key personnel or network entity

Network service authorization levels, based on criticality or potential impact of NS/EP events and scenarios, include:

- Routine – Priority/pre-emptive and planning preparations for an anticipated NS/EP event, such as an approaching hurricane or forest wildfire
- Imminent – Near-term preparations for an anticipated NS/EP event
- Response – Initial critical response to an NS/EP event that has occurred

- Sustaining – Ongoing response to, and support for, an NS/EP event after initial response activities are completed

Resource precedence states, based on the presence or lack of contention, include:

- No Precedence – No contention present or detected, requested network resource parameters (e.g., bandwidth, connection time) are available to all authenticated and authorized users
- No Precedence, Default – Threshold of minimal contention detected, default network resource parameters (i.e., standard operational profile, but no special requests) are available to all authenticated and authorized users
- Precedence – Above threshold of minimal contention detected, requested network resource parameters (e.g., bandwidth, connection time) are available to all authenticated and authorized users with any precedence level greater than none
- Precedence, Default – Above threshold of minimal contention detected, default network resource parameters are available to all authenticated and authorized users with any precedence level greater than none
- High Precedence – Above threshold of minimal contention detected, requested network resource parameters (e.g., bandwidth, connection time) are available to all authenticated and authorized users with any precedence level greater than Precedence
- High Precedence, Default – Above threshold of minimal contention detected, default network resource parameters are available to all authenticated and authorized users assigned with any precedence level greater than Precedence

Classes of service (CoS), derived as combinations of user authentication types, network service authorization levels, and resource precedence states, include:

- Best Effort
- Priority
- High Priority
- Critical
- Pre-Emptive

Traffic management schemes correspond to specified classes of service via queuing methods listed below, and are actively employed by operations personnel to manage, arbitrate or preempt access to network resources:

- First-in, first-out (FIFO) queuing with finite connection time limits supports Best Effort CoS
- Priority queuing (PQ) with Medium and Low queue weighting supports both Priority and Best Effort CoS
- PQ with Normal, Medium and Low queue weighting supports High Priority, Priority and Best Effort CoS
- Weighted fair queuing (WFQ) with Critical, Normal, Medium and Low queue weighting supports Critical, High Priority, Priority and Best Effort CoS

- Class-based queuing (CBQ) supports Pre-Emptive, Critical, High Priority, Priority and Best Effort CoS

Figure F-2: Common Operational Criteria Representative Framework

User Authentication Types	***Network Service Authorization Levels***	***Resource Precedence States***	***Classes of Service (CoS)***	***Traffic Management Schemes***
Support	Routine	No Precedence to No Precedence Default	Best Effort	**FIFO**
Support	Imminent	Precedence to Precedence Default	Priority	**PQ Med & Low**
Support	Sustaining	Precedence to Precedence Default	High Priority	**PQ Normal, Med & Low**
Essential	Response	High Precedence to High Precedence Default	Critical	**WFQ**
Essential	Response	High Precedence	Pre-Emptive	**CBQ**

User Authentication + Service Authorization + Precedence = Class of Service è *Queuing Method*

F.2.4 Common Operational Criteria Framework

Support for the Pre-Emptive service class requires the network to assign resources on a virtually unrestricted basis in support of highly critical essential users. The preferred traffic management queuing method is class-based, which permits network operations and management personnel to manually clear existing connections in favor of highly critical incoming requests or allow the network to manage access and resources through autonomous flow-based criteria. In all classes of service, network connectivity ensures access to network applications. Therefore, access to applications occurs as a result of authorization to use the network resources needed to establish connectivity with any hosts, databases and servers. A pre-emptive CoS involves policy decisions and authorization.

Within the NGN it is essential that:

1) A common operational criteria is defined for user authentication, network resource authorization, and precedence that permit definition of multiple classes of service for networks participating in the NGN.

2) Traffic management schemes are implemented supporting fair access, arbitration and priority treatment/pre-emption of network resources end-to-end.

F.2.5 NS/EP Capability Assurance

A planning, design and response criteria for the NGN is based on the summation of criteria successfully implemented by individual constituent networks. Therefore, a "global" NGN is a confederation of networks, cooperatively merged in response to common NS/EP events, which benefits from a cohesive end-to-end integration of best practices learned and implemented at a local network level. NGN planners and implementers focus on two issues concurrently: designing a resilient network that meets and exceeds user requirements at a local, regional, national and international level; and, maintaining local user and services priorities across an extensive NGN network environment.

The purpose of the NGN is to provide highly available and resilient network access, transport and services on a local and national basis, in support of myriad NS/EP scenarios. Availability and resiliency of the NGN will be enhanced over time as the evolution from an overlaid and inter-working network environment into a seamless and functional NGN environment is completed. Success of this migration, including peer-to-peer capabilities, depends on the ability of planners and implementers to continually support user requirements and expectations of service on a geographically dynamic basis.

Networks integrated into the NGN to support NS/EP activities are designed to satisfy user requirements for local network services, directly connected (adjacent neighbor) networks, and other networks as required. Agreed-upon common operational criteria are developed, disseminated and enforced both locally and between adjacent neighboring networks. Common operational criteria focuses on acceptable methods of user authentication, network resource authorization, and precedence, based upon the scope and severity of any NS/EP event at a local, regional national or international level; and successfully bind multiple networks together, as required, into a flexible and highly responsive NGN. End-to-end network availability and service support is achieved *a priori* by coordination of multiple connected networks, linked together both physically and logically via common operational criteria accepted and enforced among adjacent networks.

Maintaining end-to-end service priority across the NGN is based on supporting homogeneous CoS at a local, regional and national level. Enablement and support of multiple user and services priorities is part of the common operational criteria between connected networks within the NGN. Depending upon the scope and severity of an NS/EP event, local network policy may be supplanted by a common operational criteria agreement to provide connectivity, bandwidth and resource priority to external network users in times of emergency.

Within the NGN it is essential that:

1) The NGN meet or exceed user requirements at a local, regional, national and international level, and ensure consistency and continuity of user and services priorities throughout the NGN.

2) CoS are defined, based on common operational criteria, and are supported by all applicable network participants within the NGN.

F.3. Important Technologies

The requirements of the various NS/EP user scenarios on NGN will require a variety of technologies — some existent and some emergent. The technologies, protocols and methodologies recommended here are well understood, offering clear benefits that make their use in the NGN highly conceivable and perhaps inevitable.

F.3.1 Implications of the Internet Protocol

The current Internet Protocol Version 4 (IPv4) has served as the underlying protocol for the Internet for almost 30 years. Its robustness, scalability, and range of features are now being challenged by the growing need for new and abundant IP addresses, spurred in large part by the rapid growth of new network-aware terminals and appliances, and IP-based multimedia services, such as online or peer-to-peer interactions and Voice over Internet Protocol (VoIP). Internet Protocol Version 6 (IPv6) is a critical technology that ensures that the Internet can support a continually expanding user community worldwide. This technology will accelerate global broadband deployment, and promote proliferation of IP-connected capabilities and devices. IPv6 focuses on a number of prominent issues encountered in today's Internet. While the greatly increased addressing capability is a primary benefit, the most important difference between the two protocols lies in with the utility of the expanded address space available in IPv6. By incorporating critical capabilities, such as hierarchical addressing structure, flexible security mechanisms, and user mobility, IPv6 supports new computing and communication models that are difficult to support using the IPv4 protocol. Two features of particular importance to NS/EP users may be the auto-configuration and neighbor discovery capabilities of IPv6, which would enable NS/EP devices to quickly locate other IPv6 devices for call routing and communications. Further the simplified and extensible header in IPv6 also provides NS/EP planners an opportunity to request a certain quality of service. With IPv6, applications and services can be readily developed and deployed, and will function effortlessly, without requiring complex network configurations and routing schemas, cumbersome management supervision, or special server deployments.

F.3.2 Key Benefits of IPv6 Compared with IPv4

F.3.2.1 Expanded Addressing Space

When the IPv4 protocol's address space was first designed in the late 1970s, its exhaustion was regarded as inconceivable. However, due to advances in technology and address allocation

practices that did not anticipate a virtual explosion of devices connected to the Internet, the IPv4 address space was rapidly consumed. By 1992, it became apparent that a replacement protocol should be designed. The address space in the IPv6 protocol is 128 bits, supporting 340,282,366,920,938,463,463,374, 607,431,768,211,456 (3.4x1038) possible IP addresses. The IPv4 address space is comparatively small at 32 bits.

F.3.2.2 Highly Efficient Routing Infrastructure

Global addresses used on IPv6 segments of the Internet are designed to create an efficient, hierarchical, and easily summarized topology and routing hierarchy that is based on the common occurrence of multiple Internet service provider levels. On the IPv6 portions of the Internet, backbone routers have smaller routing tables, which correspond with routing formats of the global Internet service providers (ISPs). Developments in multi-homing show promise for future innovations such as redundancy, load balancing, and network congestion detection and management. A site is considered to be multi-homed when it connects to more than one service provider.

F.3.2.3 Enhanced Security

Private communications over a public medium, including the Internet, require secure services that appropriately protect digital information from being monitored or modified while in transit. Although an IPv4–based standard, known as Internet Protocol security (IPsec), provides security for data packets, use of this standard is optional. As a result, proprietary solutions are prevalent. In IPv6, IPsec support is a requirement of the protocol, providing standards–based network security for devices, applications, and services, while promoting interoperability among differing IPv6 implementations. IPv6 resolves additional security issues that cannot be solved using IPv4.

F.3.2.4 Mobility Support

IPv6 allows network nodes to be highly mobile, permitting arbitrary changes in location on an IPv6 network while maintaining existing connectivity. When a node connected by either IPv4 or IPv6 changes its location in the network, it typically changes its IP address as well. Without mobility support, which is not easily achievable in IPv4, loss of connectivity with peers results. With mobile IPv6 in use, the mobile node is always reachable through one permanent address. A connection is established with a specific permanent address assigned to the mobile node; and remains connected no matter how often the mobile node changes locations or acquire temporary-use addresses. Packets may be routed to the mobile or nomadic node using its permanent address regardless of the node's current point of attachment (i.e., location) to the service network or the Internet. The node (mobile or nomadic) continues to communicate with other nodes, either stationary or mobile, after transferring on to a new link. The movement of a mobile or nomadic node away from its home link, therefore, is transparent to a transport protocol, any higher-layer protocols, and/or applications. The Mobile IPv6 protocol is suitable for mobility across both homogeneous media and heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another, as well as node movement from an Ethernet segment to a wireless LAN cell. The mobile node's IP address remains unchanged regardless of movement. Another example could involve movement and

recognition of a device from a home to a mobile environment, or some other nomadic capability the NGN and IPv6 may enable.

Mobile IPv6 protocol addresses network-layer mobility management issues as well. Some mobility management applications, such as handoff among wireless transceivers, which cover only a very small geographic area, are solved using link-layer techniques. For example, in many current wireless LAN products, link-layer mobility mechanisms support handoff of a mobile node from one cell to another, dynamically re-establishing link-layer connectivity to the node in each new location.

F.3.2.5 Other IPv6 Capabilities

Other representative capabilities in IPv6 that support NS/EP requirements are listed below:

- Multiple IP addresses that disconnect identities and their IP addresses.
- Improved confidentiality through temporary IP addresses used by key individuals (POTUS) to reduce the likelihood of profiling or tracking their communications
- Multiple IP addresses that connect identities, devices and their IP addresses; especially useful for Public Safety NGN capabilities and effective peer-to-peer interactions
- Automatic self-configuration and self-healing, permitting a network to be established or re-established rapidly in response to an NS/EP contingency
- Mobile IP feature in IPv6 enabled devices to move around the Network, or even into other networks, without losing connectivity (described above)

F.3.2.6 IPv4 to IPv6 Transition Considerations

A transition from IPv4 to IPv6 is not a trivial migration, but is a complex transformation, or evolution, from one network protocol to another. Initial interest in IPv6 in the 1990s was based on a perceived shortage of addressing space and lack of security features available with the IPv4 protocol. Renewed interest in IPv6 today is based on a number of factors, including: leveraging an extensive address space for emerging network applications, enhancing user mobility across multiple networks, and supporting granular quality of service (QoS) capabilities throughout a geographically distributed network, such as the NGN. Transformation planning from IPv4 to IPv6 focuses on supporting both networking protocols concurrently, and today is an essential success factor of NGN implementations. IPv6 is an increasingly significant capability for enterprise networks requiring international connectivity.

Protocol translation and encapsulation, known as tunneling, are two key techniques used to support a mixed protocol (IPv4 and IPv6) operational environment. Therefore, networking equipment in the NGN is required to be dual-stacked, capable of operating as either IPv4 or IPv6 compliant. Emerging IPv6 networks are, and can continue to be, inter-linked with legacy IPv4 networks using either protocol translation or tunneling mechanisms to route IPv6 traffic in IPv4 packets. Network equipment interoperability and open standards-based compatibility are crucial in mixed IP protocol operational environments.

Maintaining consistency and continuity of common operational criteria in a mixed protocol environment is a complex challenge, requiring deliberate coordination and management of authentication, authorization, priority and service class credentials among networks using either the IPv4 or IPv6 protocol. Seamless network-to-network trust relationships, based on the use of centralized registration databases or distributed user credentials, are essential among constituent networks comprising the NGN to facilitate unimpeded access to network resources, once initial user authentication and network authorization transactions are successfully performed.

NS/EP service requirements for the NGN are readily supported by migrating to an IPv6 transport backbone and IPv6-enabled applications. As noted above, IPv6 provides enhanced network security via IPsec and additional integrated features of the protocol. The dynamic mobility capabilities of IPv6 support ad hoc networking applications and are readily adaptable to resilient peer-to-peer network designs. Additional security applications and software can be applied to trusted users via network edge or device to further enhance security measures.

Within the NGN it is essential that:

1) The NGN be planned, designed and implemented as a mixed protocol operational environment, capable of supporting current and anticipated user requirements with either IPv4 or IPv6 network connectivity.

2) Trust relationships to maintain and preserve the consistency and continuity of common operational criteria, including authentication, authorization, priority and service class definitions, throughout the NGN, are developed and implemented seamlessly from end to end.

F.3.3 Peer-to-Peer Networking

Peer-to-peer (P2P) networking offers a distributed alternative to legacy centralized network structures, and offers value during times of network stress or compromise to infrastructures or services. Characteristic features of P2P networking include:

- Applications are available when the network path between peers is available. No other supporting infrastructure is required to enable this connectivity. This allows a specific group of NS/EP users to fully utilize P2P-based applications even though this user community may be isolated from the greater NGN. For example, emergency workers, using mobile devices in a devastated area, are readily able to send and receive text and images between themselves on an isolated network.

- Instant messages (IM) using conventional messaging service require establishment of two sessions, with one between the sender and the messenger cloud and a second between the recipient and the messenger cloud. By use of peer-to-peer networking, bandwidth use is highly efficient, in that the IM session message traffic passes only between the connected peers.

- Communication between two entities, without connectivity to intermediaries, increases overall confidentiality. As an example, two NS/EP users on wireless VoIP phones are able to converse directly without requiring any additional support infrastructure. Another benefit of this scenario is lower latency between local and remote users due to the shorter distances required to connect them as peers. Note that P2P application may involve policy and management decisions of command entity due to resource allocation and traceability/dispatch needs. This is a typical case for Public Safety jurisdictional networks and incident command.

P2P communication techniques can be applied at the application level or at the network level. When used at the application level, two parties can communicate with each other as long as they have network connectivity with each other, without dependence on other infrastructure services. The network connectivity may be provided by centralized infrastructure through which messages are routed to the two peers.

Alternatively, the two peers may have network level connectivity with each other that does not require or depend on centralized infrastructure. In such cases the connectivity may be provided by a mesh or ad hoc network composed of devices connected using P2P communication techniques. For this reason, Common Operational Criteria among providers of constituent mesh and overlay networks should be established, as an integral component of an overarching NGN security policy. (*See Report, Section 6.7.*)

Network level P2P communication frameworks have the advantage of being fully distributed, scalable, and cost-effective to deploy on either a short- or long-term basis.

Peer-to-peer networks, elements and systems should play a key role in NGN end-to-end service for dedicated, mobile, and ad hoc users supporting NS/EP activities
Within the NGN it is essential that:

1. Peer-to-peer networks, elements and systems are integrated into the NGN long-term system design and standardization strategy to ensure effective connectivity for dedicated, mobile and ad hoc users supporting NS/EP activities.

2. Common operational criteria among constituent peer-to-peer and overlay networks supporting NS/EP activities be established, disseminated and enforced, as an integral component of an overarching NGN security policy.

F.3.4 Meshed Network Environments

Already recognized as an important component of the NGN, it is important to consider that P2P and IPv6 are easily optimized in mesh networking environments.

Advantages of mesh networks include:

- No single point of failure, which enhances resiliency; A percentage of the network remains intact and usable even though large segments of the overall meshed architecture is rendered unusable; and

- Easily configured, in that the incremental and distributed nature of a mesh network is more readily configured and built-up incrementally, especially in locations without pre-existing infrastructure.

In a typical NS/EP scenario, individual networks are integrated into a *de facto* full or partial "mesh" of wireline, wireless, satellite, private networks and worldwide Internet elements, as applicable and appropriate to mission. An NS/EP contingency requires heterogeneous environments to quickly and effectively support high availability, resiliency and security from an end-to-end services perspective. However, to support communications in these scenarios, a consolidation of myriad homogeneous (and often single-purpose) networks optimized for a dedicated user community is required. Methods for authenticating users, reserving network resources and bandwidth, assigning priority classes, enforcing end-to-end security policy, and determining optimal routes for data and management traffic among networks vary greatly. In the NGN, interconnectivity is based on deployment of an overlay, peer or hybrid architecture to support services end-to-end across multiple networks.

Current national and international standardization activity is examining the potential importance of mesh networking, especially for first responders.

F.3.5 Role of IPsec

The evolution of the NGN is based predominantly on the use of common elements like Internet Protocol (IP). IPsec is a security mechanism designed specifically for enhancing the security of the IP. It provides increased security capabilities in support of NS/EP event scenarios. IPsec isolates and protects user services and applications on the NGN, ensures authenticated access to services, ensures the authenticity of communication, preserves the integrity of messages and supports communications confidentiality.

The following capabilities of IPsec are available singly or in combination:

- User authentication;
- Device authentication;
- Integrity and authenticity of communication; and
- Confidentiality of communication.

F.3.6 Combined Use of Technologies

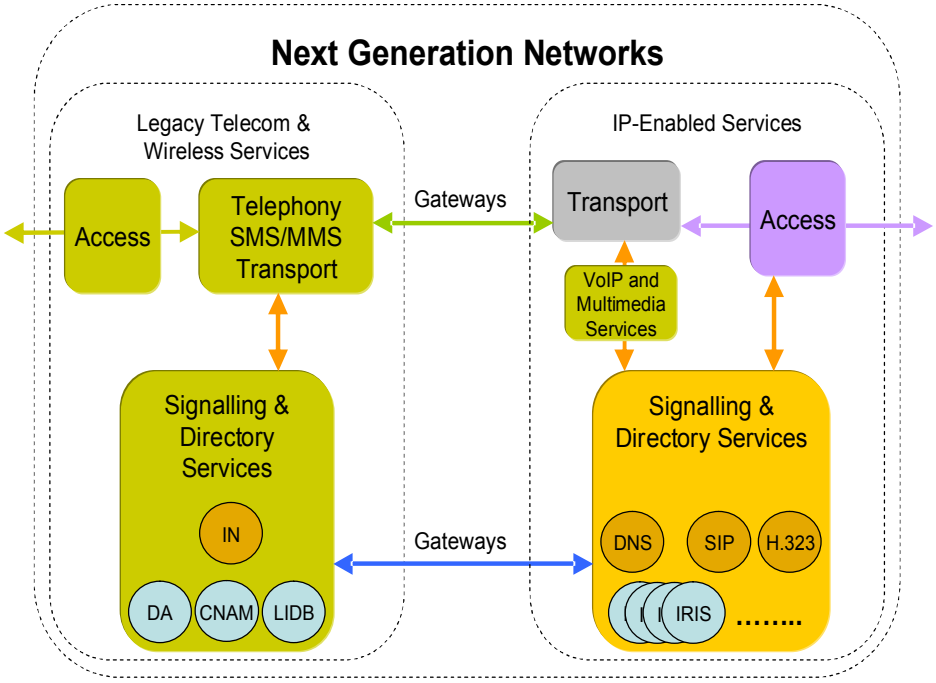
The technologies described above are individually useful but become much more so when used in combination. An example includes a set of users entering an area without infrastructure. Their user devices will auto-configure themselves and discover each other (e.g., a specific IPv6 characteristic) and can begin to communicate using P2P or other applicable connections. Similarly, the use of IPsec to preserve confidentiality and authentication of communication

becomes more important in a meshed network environment, for example, where the possible paths between two or more entities are numerous. In such situations, it is difficult to establish and ensure a level of trust among many connected devices. Support by the Federal Government Science and Technology community of full scale demonstrations of how these technologies can be used to enhance NS/EP capabilities within the NGN is vital to rapid progress and establishment of best practices for those with NS/EP requirements.

F.3.7 Transition and interaction of directory services

Further as the telecommunications world evolves another critical requirement will be the capability to enable communications between the "legacy" and the NGN environments. VOIP subscribers connecting with tradition "plain old telephone systems" (POTS) users is a current example of an application that operates end-to-end and crosses both environments. The directory services associated with routing and electronic numbering are developing between these environments and the interoperability challenge is depicted in the following diagram.[3]

Figure F-3. Interoperability: Signaling & Directory Considerations



Another recent example of a critical public safety service of the POTS environment that will need to be available in the NGN environment is enhanced 911 (E911) emergency services.[4] This

[3] International Telecommunication Union, Study Group 2 – Delayed Contribution 49, December 6-15, 2005

[4] See "First Report and Order and Notice of Proposed Rulemaking (FCC 05-116),"May 19, 2005, that it would require interconnected VoIP providers to provide E911 service. In its announcement the FCC noted; "The IP-enabled services marketplace is the latest new frontier of our nation's communications landscape, and the Commission is committed to

is a precedence setting example of how critical existing services that we rely upon for public safety will need to be developed for the NGN environment. Additionally, in 2003, the FCC recognizing the need to speed full implementation of E911 and greater coordination among all stakeholders, undertook a "Coordination Initiatives" to complement current efforts by involved parties to speed and rationalize the E911 deployment process, and to ensure that the all parties and the public have clear expectations about the roles of the respective parties and deployment plans. This further provides insight on scope of coordination efforts that will be required for assuring the NGN can meet NS/EP community needs.

Such coordination will be required to establish electronic numbering (ENUM), or telephone number mapping, either at carriers, infrastructure level or both, to meet the public/end user needs within the NGN for integrated services and mapping to the legacy public switched telephone network (PSTN) environment, as PSTN inter-working will be required for a long time. Facilitation activities and coordination among stakeholders will be required to achieve such integrated solutions for the NGN, along with necessary standards.

F.4 Conclusion

As the NGN is in an early implementation stage, actual access, transport, and service availability today may not fully support anticipated NS/EP user requirements. It is a responsibility of the Federal Government to ensure that NS/EP requirements are articulated and coordinated among its users, standard bodies and the broad range of service providers. In order for the NGN to broadly meet essential NS/EP community requirements in a consistent, continuous and reliable manner on an end-to-end basis, common operational criteria must be defined and adopted by entities supplying network access, transport and infrastructure services for this community.

allowing IP-enabled services to evolve without undue regulation. But E911 service is critical to our nation's ability to respond to a host of crises. The Commission hopes to minimize the likelihood of situations like recent incidents in which users of interconnected VoIP dialed 911 but were not able to reach emergency operators. Today's Order represents a balanced approach that takes into consideration the expectations of consumers, the need to strengthen Americans' ability to access public safety in times of crisis, and the needs of entities offering these innovative services."

APPENDIX G

SYSTEMATIC ASSESSMENT OF NGN VULNERABILITIES

G SYSTEMATIC ASSESSMENT OF NGN VULNERABILITIES

G.1 Background

This Appendix provides additional background (developed by the Vulnerabilities and Threat Modeling Working Group) on NGN vulnerabilities relevant to the conclusions and recommendations of the Next Generation Networks Task Force (NGNTF), which are contained in the main body of the Report.

G.2 Systematic Assessment

The vulnerabilities of the NGN were studied systematically[5] to determine the vulnerabilities of the NGN; the analysis included:

- A suitable framework for vulnerability assessment
- A comprehensive list of intrinsic vulnerabilities of the NGN ingredients
- Relevant trends that affect the exposure of the vulnerabilities
- Evaluation of significance of each vulnerability in the NGN

The framework selected to study NGN vulnerabilities was one already regularly used in several industry-government-academic fora.[6] The framework consists of the eight ingredients with which the communications infrastructure is built. This framework is comprehensive in the sense that all the things needed for the full operation of a communications network are included. As shown in Figure G-1, below, it also recognizes the role of other infrastructures.

[5] Over one hundred subject matter experts were included in this analysis, representing knowledge and operational experience from each of the eight ingredients that make up the framework.

[6] Rauscher, Karl. F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004; Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop, www.comsoc.org/~cqr; *Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report*, Issue 3,December 2003, *NRIC VII Wireless Network Reliability Focus Group Final Report*, Issue 3, October 2005, *NRIC VII Public Data Network Reliability Focus Group*, Issue 3, October 2005 (www.nric.org), and the *ATIS Network Reliability Steering Committee (NRSC)2002 Annual Report* (www.atis.org/nrsc).

Figure G-1. Communications Infrastructure Ingredients and Dependencies [7]

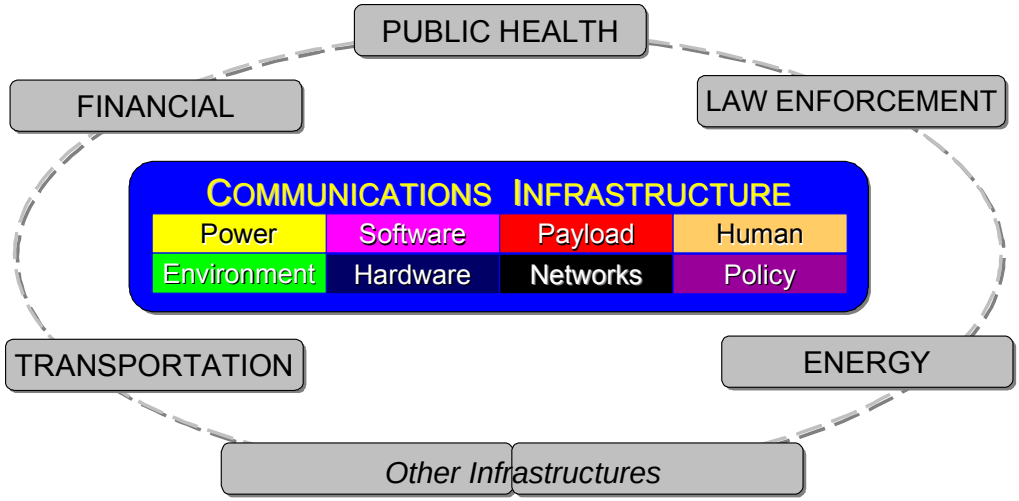


Figure G-2, below, is provided for explanatory purposes. It is an example table of the vulnerabilities lists that are provided in the following pages for each of the eight ingredients. The first column provides a comprehensive list of the vulnerabilities for that ingredient. Vulnerabilities are defined as "a characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise."[8] The second column indicates the exposure of each vulnerability in the NGN relative to legacy networks. The third column indicates the impact of significant trends, which are listed below each table.

Figure G-2. Example Ingredient Vulnerability List

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
attrribute i	-	a
attribute ii	=	a, b
attribute iii	+	n.a.

[7] *Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report*, Issue 3, December 2003; Rauscher, Karl. F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.

[8] *Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report*, Issue 3,December 2003, page 39.

G.2.1 Power

The Power ingredient includes the internal power infrastructure, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
uncontrolled fuel combustion	=	
fuel contamination	=	
fuel dependency	=	
battery combustion	=	12
battery limitations	=	6
battery duration	=	1
maintenance dependency	=	1, 4, 5, 7
require manual operation	=	4
power limitations	=	5, 8
frequency limitations	=	2
susceptibility to spikes	=	
physical destruction	=	7

Significant Trends Related to NGN Power Vulnerabilities

1. Network access devices are no longer powered by network elements (many devices do not have back-up power)
2. Increased reliance on A/C, which has more components
3. Higher voltage UPS systems have more cells in series
4. Higher voltage increases safety and training attention
5. Increased dependence on back-up power for cooling
6. A/C UPS back-up systems are currently not highly reliable
7. Increased regulation from local codes (e.g., sprinklers, battery disconnect switches) decreases reliability
8. Increased use of 208/240 V power systems because of higher density in data centers
9. Decreasing size of many locations suggests lower engineering level of back up power
10. Increased use of embedded systems ("boxes" used as commodities)
11. Decreased power consumption
12. Battery combustion concern is decreasing do to better battery design and technology
13. Increasing use of public and remote sites
14. Increasing use of network-based, software-controlled, power management systems

G.2.2 Environment

The Environment ingredient includes buildings, trenches where cables are buried, space where satellites orbit, locations of microwave towers and cell sites, and the ocean where submarine cables reside.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
accessible	=	3, 6
exposed to elements	=	2, 6
dependence on other infrastrucures	=	2, 4, 6
contaminate-able	=	6
subject to surveillance	=	2, 3, 6
continuously being altered	=	5, 6
identifiable	=	1, 2, 3
remotely managed	=	2, 3, 4
non-compliance with established protocols and procedur	=	4, 6

Significant Trends Related to NGN Environment Vulnerabilities

1. Some environments may be less significant with broad mesh distribution of functionality
2. Increasingly mobile
3. Increasingly be virtual
4. Increasingly have cooling challenges
5. Increasingly may not have a back-up
6. Increasing reliance by some on "hot spots" — more public and less under control

G.2.3 Hardware

The Hardware ingredient includes the hardware frames, electronic circuit packs and cards, and metallic and fiber optic transmission cables and semiconductor chips.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
chemical (corrosive gas, humidity, temperature, contamination)	=	11
electric (conductive microfiber particles – carbon bombs)	=	
radiological contamination	=	
physical (shock, vibration, strains, torque)	=	6
electromagnetic energy (EMI, EMC, ESD, RF, EMP, HEMP, IR)	+	12
environment (temperature, humidity, dust, sunlight, flooding)	=	3
life cycle (sparing, equipment replacement, ability to repair, aging)	=	7
logical (design error, access to, self test, self shut off)	+	4,6,9,10,15,16

Significant Trends Related to NGN Hardware Vulnerabilities

1. More portable hardware introduces more dependencies on various power capabilities
2. Widespread impact of a single mode of failure more likely with increasing use of common hardware across vendors
3. Increasing density of logic generates more heat
4. Sabotage or malicious design insertion may be more likely due to increasing trend of offshore outsourcing
5. Increasing capacity of transmission facilities
6. Increasing capacity of single devices increases their value and importance
7. More rapid technology turnover (decades to years)
8. Increasing storage of sensitive information on hardware
9. May be more common for hardware to include tamper detection and tamper response
10. Increasing ability to access and control remotely (in-band control considerations)
11. Increasing use of non-NEBS compliant devices
12. Increasingly smaller footprint results in smaller gaps between components on circuit cards - greater challenge for short circuits and physical integrity
13. Fewer large, centralized systems being replaced with more, smaller distributed systems
14. End user equipment is becoming much more sophisticated
15. Increasing complexity of devices
16. Increasing availability of capability to do firmware and microcode updates

G.2.4. Software

The Software ingredient includes the physical storage of software releases, development and test loads, version control and management, and chain of control deliver.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
ability to control (render a system in an undesirable state, e.g., confused, busy)	+	5, 18, 22, 23
accessibility during development (including unsegregated networks)	+	8, 11
accessible distribution channels (interception)	+	5, 8, 18, 23
accessibility of rootkit to control kernal/core	+	5
developer loyalties	+	11, 18
errors in coding logic	+	11, 13, 14
complexity of programs	=	13, 14, 18
discoverability of intelligence (reverse engineer, exploitable code disclosure)	+	5, 6, 29
mutability of deployed code (patches)	+	8,19,21,23,24
incompatibility (with hardware, with other software)	+	15,17to20,26

Significant Trends Related to NGN Software Vulnerabilities

1. Increased risk of over-the-air exploitation (re-keying of encryption for end user radios, gain access or intercepting upgrades, change user profile/identity)
2. Increasing use of wireless-installed software
3. Increased use of artificial intelligence (rules-based expert systems)
4. Increased risk of widespread logical single point of failure
5. More use of embedded operating systems (can be altered with in-band control)
6. Prevalence of worms and viruses common to PCs will increasingly be used as an attack vector for public networks
7. More authentication occurring at the application layer
8. More use of open source systems (tampering more of a concern) — move away from propriety code
9. Increasing risk of confidentiality failure (leak of information . . . who called whom)
10. Increasing availability of malware
11. Increasing exposure through offshore development
12. Increasing concern of mis-authorization elevating someone's privileges
13. Comprehensive inspections continue to be impractical — potential impact is getting worse
14. Software testing tools are improving
15. Continued need to support legacy code (transition issue)
16. New releases increasingly have ability to fall back on previous version
17. Increasing exposure of legacy code to new unconstrained environment
18. Shift toward service-oriented architectures (control given to many new parties, complexity of possible permutations of software component assembly is too large)
19. Patch management has a bigger impact because more of the network is based on software — more far reaching impact, more failure mode effects analysis needed
20. Configurability of software maybe more difficult
21. Network is a system of systems — patching can have large cascading effects
22. Increasing role of traffic restrictions — software will control what is and is not supposed to be there (priority services)
23. Increasing need for prioritized patch messages (fix a collapsed network using in-band management)
24. Anticipated increased use of software-controlled radios
25. More capable end-user devices
26. Increasing complexity of interfaces between systems

More incentive for people to learn the open protocols

G.2.5 Payload

The Payload ingredient includes: the information transported across the infrastructure; traffic patterns and statistics; information interception; and, information corruption. It includes both normal and signaling and control traffic.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
unpredictable variation	+	1, 6, 8, 10
extremes in load	+	1, 2,
corruption	=	5, 7, 8, 10
interception	=	2, 3, 4, 7
emulation	+	2, 3, 4, 7
encapsulation of malicious content	+	2, 7, 8
authentication (mis-authenticaton)	+	2, 3
insufficient inventory of critical components	=	1, 2
encryption (prevents observablity)	+	12

Significant Trends Related to NGN Payload Vulnerabilities

1. Includes many types of services (voice, data, video)
2. Increasing sophistication regarding prioritization
3. IP address tracking allows identity in header
4. Increased spoofing concerns
5. Increased concern for NS/EP needs to get a message through with "one shot"
6. New capabilities to control and provision bandwidth dynamically
7. Co-mingled traffic and control messages
8. Session persistence permits session hijacking
9. New challenges for AJ/LPI/ LBD (anti-jamming, low probability of intercept, laser beam detection) effects on NS/EP communications
10. More variation in Quality of Service
11. Increased concern of channel hijacking
12. Increasing challenge for preventing a negative impact from concealed messages in encrypted or otherwise hidden content
13. Service providers may give out information that can be used against its own networks and there is much data to be mined

G.2.6 Networks

The Network ingredient includes: the configuration of nodes and their interconnection; network topologies and architectures; various types of networks, technology, synchronization, redundancy, and physical and logical diversity; and network design, operation and maintenance.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
capacity limits	+	4, 9, 12, 14
points or modes of failure	=	2, 3, 6, 7, 14
points of concentration (congestion)	-	3, 5, 6, 14
complexity	+	1, 2, 5, 6, 7, 9
dependence on synchronization	=	2, 7, 20
interconnection (interoperability, interdependence, conflict)	+	2,8,10,13,14
uniqueness of mated pairs	-	13
need for upgrades and new technology	+	5,12,14,15,19
automated control (*via software)	+	1, 5, 6, 11
accessibility (air, space or metallic or fiber)	+	4, 8, 12
border crossing exposures	=	4, 8

Significant Trends Related to NGN Network Vulnerabilities

1. Shift from reliance on silicon to software
2. Departure from deterministic to non-deterministic path control
3. Shift from circuit to packet entails losing a dedicated path
4. Increasing presence of wireless increases exposure to blocking and sniffing
5. New capabilities to control and provision bandwidth dynamically
6. New real-time reconfiguration of network resources
7. Increased diversity of network practices of interconnected networks
8. Increased sensitivity of AJ/LPI/ LBD (blocking, interception) effects on NS/EP communications
9. More variation in Quality of Service
10. De-segregated traffic and control messages in payload
11. Increased use of artificial intelligence
12. More diverse modes of access
13. Non-homogeneous distribution of vulnerabilities
14. High bandwidth and powerful computing capabilities are increasingly common
15. Increasing sophistication of PSAP communications
16. Increasing concern over channel hijacking
17. Emergence of IPv6
18. Increasing use of grid and peer to peer networking (versus client-server architecture)
19. More security exploits require more software patching
20. Increasing concern over being used for harm (GPS, end user device detonation triggers)

G.2.7 Human

The Human ingredient includes: human involvement throughout the entire lifecycle of activities related to the communications infrastructure (design, implementation, operation, maintenance and de-commissioning); intentional and unintentional behaviors; limitations; education and training; human-machine interfaces; and, ethics and values.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
physical (limitations, fatigue)	=	1, 6
cognitive (distractibility, forgetfulness, ability to deceive, confusion)	=	1, 3, 4, 7
ethical (divided loyalties, greed, malicious intent)	=	2, 5, 6
user environment (user interface, job function, corporate culture)	=	1, 5, 6
human-user environment interaction	=	2, 3, 6

Significant Trends Related to NGN Human Vulnerabilities

1. Competitive challenges result in increasing work overloads
2. Increased use of biometrics (can introduce higher rejection or false positive rates)
3. Complexity takes longer time to progress along learning curve
4. Deployment of technology increasing outpaces availability of accurate and complete documentation
5. Increasing use of wireless connectivity increases dependence on authentication and authorization
6. Increased frequency of virtual and remote teams weakens social cohesion (emergency response teams, trusted environments)
7. Training and procedures remain key to familiarity

G.2.8 Policy

The policy ingredient includes: behaviors between entities, namely agreements, standards, policies and regulations (ASPR); national and international scopes, as well as Federal, State and local levels; other legal issues; and any other arrangement between entities, including industry cooperation and other interfaces.

VULNERABILITY	PRESENCE in NGN vs LEGACY	AFFECTED by TREND*
Lack of ASPR (agreements, standards, policies, regulations)	+	1,4,5,7,9,15
Conflicting ASPR	+	3,4,5,7,13,15
Outdated ASPR	+	1, 4, 5, 7, 8, 15
Unimplemented ASPR (complete or partial)	+	6,8,9,10,11,13
Interpretation of ASPR (mis- or multi-)	+	9, 13, 15
Inability to implement ASPR	+	3, 6, 9, 10
Enforcement limitations	+	2, 3, 15
Boundary limitations	+	2, 3, 6, 15
Pace of development	+	1,4,5,8,12,13
Information leakage from ASPR processes	=	2, 14
Inflexible regulation	=	2, 7, 8, 11, 15
Excessive regulation	-	2, 8, 10, 15
Predictable behavior due to ASPR	=	7, 14
ASPR dependence on misinformed guidance	=	8, 9, 13
ASPR ability to stress vulnerabilities	+	4, 7, 13
ASPR ability to infuse vulnerabilities	+	3, 4, 13
Inappropriate interest influence in ASPR	=	2, 9

Significant Trends Related to NGN Policy Vulnerabilities

1. Increasing need to redefine prioritization criteria (e.g., other infrastructures that support NS/EP)
2. Goal of protecting U.S. network is harder to distinguish with global interconnectivity of NGNs
3. Attribution and retribution framework is missing
4. Loss of functionality when inter-working between NGN and legacy networks,
5. Need for mapping the multiple NGN priority levels to the one level in the legacy networks and vice versa
6. Lack of an agreement to carry an NS/EP call (wireless roaming)
7. Priority handling of 911 calls could drown NS/EP calls
8. Migration from Time Division Multiplexing (TDM) to IP networks
9. More and smaller service provider and network operators
10. Decreasing capital investment availability
11. Multiple modalities (video, data, voice)
12. Rapid deployment of IP replacing TDM, without ASPR
13. Rapidly increasing complexity of technical solutions
14. More ASPR work published on the Internet
15. Diverging views globally on the level of regulation needed for NGNs/ the Internet
16. Increasing use of wireless spectrum

APPENDIX H

NGN THREAT ANALYSIS

H NGN THREAT ANALYSIS

H.1 Background

This Appendix provides additional background on threats to the NGN relevant to the conclusions and recommendations of the Next Generation Networks Task Force (NGNTF), which are contained in the main body of the Report.

H.2 Threat Analysis

Threats to the NGN were studied using NGN-specific threat modeling[1] approach focusing on both NGN and national security and emergency preparedness (NS/EP) communications with a focus on cyber attacks, but which also examined blended cyber and physical attacks on the NGN. To conduct a threat analysis for the NGN environment, the NGN scenarios described above were taken and broken down into an appropriate collection of user classes that could be analyzed in a more granular fashion. These user classes represented unique user types and requirements[2] within each NGN scenario context.

Next, four levels of threat classes were identified based on motivations and capabilities, ranging from Class A, a nation-state or agency with extensive resources, to Class D, an individual with limited resources. These threat classes were evaluated not just based on resources but also on their motivations and their anticipated and developed cyber and kinetic capabilities (e.g., computer network attack, electronic warfare, psychological operations, military deception, kinetic).

As a final step is the threat modeling exercise, the NGN scenarios, user classes, and requirements were combined with the threat landscape and an analysis of susceptibility a particular user class (in the context of an NGN scenario) to the various threat actor classes was performed. The result was enumeration of the threat types to which each user class was likely to be susceptible. The analysis addressed threats to the confidentiality, integrity, and availability of information or services in an NGN environment. The threat types were based on the STRIDE classification method proposed by Howard and LeBlanc.[3] STRIDE denotes **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**scalation of Privilege. The threat analysis for the NGN environment and scenarios was primarily focused on cyber and/or blended cyber/kinetic attacks. The result of this exercise was a matrix detailing the anticipated and likely threats for each user class within the context of an NGN NS/EP scenario. In this analysis, several threat trends surfaced.

H.2.1 Widespread Susceptibility

Most user classes were susceptible to significant threat types from virtually every threat actor class. For example, in the Continuity of Government scenario, information disclosure and denial

---

1 As one example, see Microsoft's Threat Modeling methodology as published by Swiderski and Snyder, ISBN: 0735619913.

2 See Section 4 of this Report.

3 See NGN Scenario Threat Profile matrix below for more information on STRIDE. Also see Howard and LeBlanc, STRIDE Classification for Threat Modeling.

of service are significant threats to all user classes including the National Command Authority (NCA). In addition, the most secure NCA mechanisms (e.g., nuclear launch) may be very unlikely to be threatened but other operational functions, such as emergency response authority, may be highly susceptible to a wide range of threat types.

H.2.2 Threat Actor Convergence

Due to the complex web of relationships between threat actors, the threat landscape has become converged leaving old methods of threat analysis potentially obsolete. For example, the growing financial motivation for cyber crimes has overshadowed motivations around personal fame and reputation for individual hackers. The likelihood of collaboration across threat classes is extremely high. For example, a nation-state, foreign intelligence service, terrorist group, or organized crime group could employ an individual hacker who is motivated by financial gain but does not necessarily share his employer's motivations and/or ideological views. Conversely, an individual hacker with no affiliation to a nation state or terrorist group might be sympathetic to the political or ideological cause and become a voluntary agent in the furtherance of that cause. Finally, the insider threat is not a standalone threat class but one that crosses all threat classes — there can be insiders in every scenario that are employed by any threat actor.

H.2.3 Network Convergence Threat Impacts

Convergence in the NGN environment will create an inherently more complex environment where various "planes" (i.e. control, data, user, etc.) are merged. Convergence creates a scenario where the threats and adversaries of the individual converged systems are inherited by the entire converged system. For example, a threat scenario unique to and perhaps well known to the public switched telephone network (PSTN) and not present for the Internet, would now be faced by all in the converged environment. In addition, traditional PSTN network security focus is only put on the network elements. In a converged network, the threat to data integrity/validity must also be examined in addition to threats to network elements. Convergence will present a greater threat to control systems as control and management networks via wireless, PSTN, and the Internet are converged. Finally convergence, legacy network interoperability requirements, the infancy of converged network management tools, and other factors in the NGN environment have made network management in the NGN environment increasingly difficult.[4]

The NGN Scenario Threat Profile Matrix, shown below, details anticipated threats for each user class within the context of an NGN NS/EP scenario.

[4] See the NSIE 2005 Assessment of Risks to the Security of the Public Network prepared by NSTAC/NCS.

NGN Scenario: Continuity of Government

Threat Classes:	Motivations	Capabilities[5]
A - Nation State/Agency (10^{12})	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B – Ideological/NGO (10^{9})	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (10^{6})	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (10^{3})	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
National Command Authority	Survivability Interoperability Broad Application Support Authentication Priority over Non-NS/EP Mobility NLA and/or Non-traceability Fail-secure only Content-aware security Emergency Alerts	Information Disclosure Denial of Service	Information Disclosure Denial of Service	Information Disclosure Denial of Service	None
Departmental-Level (e.g. DoD, DoS, DHS)	Survivability Interoperability Broad Application Support Authentication Priority over Non-NS/EP Mobility NLA and/or Non-traceability Fail-Safe and/or Fail-secure Communities of Interest Content-aware security Emergency Alerts	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service	Denial of Service
Regional, State & Local	Broad Application Support Interoperability Authentication Priority over Non-NS/EP Mobility Fail Safe (defaults to available) Communities of Interest Content-aware Security Emergency Alerts	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service

[5] See p. H-14 for explanation of Threat Class Capabilities.

CI Provider (Private or Public sector)	Survivability Interoperability Authentication Internal priority over Non-NS/EP Mobility Fail Safe and Fail Secure Content Aware Security	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service
General Public	Multi-lingual/Accessibility Broad platform support Broad Authentication Support Mobility Fail Safe Only Emergency Alerts	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

NGN Scenario: Critical Government Networks

Threat Classes:	Motivations	Capabilities
A - Nation State/Agency (10^{12})	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B – Ideological/NGO (10^{9})	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (10^{6})	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (10^{3})	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Financial Transaction Networks (e.g. FedWire)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Mobility Fail secure Content-aware security Services Restorability Secure networks International connectivity Interoperable Scalable bandwidth Reliability/Availability Network Location Awareness Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service
Government Operations Command and Control (e.g. FAA Air Traffic Control)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Fail safe Content-aware security Services Emergency alerts Scalable bandwidth Reliability/Availability Restorability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service

	Traceability				
Intelligence Networks (SIPR, JWICS, etc.)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Mobility Network-based location Awareness and/or non-traceability Fail secure Communities of interest Content-aware security Services Restorability International connectivity Scalable bandwidth Reliability/Availability Affordability Secure Networks	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service	None	None
Information Sharing Networks (HSIN, HSIN-Secret, CWIN, etc.)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Mobility Multi-lingual/Accessibility Fail secure Communities of interest Content-aware security services Emergency alerts Restorability Enhanced priority treatment Secure networks International connectivity Scalable bandwidth Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service

NGN Scenario: Critical Infrastructure – Control Systems (e.g., Supervisory Control and Data Acquisition, Process Control Systems, Digital Control Systems)

Threat Classes:	Motivations	Capabilities
A - Nation State/Agency (10^{12})	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B – Ideological/NGO (10^{9})	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (10^{6})	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (10^{3})	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Control Systems Management Entity (e.g., data historian server, application server, human machine interface, energy management system , operations support systems)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Fail safe Emergency alerts Restorability Secure networks Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Information Disclosure Denial of Service	Information Disclosure Denial of Service
Control Systems Network	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Fail safe Restorability Secure networks Ubiquitous coverage Scalable bandwidth Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service
Control Systems Endpoint (e.g., program logic controller, remote terminal unit, sensor, switch/relay)	Survivability Broad platform support and interoperability Strong, usable network authentication	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Tampering Information Disclosure Denial of Service

	Priority over non-NS/EP Fail safe Emergency Alerts Reliability/Availability Affordability	Elevation of Privilege	Elevation of Privilege	Elevation of Privilege	

NGN Scenario: Public Safety

Threat Classes:	Motivations	Capabilities
A - Nation State/Agency (10^{12})	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B – Ideological/NGO (10^{9})	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (10^{6})	Financial, Competitive Advantage	CNO, PO
D - Hacker/Individual (10^{3})	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Emergency Responder (e.g., Police, Fire, EMS, hospitals)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Mobility Network-based location awareness Fail safe Communities of interest Content-aware security services and/or transparency Emergency alerts Restorability Ubiquitous coverage International connectivity Scalable bandwidth Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service	Repudiation Information Disclosure Denial of Service
Government Public Safety Leadership (e.g., elected officials and staff)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Mobility Fail safe Communities of interest	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Information Disclosure Denial of Service	Information Disclosure Denial of Service

	Content-aware security services Emergency alerts Restorability Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service				
Media (e.g., TV, radio, print)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Mobility Multi-lingual/accessibility Relative priority Fail safe Communities of interest Emergency alerts Restorability Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service
Emergency Communication Networks (e.g., E-911, PSAP, WPS, SHARES)	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Mobility Multi-lingual/Accessibility Network-based location estimation Fail safe Emergency alerts Ubiquitous coverage International connectivity Scalable bandwidth Broadband service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

	Reliability/Availability Restorability Affordability Voice-band service				
General Public	Broad platform support and interoperability Broad application and data-type support Mobility Multi-lingual/Accessibility Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

NGN Scenario: General Public/Home User

Threat Classes:	Motivations	Capabilities
A - Nation State/Agency (10^{12})	Military, Intel, Industrial	CNO, EW, PO, MILDEP, Kinetic
B – Ideological/NGO (10^{9})	Force Multiplier, Ideological, Fear	CNO, PO, MILDEP, Kinetic
C - Organized Crime/Corporate (10^{6})	Financial, Competitive Advantage	CNO, PO
D - Individual/Hacker (10^{3})	Challenge, Recognition, Financial, Revenge, Coercion	CNO, PO

User Class	NGN Requirements	Threat Class A	Threat Class B	Threat Class C	Threat Class D
Roaming/Nomadic (e.g., hotspot, wireless)	Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Mobility Multi-lingual/Accessibility Network-based location estimation Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service Reliability/Availability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege
Home-based	Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Mobility (to nomadic) Multi-lingual/Accessibility Network-based location estimation Fail safe Communities of interest Emergency alerts Ubiquitous coverage International connectivity Broadband service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege

	Reliability/Availability Affordability Voice-band service				
Privileged NS/EP User – Outside of COG/CGN Scenario	Survivability Broad platform support and interoperability Broad application and data-type support Strong, usable network authentication Priority over non-NS/EP Mobility Fail Safe and/or fail secure Communities of interest Content-aware security Emergency alerts Secure networks Ubiquitous coverage International connectivity Scalable bandwidth Broadband service Reliability/Availability Non-traceability Affordability Voice-band service	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	Tampering Repudiation Information Disclosure Denial of Service	Information Disclosure Denial of Service

Notes

1. **Threat Classes**
    a. Threat classes are denoted based on their intentions/motivations and capabilities. In addition, a descriptive resource classification is used referring to the dollar value potential for a given class (e.g. $\$10^{12}$ for a nation-state).
    b. A certain degree of overlap in threat classes is understood and accepted as part of the analysis.
2. **Threat Capabilities Definitions**
    a. CNO - Computer/Network Operations (includes computer/network attack – CNA, computer/network exploitation – CNE, and computer/network defense – CND)
    b. EW - Electronic Warfare (including directed and non-directed energy weapons)
    c. PO - Psychological Operations (including social engineering, extortion, etc.)
    d. MILDEP - Military Deception (i.e. counter intelligence, counter-counter intelligence, etc.)
    e. Kinetic (Physical attack, damage, degradation, destruction, etc.)
3. **Threat Type/Classification**
    a. Threats to Confidentiality, Integrity, and Availability of information or service
    b. **STRIDE**: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**scalation of Privilege
    c. Threat analysis is primarily focused on cyber and/or blended cyber/kinetic attacks.
4. **Requirements**
    a. Requirements used are derived from the following two sources and several overlaps exist between the two taxonomies.
        i. NSTAC NGNTF Scenario and User Requirements Working Group (SURWG)
        ii. Federal Enterprise Architecture Functional Requirements
5. **Threat Applicability to Requirements**
    a. For a given threat type (STRIDE) there may or not be applicability to a specific requirement. Further analysis would be required to specify which of the requirements for a given user class would be impact by a given threat.

APPENDIX I

NGN AND NATIONAL SECURITY AND EMERGENCY PREPAREDNESS AGREEMENTS, STANDARDS, POLICIES, AND RECOMMENDATIONS ECOSYSTEM

I NGN NATIONAL SECURITY AND EMERGENCY PREPAREDNESS AGREEMENTS, STANDARDS, POLICIES, AND RECOMMENDATIONS ECOSYSTEM

Figure I-1 provides a brief description of selected work efforts underway in various agreements, standards, policies and recommendations (ASPR) bodies that are related to national security emergency preparedness (NS/EP) communications (excluding lawful intercept).

Figure I-1. Selected NGN NS/EP ASPR Activities

Type of ASPR	Body	Working Party	Work Description
International NGN Technology Standards	ITU-T	SG 2, 13, 16 and 19	§ Emergency Communications § SG 2 is developing the International Emergency Preparedness Scheme (IEPS) requirement
		SG 11	§ International Emergency Call Priority
	ITU-R	SG 8 (WP8F)	§ Emergency Calling and Priority Treatment § Geographic Location/Privacy for IMT-2000-ADVANCED
	GSC	GTSC/GRSC	§ Emergency Communications for Public Protection and Disaster Relief § Crash Notification and PSAP/Public Communication
	ETSI/TIA	MESA	§ Broadband Public Safety Partnership Project for User Requirements and Service/Feature Specifications
	ISO	TC 204 (WG 16)	§ Emergency Communications over Intelligent Transport Systems (ITS)
Global Internal Protocol (IP) Telephony & Internet Standards	IETF	WG geopriv	§ Emergency Calling Geographic Location/Privacy
		WG ecrit	§ Routing Emergency Calls to PSAPs § Security Threats to Emergency Calling
		WG ieprep	§ Emergency Telecommunications Service § Priority Services
		BOF GIG	§ Global Communications for Disaster Recovery § Global Information Grid (GIG)
European NGN Technology Standards	ETSI	EMTEL	§ Emergency Communications Network Resiliency § Emergency Communications between Authorities § Emergency Communications from Authorities to Citizens § Emergency Communications between

			Citizens § Emergency Messaging
North American NGN Technology Standards	ATIS	PTSC / WG SAC	§ Emergency Telecommunications in IP Networks § Packet Priority and Call Priority
		PRQC / WG SEC	§ Emergency Telecommunications Services
		ESIF	§ Interconnection of E9-1-1/Emergency Services § PSAP Network Interfaces and Protocol for NGN (TaskForce 34) § Wireless E9-1-1 Readiness Implementation Plan § Federal Telecommunications Service Propriety PSAPs
	TIA	TR-8	§ Broadband Public Safety Communications
		TR-30	§ Textphone Accessibility to Emergency Services in IP Environments
		TR-34	§ Emergency Capabilities for IP over Satellite (IPoS) Communications
		TR-41	§ IP Terminal and Enterprise Network Support for Emergency Calling Service § Enterprise Location Information Server Interfaces
		TR-45	§ Wireless Emergency Calling and Priority Services for cdma2000® § Location Identification/Determination Services § Broadband Data Capabilities for Enhanced Public Safety Services
IMS-3G Specifications	3GPP	WG SA1	§ Priority Services
	3GPP2	WG1	§ Services and Systems Requirements
NGN Service Control Interface / Service Enabler Specifications	Parlay Group		§ Emergency Telecom Services
North American Service Provider Specifications	NENA		§ Next Generation E9-1-1 Services
	Telcordia		§ E9-1-1 Service Requirements
	Network Reliability and Interoperability Council	various	§ Voluntary Best Practices on physical security, cyber security, network reliability, infrastructure protection, interoperability, public safety, emergency preparedness

Figure I-2 reflects the complexity of the NGN standards ecosystem.

Figure I-2. The NGN Standards Ecosystem

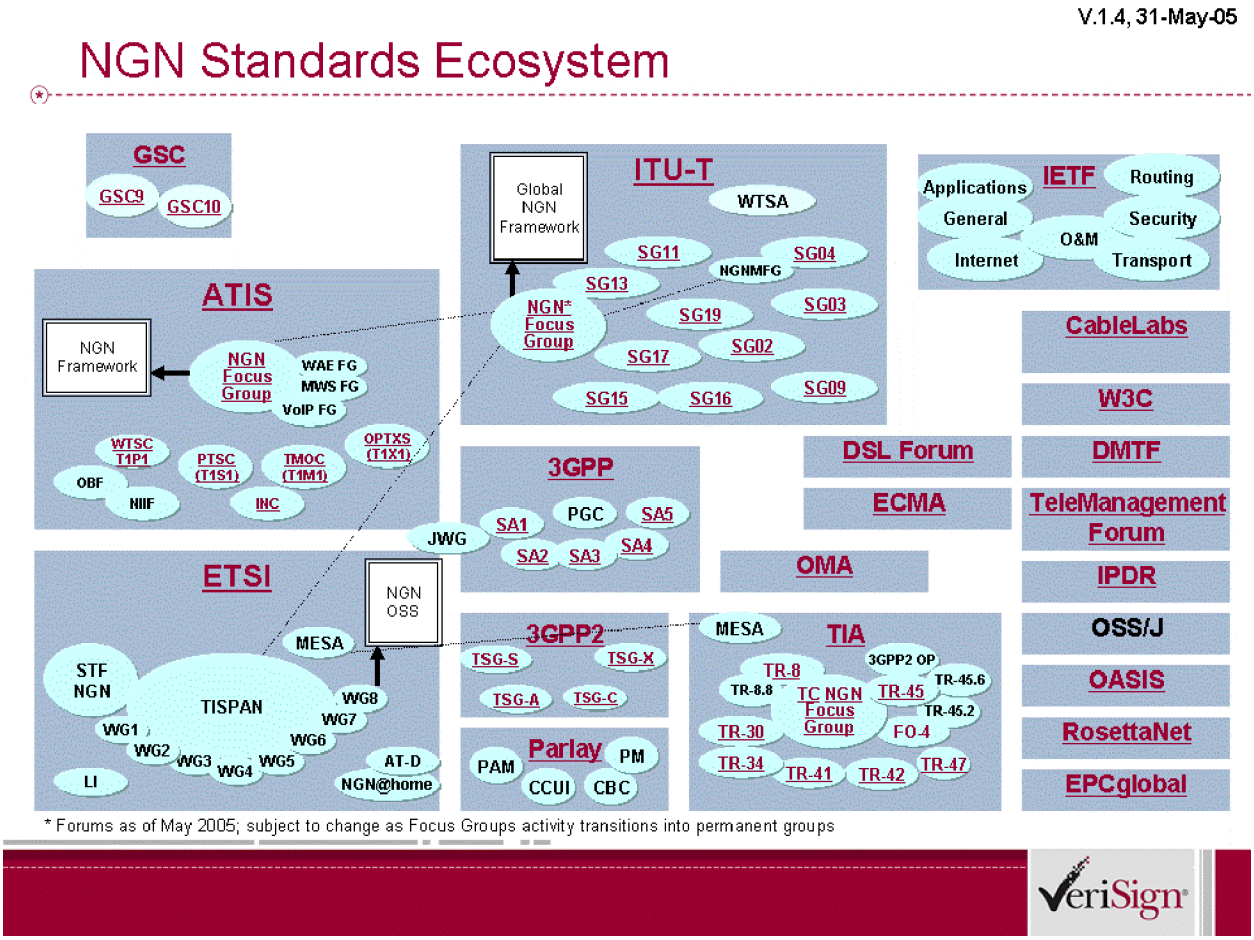


Diagram courtesy of Mr. Anthony M. Rutkowski, Verisign