THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NEXT GENERATION NETWORKS TASK FORCE

Report

March 28, 2006

TABLE OF CONTENTS

EXECUTIVE SUMMARY **1**

1.0 BACKGROUND AND CHARGE **1**

2.0 THE NGN **3**

2.1 Introduction 3
2.2 NGN Description 4
2.3 Security on the NGN 8

3.0 NS/EP COMMUNICATIONS AND THE NGN **8**

4.0 NS/EP FUNCTIONAL REQUIREMENTS IN AN NGN ENVIRONMENT **10**

4.1 "Legacy" Functional Requirements 10
4.2 Key "New" Functional Requirements 11

5.0 IDENTITY MANAGEMENT **13**

5.1 Introduction 14
5.2 Identity Management Criticality 15
5.3 Identity Management Mechanisms, Standards, and Taxonomy 15
5.4 Resiliency of Identity Management 16
5.5 Anonymity and Identification 16
5.6 Federation, Interoperability, and Credentials 16
5.7 Commercial Technologies and Deployment 17
5.8 Trust/Social Concerns 18

6.0 COORDINATION ON COMMON OPERATIONAL CRITERA FOR NGN NS/EP END-TO-END SERVICES **18**

6.1 Unique NGN End-to-End Service Issues 19
6.2 Common Operational Criteria 19
6.3 Local Access and Priority 21
6.4 Scope and Relative Levels of Priority 22
6.5 Internet Protocol version 6 22
6.6 Peer-to-Peer Technology 23
6.7 Meshed Network Environments and IP Security 23

7.0 RESEARCH AND DEVELOPMENT **24**

8.0 TECHNOLOGY LIFECYCLE ASSURANCE AND TRUSTED TECHNOLOGY **25**

9.0 RESILIENT ALTERNATE COMMUNICATIONS **26**

10.0 AGREEMENTS, STANDARDS, POLICY, AND REGULATIONS **29**

11.0 INCIDENT MANAGEMENT ON THE NGN **32**

11.1 Introduction 32
11.2 Unique NGN Incident Response Issues 33
11.3 Industry Involvement Throughout the Planning Process 34

11.4 Joint Coordination Center 34
11.5 Exchange Program 35
11.6 Federal Incident Management Training Academy 35
11.7 Exercise Program 35
11.8 Increased Research and Development Funding 36

12.0 INTERNATIONAL POLICY 36

13.0 FIRST RESPONDERS 37

14.0 CONCLUSION 38

EXECUTIVE SUMMARY

The convergence of wireless, wireline, and Internet Protocol (IP) networks into global Next Generation Networks (NGN) is changing how the Federal Government will meet its needs for national security and emergency preparedness (NS/EP) communications today and in the future. The NGN will offer significant improvements for NS/EP communications as bandwidth and software continue to improve, but the transition to the NGN presents challenges for ensuring the security and availability of NS/EP communications.

Although the complete network evolution is expected to take many years, the process is well underway. It has become clear that the scale, scope and character of the NGN will fundamentally change the way NS/EP communications are planned for, prioritized, and ultimately delivered. It is critical that this issue be addressed.

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 meet NS/EP requirements and address emerging threats on the NGN. 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.

The NGNTF worked extensively on these taskings, sponsoring two formal Subject Matter Experts (SME) Meetings and creating working groups to address each issue thoroughly with deep SME involvement. Ultimately, the NGNTF agreed upon nine recommendations, the implementation of which would support the ability of the NGN to meet NS/EP functional requirements while also providing greater capabilities to NS/EP users.

The NSTAC recommends that the President:

- **Identity Management.** Direct the Office of Management and Budget (OMB), the Department of Commerce (DOC), and Department of Homeland Security (DHS) to work with the private sector in partnership to build a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity "silos," allows federation between the Government and commercial domains, and supports use of Government-issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including for priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.

- **Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services.** Direct the Office of Science and Technology (OSTP), with support from the collective National Communication System agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor programs that would foster NS/EP capabilities within the NGN, including initiatives concerning:
  - A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user's NS/EP authorization and required class of service; and
  - NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into Internet Protocol (IP) version 6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IP Security for authentication and confidentiality.

- **Research and Development (R&D)**. In support of the prior recommendation, direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, the National Institute of Standards and Technology (NIST), and the Department of Defense (DOD) to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/ information technology and service providers.

- **Technology Lifecycle Assurance and Trusted Technology.** Direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of: (1) technology lifecycle assurance mechanisms and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.

- **Resilient Alternate Communications.** Direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure.

- **Agreements, Standards, Policy, and Regulations.** Direct DHS, the Department of State, and DOC (including NIST and the National Telecommunications and Information Administration) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally distributed NGN environment.

- **Incident Management on the NGN.** Direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

- **International Policy.** Direct departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-U.S. companies in NS/EP incident response in the United States; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.

- **First Responders.** Direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

1.0 BACKGROUND AND CHARGE

Dramatically changing business models of traditional telecommunications carriers, along with new technologies, are driving fundamental changes in global communications networks. For several years, global communications networks have been in transition. Customer demands and business imperatives catalyzed a "convergence" of traditional circuit-switched networks interoperating with broadband packet-based Internet Protocol (IP) networks. For almost a decade, this convergence has been increasing and evolving toward "Next Generation Networks" (NGN). This convergence of wireless, wireline, and IP networks into the global NGN will alter the way governments and critical infrastructures meet their needs for national security and emergency preparedness (NS/EP) communications. In many cases, it has already effected change. Although the complete evolution to the NGN is expected to take many years, the process is well under way. Many networks and providers have already developed the capability to carry voice, video, text, and data transparently to many types of end-user devices, a key characteristic of the NGN. Mobile phones able to access an array of Web-based services are only one example of this enhanced ability.

The scale, scope, and character of the NGN will fundamentally change the way NS/EP communications are planned for, prioritized, and ultimately delivered. NGN networks, which are largely, packet-switched networks, differ greatly from legacy circuit-switched networks. For example, packet-switched environments place control capabilities at the network "edge" and rely heavily on intelligent devices to execute key functions. In this new environment, confusion exists among end users concerning how their responsibilities will change. At the same time, NS/EP communications and critical business communications will be subject to an increased number of cyber threats based on inherent vulnerabilities and interdependencies known or expected to exist in the NGN. With these changes, one of the major issues facing network operators, infrastructure custodians, and NS/EP users is how best to meet NS/EP user requirements on the NGN.

The transition to the NGN presents challenges for ensuring the security and availability of NS/EP communications. Some vulnerabilities that existed in legacy networks present more of a challenge on the NGN. For example, the enhanced interconnectedness of the NGN can be used by threats to provide rapid and far-reaching propagation of malicious payload (attacks). Another vulnerability is the emulation of network control messages. Unlike legacy networks, which used separate paths to separate network control messages from normal network payload, NGN architectures have network control messages co-existing with normal payload traffic, providing more open access to threats to interfere with these messages. These and other vulnerabilities create complex risk scenarios for NS/EP communications in an NGN environment, which depends on its own components as well as other infrastructures, as Figure 1 illustrates. A further challenge is the global nature of the NGN and, thus, methods for managing incidents of national significance may require international cooperation. These concerns must be addressed.

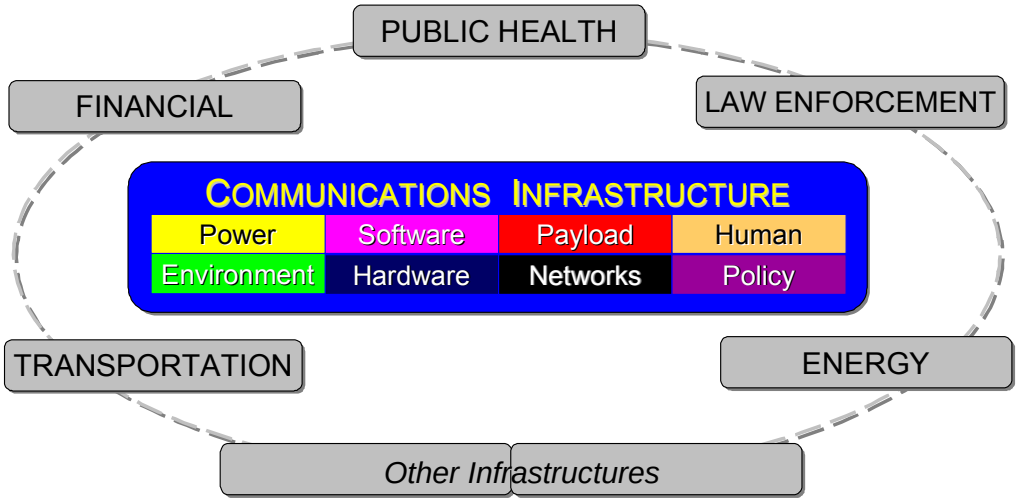

Figure 1. Communications Infrastructure Components and Dependencies[1]

On the other hand, the NGN will offer significant improvements for NS/EP communications as bandwidth and software continue to improve. New communications capabilities, including greater access to data and new services, will support NS/EP functions in critical ways, enabling first responders, for example, to obtain real-time access to voice, data, and video necessary for the most effective completion of their jobs. The NGN will also naturally increase network robustness and resiliency by the nature of its mesh architecture, offering many possible paths for service and redundancy of equipment and servers. In short, the NGN can provide new capabilities and greater resiliency; to achieve these benefits, and to speed and enhance the transition to NGN, solutions must be found that address NS/EP functional requirements, especially for security and availability. Doing so requires forward-looking action by industry and Government.

Principals of the President's National Security Telecommunications Advisory Committee (NSTAC) agreed at the NSTAC XXVII Meeting held on May 19, 2004, that a task force should be created to engage subject matter experts (SME) in an examination of NS/EP requirements and emerging threats on the NGN. Accordingly, the Next Generation Networks Task Force (NGNTF) was created to:

- 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;

    - 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

[1] *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.

- Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements.

It was also agreed that the task force should explore international issues, both in terms of NS/EP functions that must be provisioned internationally, and international threats to the NGN.

The NSTAC previously examined network convergence issues via its Convergence Task Force (CTF) and Network Security Vulnerability Assessments Task Force (NS/VATF). The CTF presidential report (June 2001) analyzed the potential security and reliability vulnerabilities of converged networks. The NS/VATF report (March 2002) addressed public network policy and technical issues related to network disruptions, the security and vulnerability of the converged network control space, and needed countermeasures. Issues presented by convergence and cyber security also arose during the Financial Services Task Force examination of network resiliency to physical disruptions.

2.0 THE NGN

2.1 Introduction

Until recently, communications networks each delivered a single type of service. Telephone networks delivered telephone service, cable television networks delivered television service, and so forth. Now public wireless networks, including both mobile telephone and wireless data networks, public fixed networks, including the public switched telecommunications network (PSTN) and other voice and data broadband networks, and private customer premises networks, including broadband user networks, are converging into the emerging global NGN, which provides a range of services.

As single-function networks disappear, open and dynamic networks are replacing them. These new networks offer greater functionality and processing capabilities and, through associated changes in the underlying transport networks and their architecture, will bring a radical change in the array and availability of services provided to end users. On the NGN, user-centric services will no longer be associated with the type of network access or transport, but rather with the user need that is satisfied regardless of user terminal, access type, transport mechanism, or data type.[2] An idealized NGN will enable end users to get the information content they want, in any media/format, over any facilities, anytime, anywhere, under any condition, and in any volume.[3]

[2] "Next generation networks will take communications beyond vertical silos of function and capability to one packet-based network delivering multiple services that are accessible by multiple types of devices." *ATIS Press Release*, Dec. 6, 2004. *See also*: "IP [the Internet Protocol] is the common thread of a whole host of new and emerging multimedia applications that blend video, voice and data capabilities." TIA Press Release, Feb. 9, 2005. (*http://www.tiaonline.org/media/press_releases/index.cfm?parelease=05-04*).

[3] Thus, the NGN may be said to be *service oriented*, as it is focused on delivery of services that are agnostic of the network or terminal type. The U.S. Department of Defense calls this concept *Net Centricity*: that "Anyone, anywhere can get to any data source and exploit the information they are authorized to access."

The NGN has the ability to significantly improve how the Government and critical infrastructures use and deliver NS/EP[4] communications. However, the promise of enhanced NGN-based services for NS/EP users cannot be realized without significant industry and Government action. As the NGN evolves, parts of the existing networks will continue to be replaced or upgraded to the corresponding NGN components. That said, existing "legacy" networks and gateways to the NGN will exist for the foreseeable future; therefore, NGN implementations will need to interoperate[5] with and allow for a migration path from existing networks and services.

2.2 NGN Description

The NGN will logically consist of applications that deliver services, the services provided to users, and the underlying transport networks. See Appendix C. The NGN itself is a capability that will enable many services and applications. Some services will be provided by the network and some will be external to it, but depend upon it. NGN user-centric services will be delivered over various networks, some of which, like private customer premises networks and mesh networks, lie outside the wide scope of the public network.

However, there is no single, universally accepted definition of the NGN. As used in this report, the term NGN is not intended to represent any single configuration or architecture. Instead, it represents the set of converged networks, illustrated by Figure 2, expected to arise that will transparently carry many types of data and communications and allow delivery of services and applications that are not coupled to the underlying network. However, it is possible to note several key NGN elements or attributes over which there is little, if any, dispute. These elements, discussed in the following subsections, relate both to architectural and technical differences—how the NGN will be built and work—and the capabilities it will provide as a result.

4 Office of Science and Technology Policy (OSTP) and National Security Council (NSC) policies define NS/EP telecommunication services as: "[T]hose telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States" (47 CFR 201.2[g]). Furthermore, the term telecommunications is defined by the OSTP and the NSC policies as: "[A]ny transmission, emission, or reception of signs, signals, writing, images, graphics, and sounds or intelligence of any nature by wire, radio, optical or other electronic means" (47 CFR 201.2[k]). The extent to which these and other Government NS/EP policies apply to new communications mechanisms remains under discussion.

5 "Interoperability" is the "ability of software and hardware on different machines to communicate with each other." *Computer User High Technology Dictionary,* http://www.computeruser.com/resources/dictionary/dictionary.html (hereinafter "*Computer User High Technology Dictionary*").

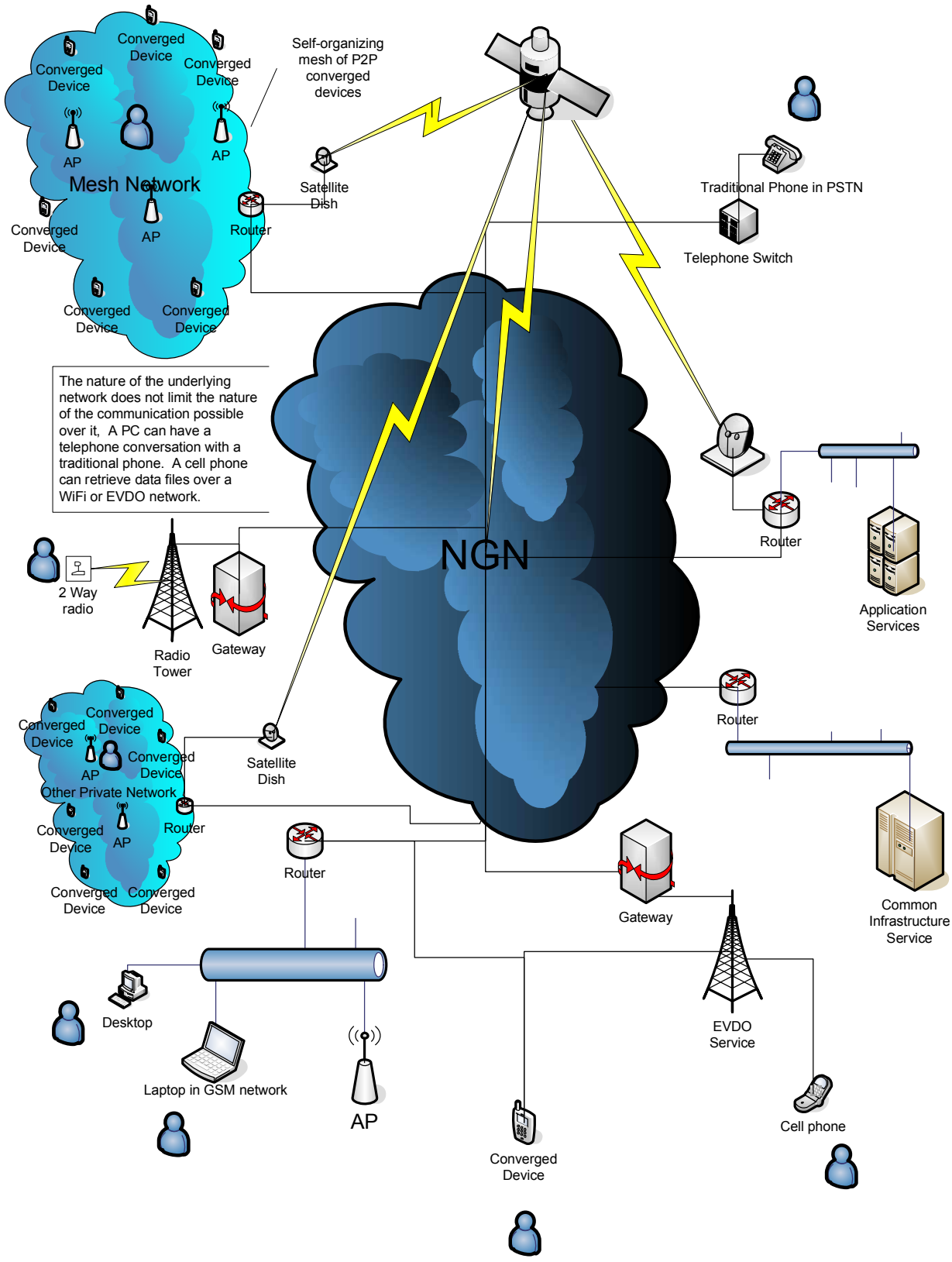

Figure 2. Network Convergence and the NGN

2.2.1 Architectural and Technical

2.2.1.1 Packet-Based

In packet-based (or "packet-switched")[6] networks, digital information (whether video, voice, data, or a combination of these) is divided into pieces, called packets, that travel across the transport network to their destination following a set of rules implemented by the network and its protocols. This differs from how the circuit-based (or circuit-switched) PSTN works.[7] In the circuit-based phone network, each communication receives a dedicated amount of network resources when a phone call is first set up, creating a "virtual circuit."

2.2.1.2 Open, Layered Architecture

The NGN is being designed with an open, layered architecture, which offers multiple services virtually independent of transport.[8] The NGN will also provide multiple transport options for a single service or communication.[9] This layered architecture provides open and standardized[10] interfaces between layers, providing layer independence. Layering, therefore, permits rapid changes or improvements to one layer of the network without having to reconstruct other layers,[11] enabling a more flexible and vibrant architecture for new services.

There are several models for conceptualizing the various layers of the NGN. Telecommunications providers view the NGN as having three fundamental layers: (1) application; (2) service control; and (3) transport. An alternative model is the classic, logical Internet categorization of four simple layers: (1) "physical" connection layer; (2) interconnection or "network" layer provided by IP; (3) end-to-end "transport" layer; and (4) "application" layer, or, combining the second and third layers into a three-layer construct of physical connection, packet transport, and application.

---

6 "Packet Switching: A technology for sending packets of information over a network. Data is broken up into packets for transmission. Each packet has a header containing its source and destination, a block of data content, and an error-checking code. All the data packets related to a message may not take the same route to get to their destination; they are reassembled once they have arrived." *Computer User High Technology Dictionary.*

7 "Circuit Switching. A communications method which establishes a dedicated channel for the duration of the transmission, allowing data to be transmitted in real time. The telephone network is a circuit-switched network." *Computer User High Technology Dictionary.*

8 For example, the U.S. Department of Defense next generation capability, the Global Information Grid (GIG), involves the concept of Network Centric Enterprise Services (NCES), which includes nine basic next generation services: information assurance (IA); user assistant; messaging; applications; ESM; mediation; discovery; storage; and collaboration.

9 Because services are virtually independent of transport, and there are multiple transport options for a given service, this architecture may be said to be "componentized."

10 An open standard is a document either developed or ratified by standards organization that operates by consensus or agreement and whose membership is generally open to those impacted by the standards.

11 "New applications can be invented and provided over the NGN via software installed at each endpoint without requiring modification to the [Next Generation Service Provider's] network or services." *ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture, Issue 1.0, November 2004*, at p. 19 ("ATIS Framework"), available on the net at: http://www.atis.org/topsc/Docs/ATIS-NGN-Framework-Part1-Issue1.pdf.

2.2.1.3 More Powerful and Varied User Devices – Distributing Network Intelligence

The NGN's open nature permits users to connect powerful, multifunctional devices to it using NGN-provided protocols. Personal computers, personal digital assistants, powerful mobile phones running their own applications, etc., are already replacing current PSTN communications devices, the caricature of which is the old, black rotary phone. These more powerful devices, which can have control capabilities and distribute network intelligence, make applications and other software running on them of more relative importance than software on the PSTN. For example, end-to-end encryption will likely be far more common on the NGN given the ability of end-user devices to provide such encryption at either the application or end-to-end transport (e.g., via IP Security [IPsec], *see* Section 6.7) layers. Some devices will be able to communicate without the use of network-provided services by using peer-to-peer communications. End users can also use peer-to-peer applications and devices to improve robustness and remove single-points-of-weakness, and to provide a backup or supplement for primary communications technology.

2.2.2 Capabilities

2.2.2.1 Multi-Modal and Converged Services (Voice, Video, Data) and Data Transparency

NGN services will allow users (human and machines) to communicate with each other using different modes of communication: voice, text, image, and video. Whereas traditional networks have been focused on uni-modal services, such as voice services, the NGN will provide a multi-service architecture intended to support multimodal communication environments on top of a generic IP transport. In these environments, information can be communicated through various terminal devices, network access technologies, and underlying infrastructures.

Moreover, data transparency in an NGN means that the data content is not permanently altered in the transport network itself.

2.2.2.2 Information Presented Real-Time, Time-Shifted, and Transformed

Information traveling across the NGN may be presented in real-time (interactive voice) or time shifted (voice mail); and in its original format (analog speech) or transformed (file attachment). The information can be delivered by the network to a location, a device, a person, or broadcast to many, and may reflect personal preferences and mobility options.[12]

2.2.2.3 Greater Mobility and Ubiquity

The NGN is expected to approach near ubiquitous access, providing access and services anytime and anywhere where a wireless, wireline, or satellite signal can reach. The NGN will also improve mobility: open NGN interfaces will enable users to stop work at one location and

12 *See* ATIS Framework at 8.

resume at another. The NGN should also be able to provide continual connectivity while in motion.

2.3 Security on the NGN

Security mechanisms on open packet networks will differ from those of legacy telecommunications services in access control, control traffic protections, and trust accorded to other network elements. Legacy networks were circuit-oriented vertical networks, and so, much policy management was implied or "built into" the integrated service, and managed across all aspects of the network. Nevertheless, although security will need to be addressed differently on the NGN, it is likely that migration and convergence will create the opportunity for enhanced security features that will replace fundamental pre-NGN security capabilities. For instance, with NGN technologies, network architecture affords the opportunity to "build on" and improve policy management and service capabilities to aid emergencies.

Notably, on an open network such as the NGN, capabilities and responsibilities for providing security may reside at any level/layer or with any participant, making security an end-to-end challenge. The use of the NGN for NS/EP depends upon transport networks being highly available, reliable and tamper-free, even under stress. Applications must maintain high integrity, protect ownership rights of information, and protect against malicious attack.

3.0 NS/EP COMMUNICATIONS AND THE NGN

The NGN can provide considerable benefits for NS/EP communications; however, to realize these benefits, and to speed and enhance the transition to NGN, we need solutions that address NS/EP functional requirements, especially for security and availability. This is an end-to-end problem; on a packet-based network such as the NGN, information will travel over a variety of networks and equipment, and a failure at any critical point, absent mitigation such as an alternative communications path, could impair communications. For the NGN to broadly meet essential NS/EP functional requirements in a consistent, continuous, and reliable end-to-end manner, a set of mechanisms must be promoted and adopted by those supplying network access, transport, and infrastructure services for this community, as well as NS/EP users.

In order to meet NS/EP requirements on the NGN, the NSTAC recommends that the President:

- **Identity Management.** Direct the Office of Management and Budget (OMB), the Department of Commerce (DOC), and Department of Homeland Security (DHS) to work with the private sector in partnership to build a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity "silos," allows federation between the Government and commercial domains, and supports use of Government-issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including for priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.

- **Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services.** Direct the Office of Science and Technology (OSTP), with support from the collective National Communication System (NCS) agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor programs that would foster NS/EP capabilities within the NGN, including initiatives concerning:
  - A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user's NS/EP authorization and required class of service; and
  - NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into IPv6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IPSec for authentication and confidentiality.

- **Research and Development (R&D)**. In support of the prior recommendation, direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, the National Institute of Standards and Technology (NIST), and the Department of Defense (DOD) to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/ information technology and service providers.

- **Technology Lifecycle Assurance and Trusted Technology.** Direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of: (1) technology lifecycle assurance mechanisms and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.

- **Resilient Alternate Communications.** Direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure.

- **Agreements, Standards, Policy, and Regulations.** Direct DHS, the Department of State, and the Department of Commerce (including NIST and the National Telecommunications and Information Administration [NTIA]) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally distributed NGN environment.

- **Incident Management on the NGN.** Direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

- **International Policy.** Direct departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-U.S. companies in NS/EP incident response in the United States; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.

- **First Responders.** Direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

These recommendations are detailed in sections 5 through 13, respectively. Implementation of these recommendations would support the NGN's ability to meet NS/EP functional requirements, described below, while also providing greater capabilities to NS/EP users.

4.0 NS/EP FUNCTIONAL REQUIREMENTS IN AN NGN ENVIRONMENT

4.1 "Legacy" Functional Requirements

The Federal Government has identified 14 functional requirements for NS/EP communications: enhanced priority treatment, secure networks, ubiquitous coverage, international connectivity, interoperable, scalable bandwidth, mobility, broadband service, reliability/availability,

restorability, survivability/endurability, non-traceability, affordability, and voice band service.[13] Overall, these "legacy" requirements remain generally applicable to the NGN. However, the functional requirements themselves are insufficient to describe and define the needs of the Federal Government in an NGN environment. Concepts such as "secure networks" do not go far enough in describing what technologies, services, and applications will be needed to support the NS/EP mission in an NGN environment.

4.2 Key "New" Functional Requirements

The task force developed the following "new" functional requirements by examining five NS/EP scenarios (continuity of Government, critical Government networks, industry and critical infrastructure, public safety, and general users) as described in Appendix D. Not all functional requirements apply equally to every scenario. However, several requirements were common to all scenarios. These elements will be critical for NS/EP communications in an NGN environment:

- **Survivability.** Survivable networks can be made from imperfect components; alternatively, use of highly redundant elements does not guarantee a survivable network. To satisfy survivability requirements, numerous techniques could be combined, including but not limited to, hardware and software certifications, secure development processes for software that reduce vulnerabilities, diverse routing of local access and backbone transport, integration of wireless and wireline services, equipment redundancy, backup power technologies and restoration priorities, dynamic network restoration protocols, dedicated out-of-band management networks, and host and network-based intrusion detection. Highly survivable networks may also depend on technology that is not yet available that quickly and automatically restores end-to-end NS/EP services on the NGN.

- **Broad Platform Support and Interoperability**. This requirement entails supporting the widest possible variety of hardware platforms with their concomitant ranges of access speeds, transmission power, processor speed, software, and cost. Such requirements would span battery and solar-powered sensors in the short term to supercomputers and "smart dust" sensors that run custom micro-kernels on ambient energy absorbed from their environments in the very long-term.

- **Broad Application Support**. Broad support for a variety of applications that can be layered upon and be independent of the underlying transport would include both real-time and non-real-time communications, with the latter including store-and-forward, publish-and-subscribe, and archive models. For this requirement, multiple forms of audio, video, and data must be able to be sent using dedicated applications, as well as using umbrella applications such as web browsers that incorporate complex functionality. Familiar mechanisms such as dial, push-to-talk, fax, video conferencing, instant messaging, e-mail, and evolving peer-to-peer capabilities must all be considered. And, in addition to such point-to-point services, multicast service may increase the efficiency of delivering some applications.

[13] National Security Telecommunications Advisory Committee, Convergence Task Force Report, 2001.

- **Strong Usable Authentication.** NS/EP services must be reserved for authorized personnel. Violations or compromise could result in increased economic loss, widespread panic, loss of public confidence, or even loss of life. Strong authentication of users, devices, processes, and communications is a prerequisite for authorizing access level by role or responsibility. This includes authorization by link, device, and user, and a recognition that this capability should be platform independent, whenever possible.

- **Priority and Preemption Over Non-NS/EP Users.** Authorized NS/EP users should be given priority access to required network resources, including transmission capacity, servers, and operations personnel during crises when impairments or transient loads constrain available resources from satisfying both NS/EP and non-NS/EP demands. Priority must extend to the application level, i.e., emergency e-mails should take priority over all other messages even if transmission capacities and servers are operating normally. End-to-end prioritization may be required beginning with the access link of the authorized, authenticated user, and such priority may need to be applied in those places where congestion can or may occur. Therefore, a wide variety of priority techniques will be needed along with methods to pass authorization among users, devices, communications, and network layers. Wireless end node link layers will have to fairly share or cede link capacity.

- **Mobility.** Mobility will require a combination of technologies used for strong authentication, along with wireless access methods including terrestrial, aerial, and satellite communication. The required solution also includes detailed radio technical requirements beyond the scope of this report, along with network layer techniques similar to ad hoc networking protocols.

- **Multilingual and Equal Access**. NS/EP communication among authorized users, as well as the general public, must accommodate users with a wide range of communication abilities. The NGN must facilitate support for multiple languages, and people with visual, auditory, cognitive, or other impairments.

In addition, while most scenarios demand or assume communications protection, it is expected this requirement will largely be met by end-to-end encryption provided by the communicating systems or applications. Of course, different NS/EP communities will require different levels of data confidentiality and integrity that must be met.

Other requirements are critical, but in some instances are at odds with the requirements of other scenarios. While these may also be critical, they are not common to all scenarios:

- **Relative Priority.** The scenarios highlighted varying requirements for priority within the NS/EP user community based on many factors, including situation-based, role-based, and application-based priority. Assigning data priority according to these factors is difficult. Should an acceptable, widely deployable solution be identified that can assign data priority, existing network elements and design methods are adept at guaranteeing performance up to design load and isolating the effect of one traffic class on another.

- **Network-Based Location Estimation Versus Untraceability.** Use of location-based technologies continues to increase, both by the general public and within the NS/EP community. As these capabilities gain popularity, there are nonetheless instances where NS/EP users may not want location information or other information to be identifiable to others. Untraceable applications will also need to be available in the NGN environment.

- **Fail Safe Versus Fail Secure.** Some communications require systems to "fail secure;" if confidentiality, integrity, or other security services cannot be guaranteed, then no communication is to occur. In contrast, other uses require "fail safe" operation, preferring unencrypted communication to none at all. Either option will need to be available in the NGN environment.

- **Communities of Interest.** Applications and technology must be provided that will enable NS/EP users or other groups that support NS/EP to come together in a dynamic, authenticated manner over a multitude of platforms.

- **Content-Aware Security Services Versus Transparency.** Today, both active and passive content-aware security services are available. Some entities would prefer, as part of a layered defense-in-depth strategy, to depend on content-aware security services, for example, to block attacks before they reach systems. However, many entities do not require content awareness within the network or prefer to explicitly deny such capabilities. For example, logging of traffic or even statistics may reveal sensitive information. Therefore, such services should be available to NS/EP users on a per-connection or per-user basis,[14] and user requests should not be overridden.

- **Emergency Alerts.** Emergency alert capabilities may leverage several existing technologies, including captive portals, broadcast and multicast capabilities, and peer-to-peer networking. The NGN must be able to absorb and manage a large amount of alert message traffic, and new traffic management capabilities may need to be examined or understood, along with safeguards to prevent abuse.

5.0 IDENTITY MANAGEMENT

Recommendation: The President should direct OMB, the Department of Commerce, and DHS to work with the private sector in partnership to develop a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity "silos," allows federation between the Government and commercial domains, and supports use of Government issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including for priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.

[14] Control mechanisms should not rely on inspection of data content to perform control functions (although they may use such inspection as an optimization), as data may be compressed, encrypted, or otherwise transformed either end-to-end or in-transit.

5.1 Introduction

Identity management is a key underpinning of security for NS/EP communications on the NGN. The NGN provides open access to a broad array of communications, data, and services, and interconnects an increasing number of users, processes, and devices. This open access to an increased number of communicators introduces an enhanced set of vulnerabilities as compared to traditional voice and private line networks, where identity is generally directly linked to the service. Moreover, given the breadth of the NGN, interoperability among identity management mechanisms is critical; federation is essential. Government must leverage new and existing technologies in implementing its identity management processes.

Strong authentication of users, devices, processes, and communications is a prerequisite for authorizing access level by role or responsibility.[15] This includes authorization by link, device, and user. Moreover, it is clear that this capability should be platform independent whenever possible. Identity management systems must be independent of the underlying hardware platforms. In particular, they must support the broadest possible range of access speeds, transmission power, processor speed, memory, and operating system. Identity management systems must also be independent of the underlying application in order to enable any and all applications to use authenticated identity for access control and authorization when necessary. The authentication protocols used by the identity management system should also be, to the extent possible, independent of the underlying transport.

The President's NSTAC has made recommendations in this area in earlier reports, notably with regard to the T1.276-2003 standard in the *Operations, Administration, Maintenance, and Provisioning (OAM&P) Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane Report*, issued on August 28, 2003. However, this section aims to elucidate specific identity management issues that relate to NS/EP communications in the NGN.

The Federal Government has also taken efforts to address the need for a common identification standard through the issuance of Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, the Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors,* and General Services Administration (GSA)'s *Federal Identity Management Handbook*.[16] FIPS 201 was developed to satisfy the requirements of HSPD-12 and provides procedures and specifications for improving the identification and authentication of Federal employees and contractors to allow for physical and logical access to Government resources. HSPD-12 and FIPS 201 focus on human authentication, personal identity verification (PIV) card management, and access control to physical and IT systems. Authorization decisions related to logical resources are not a part of the program and will remain at the enterprise level. The program's current phase focuses on interface interoperability and the adoption of common assurance, biometric, and cryptographic standards. No efforts have yet been taken to explore

[15] Identity management, while critical, does not replace the need for encrypting information during its transmission (e.g.., encryption of the payload of packets) on the NGN to avoid eavesdropping. *See* Section 4.2 above.

[16] The FIPS 201 standard can be accessed from the NIST web site at http://csrc.nist.gov/piv-project/index.html. The Federal Identity Management Handbook is available at http://www.cio.gov/ficc/documents/FederalIdentityManagementHandbook.pdf.

how FIPS 201 might include common credentialing standards that could be used to support prioritized, end-to-end NS/EP communications on the NGN. Although a common assurance taxonomy has been set forth, it has not been developed in partnership with the private sector to ensure federated interoperability between commercial and Government systems.

5.2 Identity Management Criticality

Identity management is a crucial underpinning of NS/EP communications over the NGN, which is likely to provide open access to a broad array of communications, data, and services, and interconnect an increasing number of users, processes, and devices. Without the ability to identify NS/EP users in the open NGN environment, NS/EP privileges cannot be properly assigned. Strong authentication for users, devices, processes, and communications is a prerequisite for authorizing access level by role or responsibility. If NS/EP services are not reserved for authorized personnel, Federal and private sector responses to natural disasters, terrorist attacks, or national security threats could be impeded. For example, without an effective identity management regime, NS/EP priority in a time of contention for access cannot be reliably and consistently granted. Furthermore, identity management is critical for NS/EP services such as information sharing among communities of interest. Accordingly, any identity management failures on the NGN could imperil access, connectivity, and delivery of critical NS/EP services.

5.3 Identity Management Mechanisms, Standards, and Taxonomy

Coordinated Federal agency efforts and public-private partnerships could dramatically improve identity management on the NGN. Federal department and agency support for the prompt development and use of identity management mechanisms, including strong authentication, could accelerate the implementation of more secure systems than currently exist on the PSTN. Coordinated agency efforts would greatly enhance secure access for both current Federal NS/EP users and those Federal officials who may become ad-hoc NS/EP users in a crisis.

No cohesive effort to ensure that NS/EP requirements are addressed in identity management protocols and standards now exists. Given the need for interoperability between and within Government and commercial domains, a public-private partnership is essential to provide an appropriate forum for identifying requirements and leveraging existing and emerging protocols and standards. As executive agent for the NCS, DHS will be a critical participant in this effort. It will be important for the Manager of the NCS to engage with the appropriate senior officials and chief information officers in other agencies.

A public-private partnership could play an important role in developing and implementing a common assurance taxonomy that would be accepted within both Government and commercial domains. A broadly accepted taxonomy of identity assurance levels of operational requirements and levels of intensity is expected to contribute to pervasive interoperability of identity management mechanisms. Such taxonomies exist; for example, *NIST Special Publication 800-63 Electronic Authentication Guideline* defines a four-level assurance taxonomy for U.S. Government credentials. More recently, NIST issued FIPS 201, which Federal agencies are required to follow. FIPS 201 includes graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The

graduated levels of a security access could potentially accommodate NS/EP users. However, neither the guidelines (Special Publication [SP] 800-63) nor the Federal standards (FIPS 201) reference any special NS/EP-related authentication requirements. Federal standards must recognize NS/EP requirements and define scalable assurance levels to address unique NS/EP assurance needs. Bodies chartered with the responsibility for ensuring the adequacy of authentication mechanisms on the NGN for NS/EP use need to communicate requirements to standards-making organizations. Finally, a common assurance taxonomy could also further the harmonization of protocols and standards.[17]

5.4 Resiliency of Identity Management

While networks can be built from imperfect components and still meet survivability requirements, identification mechanisms must be at least as survivable, standing alone or in combination with alternatives, as the NS/EP services that rely on them.

When Federal and critical infrastructures officials respond to NS/EP-related incidents, they need to rapidly establish their identity on any available network. A resilient identity management capability is critical for authenticating the NS/EP user so they can share important information and manage the crisis at hand.

5.5 Anonymity and Identification

Some NS/EP applications and services will be available only to identified objects or persons, who may or may not be regular NS/EP communicators. However, certain uses of the NGN, even for NS/EP communications, will likely remain anonymous, such as the reporting of public health information.

Given the increasing number of communicating users, processes, and devices, a user's identity on the NGN will be required more often, in a broader number and type of settings, and more frequently than today. Depending on the nature of the situation, ordinary users may need to receive NS/EP alerts, contact emergency services, or access other NS/EP services. In this context, identification for NS/EP purposes is not limited to the needs or activities of Government or other large organizations. The special vetting requirements for access to NS/EP services may compel the surrender of personal information by individuals, in order to obtain the necessary credentials for such access. That said, some NGN communications may or must be available to unidentified recipients (receiving alerts) or senders (emergency "911" communications, possibly), and "best efforts" transport services may well remain anonymous.

5.6 Federation, Interoperability, and Credentials

Government should ensure that its identity management mechanisms can be federated with the commercial sector, with international networks, and across the Federal Government; there should be no isolated "identity management silos" without strong justification. While Government may

[17] In addition, the E-Authentication E-Gov initiative has developed the components of a federated identity management architecture across the Federal Government, intended to allow citizens, businesses, and State and local government to use a credential of their choice to access e-Government services.

choose to build "identity management silos," adopting its own authentication requirements, the end result is usually unsatisfactory. The resulting isolated systems often atrophy, and even Government employees and contractors begin to route around them. For example, agencies that failed to provide e-mail to employees sometimes found that employees would use personal e-mail accounts to communicate.

Even when NS/EP needs are at their greatest, such as for national security communications, silos tend to be reconnected because of operational needs to communicate. This can lead to higher costs and lower assurance. Government can and should mitigate against the risks of unplanned interconnection by planning for interoperability as systems are initially deployed.

Issuing Government (State or Federal) credentials that are capable of operating in a federated identity management environment could greatly improve identity management, especially in response to an incident. For example, priority could be afforded to appropriate persons or devices in an emergency on an ad-hoc basis (e.g., persons living near a weapon of mass destruction event). Federated identify management helps to resolve two challenges: (1) it is almost impossible to determine in advance who may need to send or receive NS/EP communications; and (2) one individual or entity may have multiple identities and need differing levels of access because of the roles they may perform in a given incident.[18]

Moreover, interoperability maximizes utility. Accordingly, interoperability or federation between sponsoring commercial and Government domains, voluntarily accepted by them, is essential to ensure the ability of users with credentials from diverse sources to communicate in times of crisis (e.g., a local first responder with an employee of the Department of Defense).

Government can greatly simplify implementation of an identity management system by relying upon and deploying existing and emerging interoperable protocols and standards for exchanging and storing security credentials, including mechanisms for revoking previously issued credentials. Consistent and coordinated Government implementation would also encourage the development and implementation of existing and emerging standards for hardware interfaces and communication protocols for portable hardware cryptographic devices (e.g., smart cards, PDAs, cell phones) to enable flexible access to NGN services.

In sum, technical mechanisms (e.g., protocols) and policy mechanisms (e.g., a common taxonomy of assurance levels) support interoperability between and within commercial and Government domains, and should be accompanied by an enforcement capability, which could be distributed.

5.7 Commercial Technologies and Deployment

The Government could realize multiple benefits by encouraging the Federal use of more secure commercial existing and emerging identity management mechanisms for NS/EP. For example,

[18] The identity management strategy should recognize that an individual might have separate identities (persona) that cannot be associated with each other except by the individual. This would happen where an individual participates in non-interoperable identity-management systems, and could occur within a single identity-management system if the individual needs unrelated identities. These multiple identities are different from the multiple roles that an individual might have associated with a single identity.

Government use of commercial identity management technologies will create incentives for the further commercial development of such mechanisms and infrastructure to support them, leading to overall security improvement on the NGN. Commercial mechanisms are typically available at lower cost, provide greater capabilities, and are updated rapidly as technology improves. Deployment and use of mechanisms being deployed commercially will also support interoperability between commercial and Government domains (and support deployability of solutions). Therefore, preferences for Commercial-Off-the-Shelf (COTS) solutions should explicitly extend to identity management services and technologies.

To be effective for NS/EP communications, identity management solutions must be deployable —practicable, acceptable to the community using them, and scalable. Users will "route around" solutions of limited utility or that otherwise do not meet their needs, using alternative channels of communications, and NS/EP users will default to insecure methods of communication. Accordingly, Government efforts regarding identity management should, to the greatest extent possible, permit the market to determine and build the best mechanisms for meeting Government-specified NS/EP identification needs.

5.8 Trust/Social Concerns

Users should be required to reveal as little personal information as necessary to gain authorization, such information should be sufficiently protected, and entities must be accountable for the security of the information they collect. Technologically elegant solutions that are perceived to violate personal privacy will be criticized.

Care must be taken with issues of privacy and usability. To entice the voluntary, cooperative participation of individuals and organizations outside the sphere of Government activities, the "value proposition" must convincingly deliver a net benefit in the eyes of a potentially very large and diverse user population. The user experience must be simple, quick, satisfying, and highly resistant to abuse or error, because much of that population may have limited experience in the fundamental mechanisms underlying the identity management regime.

6.0 COORDINATION ON COMMON OPERATIONAL CRITERA FOR NGN NS/EP END-TO-END SERVICES

Recommendation: The President should direct OSTP, with support from the collective NCS agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor initiatives that would foster NS/EP capabilities within the NGN, including initiatives concerning:

- A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user's NS/EP authorization and required class of service; and

- NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into IPv6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IPSec for authentication and confidentiality.

6.1 Unique NGN End-to-End Service Issues

Top-level elements and critical functional aspects for NGN end-to-end service include access, transport, and the availability of infrastructure and application-level services. If access, transport, and service availability can be assured for NS/EP functions, it is then possible to maintain the required state of readiness to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. However, the fundamental requirements of access, transport, and availability of services must be provided in a manner that assures that NS/EP communities receive the appropriate priority among potentially competing users.

Fulfilling any of the requirements above entails an ability to have packets within the NGN delivered with required performance, reliability, and priority end-to-end. To meet these needs, ensuring quality of service during normal periods of operation and during periods of network stress will be essential. Periods of network stress can result for any number of reasons, including physical, logical, malicious, unintentional, accidental, or other events that degrade the performance of a network or network service upon which a critical function relies.

End-to-end 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 inter-connected 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.

6.2 Common Operational Criteria

For the foreseeable future, the NGN will be based on a set of interconnected individual networks. See Section 6.7. End-to-end service will be achieved through coordination of these multiple

connected networks, linked both physically and logically via common operational criteria accepted and enforced among adjacent networks. Depending on the scope and severity of an NS/EP event, local network policy may need to be supplanted by a common operational criteria agreement. Policies for handling contention for resources and other critical issues on an individual network or across multiple networks in an NS/EP event require definition and enforcement of common operational criteria.

The common operational criteria should be defined for user authentication, network resource authorization, and precedence, permitting definition of multiple classes of service across constituent networks of an NGN, and ultimately should be a requirement for any network provider involved in NS/EP communications. 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.[19] Common operational criteria also would facilitate the transition from Internet Protocol version 4 (IPv4) to version 6 (IPv6), and would allow for more seamless peer-to-peer and meshed network communications.

The evolution of technology and communication services is triggering substantial changes in the makeup of the communications sector. The number of companies playing a significant role in providing the Nation's communication services is expanding dramatically, with an associated increase in complexity due to technology, services, and points of responsibility. Government coordination with the communications industry will need to be modified to account for these changes. Today, existing NS/EP programs such as the NCC and the priority services programs it oversees are built to support the small community of carriers that have traditionally supported the NS/EP role. The NCC's processes and approaches for coordination as they stand today will not support the increased number of NS/EP providers. Existing priority services programs rely on direct relationships with the individual wireline and wireless carriers providing the service. As complexity increases, new collaboration approaches must be developed for ensuring reliable NS/EP communications. To address the larger number of participants, technology, services, and points of responsibility, the common operational criteria should be developed using an inclusive joint industry-Government planning process. Because of the complexity and broad range of NGN operators and other stakeholders, it will be necessary to hold regular summits to foster the development of NGN criteria for NS/EP requirements. Annual or even more frequent reporting from this development framework would enhance coordination among Government and industry and tracking of progress by them.

The criteria should be agreed upon by participating networks in an NGN context, to provide a framework for supporting NS/EP activities that extend beyond a local network level. Network providers should demonstrate that they have the capability to support the criteria prior to an NS/EP event, including assignment of user priority and enforcement of NGN policy end-to-end.

[19] Common operational criteria define classes of service available or supported based upon accepted definitions of these three criteria for an individual network, or multiple networks in the NGN.

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 materially affect 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 supported by all network participants within the NGN.

6.3 Local Access and Priority

In an NGN context, local access is defined as: (1) physical access and connectivity to communications, and (2) a local end point connection and the destination end point connection. Local access is critical to end-to-end service, connecting people and devices with network resources, and many issues with connectivity tend to occur at the access point.

Authentication should be required for a valid NS/EP user to gain access to limited NGN NS/EP resources, including approval of NS/EP priority requests at the local access and transport partitions. A network user can be an individual, a communications device, or another network, as all three may request network access and resources from one or more sub-networks within the NGN.

During an NS/EP event, many different types and levels of priority users may need to access the network. Priority management must be 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. Additionally, common operational criteria across the NGN could include a standard mechanism to ensure uniformity of priority definition and support end-to-end.

Establishing local access priority will require:

- 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.

6.4 Scope and Relative Levels of Priority

As noted above, when extremes in load are present, NS/EP communications need appropriate prioritization. In this regard, priority must be provided on per-packet basis to "payload" or "content" as well as control traffic and other information used to set up a communication or gain access to an NS/EP service. Merely prioritizing packets that allow access to an NS/EP service could be insufficient in several circumstances, such as if the network loses some capacity, causing packets to be discarded even if appropriate bandwidth had been reserved or assigned. Accordingly, prioritization methods should protect the quality of an entire session and prevent packets from being discarded on the NGN.

The NGN should provide prioritization of command and control activities above all communications traffic including priority communication traffic so that the network control centers can appropriately manage and reconfigure the systems to respond to traffic conditions (especially in times of congestion). Patch prioritization is an example of a command and control capability. When software flaws impair network conditions, distributing to and installing critical software patches on various NGN network components must be possible in order to take corrective action.

Finally, prioritization should extend to wireless communications on the NGN. In the circuit-switched network, Wireless Priority Service (WPS) is supported via a system whereby callers dialing a WPS feature code followed by a telephone number receive priority treatment (assuming they are subscribers to WPS) via radio queuing. In the NGN, a similar service should be supported. However, a vulnerability exists such that a flood of calls placed by a malicious attacker at the time of an emergency (some of which would likely be completed), or even repeated attempts from non-malicious users given the availability of automated access attempts, could clog the network and make it difficult for emergency responders to complete communications even with the use of WPS.

6.5 Internet Protocol version 6

IPv6 provides fundamental benefits over IPv4, including a vastly increased number of available IP addresses, more efficient routing infrastructure, better security implementation, and increased mobility while maintaining existing connections. One key benefit to NS/EP users may be the protocol's auto-configuration and neighbor discovery capabilities. These features 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.

The flexibility of IPv6 provides NS/EP users opportunities to logically control and manage their network communications over a shared or public infrastructure. This flexibility, combined with

the ability to authenticate and encrypt end-to-end communications with IP security, provides new opportunities for providing temporary NS/EP services that can support incident management.

The transition to IPv6 is already under way in many networks. Such networks are, and can continue to be, inter-linked with legacy IPv4 networks using either protocol translation or tunneling mechanisms to route IPv6 data traffic within IPv4 packets. Network equipment interoperability and open standards-based compatibility are crucial in mixed IP protocol operational environments.

Seamless network-to-network trust relationships are essential among constituent networks comprising the NGN to ease access to network resources after initial user authentication and network authorization procedures have been successfully performed. Therefore, networks must accommodate a mixed protocol operational environment, supporting current and anticipated user requirements with either IPv4 or IPv6 network connectivity.

6.6 Peer-to-Peer Technology

Peer-to-peer (P2P) technology offers independence from centralized infrastructure, and is especially useful in times of crisis.

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 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.

6.7 Meshed Network Environments and IP Security

In a typical NS/EP scenario, individual networks are integrated into a full or partial mesh of wireline, wireless, satellite, and private networks, including the Internet. 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 is required of myriad homogeneous (and often single-purpose) networks optimized for a dedicated user community.

Methods vary greatly 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. In the NGN, interconnectivity is based on deployment of an overlay, peer, or hybrid architecture to support services end-to-end across multiple networks.

Meshed networks have the following advantages: (1) no single point of failure, which enhances resiliency; (2) a percentage of the network remains intact and usable even though large segments of the overall meshed architecture is rendered unusable; and (3) the incremental and distributed nature of a meshed network is more readily configured and builds incrementally in locations without preexisting infrastructure. Tradeoffs must be considered in implementation, however, such as possible instability in tightly meshed operational environments.

Using IPsec, a standard for providing security at the network layer by encrypting and/or authenticating all IP packets, to preserve confidentiality and authentication of communication increases in importance in a meshed network environment, where the possible paths between two or more entities are more numerous. In such situations, it is difficult to establish and ensure a level of trust among connected devices. IPsec provides capabilities for user authentication, device authentication, integrity and authenticity of communications, and confidentiality of communication, which can be used independently or in combination.

7.0 RESEARCH AND DEVELOPMENT

Recommendation: In support of the prior recommendation, the President should direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, NIST, and DOD to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria, and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/information technology and service providers.

Industry often pursues R&D in areas where it anticipates a clear financial return. Industry funding for basic research and for meeting non-market requirements, possibly including NS/EP communications, is less certain. Government-sponsored research is recommended to provide a forcing function for developing necessary end-to-end NS/EP capabilities. These efforts should focus on areas in which investments would not otherwise be made, that is, those that may not have a clear financial motivation but would further the cause of NS/EP communications. Funding of demonstrations, especially end-to-end focused efforts, will assist NS/EP communities in capitalizing on new technologies. Results must be shared with and be commercializable by industry.

Another area warranting research attention is the NGN architecture. In the current architecture, messages that control network elements are co-mingled with general payload. This presents the concern that network control messages could be accidentally or intentionally embedded within general payload traffic. The technical community is examining ways to increase security of network control messages within various industry standards organizations. An investigation of

methodologies that can protect the control plane and ensure that capabilities are not accessed inappropriately would be appropriate.

8.0 TECHNOLOGY LIFECYCLE ASSURANCE AND TRUSTED TECHNOLOGY

Recommendation: The President should direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of (1) technology lifecycle assurance mechanisms; and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.

Hardware and software flaws represent potential vulnerabilities that will likely be exploited to the detriment of NS/EP capabilities. Hardware (including programmed and programmable semiconductor "chips") and software are pervasive in our society and will continue to be so in the NGN; flaws or even the deliberate introduction of vulnerabilities in this hardware and software, can occur across the entire technology lifecycle (design, development, and deployment). In addition, the current trend by vendors and service providers to leverage the advantages of outsourced and offshore mechanisms may present increased risk because there are few broadly-used standards, mechanisms, controls, or capabilities for lifecycle assurance. Further, during the deployment and sustaining phases of the technology lifecycle, there is a potential for incorrect installation, configuration, and maintenance errors to occur resulting in vulnerabilities exploitable by threat actors of varying capabilities and motivations.

Notably, as compared to the PSTN, the NGN depends to a much greater degree on widely distributed and powerful hardware and software components, raising the importance of the trustworthiness and security assurance of these components in order to protect security end-to-end on the NGN as part of a comprehensive risk management strategy. These components will also be produced by an increasing number of entities, and NGN services will be delivered by an increasing number of providers (see Section 6.2); these producers and providers will have varying levels of competency and discipline.

As part of a comprehensive risk management strategy, the Government should address these risks by encouraging, by policy and incentive, research regarding, and implementation of, supply-chain processes and safeguards that provide trustworthy assurances for technology regardless of where or by whom technology is designed, developed, manufactured, or deployed. Use of technology lifecycle assurance mechanisms proven to increase the security of technology across the lifecycle (design, development, deployment, etc.) can thereby increase the security assurance of information and telecommunications systems used for NS/EP. These mechanisms may include advanced engineering disciplines, standards and certification regimes, and best comprehensive practices. For example, software development lifecycle mechanisms that incorporate secure development techniques, such as threat modeling, code reviews, and use of appropriate tools, can identify vulnerabilities, regardless of how they are introduced. The Government should encourage by policy and incentive techniques and processes that can be demonstrated to improve security and reduce vulnerabilities, and should support certification regimes that test implementation of such techniques. Infrastructure providers and NS/EP users, including Government agencies and enterprises, will bear more responsibility on the NGN

because of the powerful hardware and software they possess that will affect the security of NS/EP communications. Effective certification regimes[20] will enable these users to make appropriate choices in order to protect NS/EP communications.

Moreover, further research and investment in technology lifecycle assurance mechanisms is needed in the public and private sectors as well as academia. Cooperation is needed among these entities in developing deployment and configuration standards, best practices, and guidance that will better manage and mitigate risks inherent in using the NGN for NS/EP.

Going forward, fundamental changes in technology can enhance the reliability of the NGN for NS/EP communications. The current state of technologies and architectures used in the Internet and NGN environment are wrought with long-known, recognized potential vulnerabilities.[21] Many recent efforts have been focused on the mitigation and patching of these vulnerabilities and weaknesses. However, fundamental changes in technology, including new architectures not subject to the known vulnerabilities, offer the prospect of comprehensive change in system security. Investments must therefore be made in trusted technology research. Moreover, the "R&D cycle" itself should be conducted under a threat modeling and vulnerability analysis framework. If this were to be done, new technologies would have threats and vulnerabilities already mitigated, and be more trustworthy.

One example of this work is the trusted hardware root technologies. [22] Software-only security solutions that attempt to protect sensitive data have systemic vulnerabilities.[23] Hardware-based solutions to security problems have advantages that complement software-based solutions, thus counteracting remaining vulnerabilities and providing defense in depth. This layered defense could allow such systems to be inherently more trustworthy by providing features such as secure boot as well as process and data signing and attestation.

9.0 RESILIENT ALTERNATE COMMUNICATIONS

Recommendation: The President should direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can

20 One relevant regime is the "Common Criteria for Information Technology Security Evaluation" (CCITSE), referred to as the "Common Criteria" and adopted as an international standard: ISO/IEC 15408. The Common Criteria, at commercially-used evaluation levels, focuses on the correctness of security features as opposed to vulnerabilities in the non-security features of software.

21 For example, there are inherent weaknesses of Von Neumann architectures versus Harvard architectures in processor technology. Attacks against software have been known for some time, and attacks against hardware are now being published. *See SemiInvasive Attacks—A New Approach to Hardware Security Analysis*; Sergei P. Skorobogatov, University of Cambridge, April 2005.

22 The Trusted Platform Module (TPM) (specification and other information can be found at https://www.trustedcomputinggroup.org/groups/tpm) is one example of a hardware/firmware-based solution that helps security system hardware and software designers and builders work cooperatively to address these issues.

23 *See* Appendix G, Systematic Assessment of NGN Vulnerabilities. The vulnerabilities may also be addressed substantially by special purpose systems that are not widely deployed, perhaps due to the cost or reduced functionality of such systems.

augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure.

Convergence of most communications to an IP-based backbone (the NGN) will result in more communications resilience. Most disruptions in the NGN will be relatively easy to repair or work around.[24] Regional service may be disrupted, but will be brought back online promptly in most cases. Unfortunately, NS/EP professionals and the public they serve cannot settle for communications that are up and running "in most cases." As NS/EP depends more on NGN communications, damage or destruction to communications infrastructure can seriously impair NS/EP mission-critical response and recovery efforts; including those of Federal and localized first responders, non-governmental organizations (NGO), general public initiatives, and private-sector response and restoration. Because the point of access to the NGN is the point most likely to suffer congestion (with the most limited bandwidth, typically) or a single-point-of-failure, it is the point of greatest concern.

NS/EP responders already depend on alternate communications methods. They use cellular phones to provide communications redundancy, for example, where a cell-tower infrastructure is operating. Other examples include the use of a separate two-way radio system to provide primary system redundancy, and the provision of satellite capabilities. In the later case, satellite capabilities not only provide another preferred alternate access means, they also offer a non-terrestrial infrastructure base unaffected by most terrestrial disasters. Hand-carried devices can be designed to connect to an antenna or satellite system affixed to the exterior of a vehicle (or similar unit) or to other network "aware" devices that could extend service areas through interconnection and resulting geographic dispersion. And, the Federal Communications Commission (FCC) supports use of amateur radio organizations to provide alternate communications services. In short, the best resiliency is achieved by diverse communication methods.

Use of alternate communications for resiliency will become easier on the NGN given the capabilities of end-user devices. In the emerging NGN, many NS/EP-utilized communication devices will contain multiple access capabilities within the same form factor. Examples could include devices that access multiple commercial networks, satellite, and/or other private systems, depending on availability, device functionality, and user authority. In this regard, private industry is developing devices with the innate ability to access multiple types of access networks (i.e., "on-ramps") and infrastructure types (i.e., dynamic access/homing), which will be significant with regard to NGN NS/EP user capabilities, and strategic with regard to continuity of operations (COOP) planning. These devices should be adopted by NS/EP users.

Other techniques important for communications resiliency include having a resilient (robust) or alternate power supply, including devices and infrastructure components operated on available fixed electrical power systems, fuel-based fixed and portable electric generation, battery-based

[24] As noted above, the NGN will increase network robustness and resiliency through the nature of its mesh architecture, offering many possible routes for traffic and redundancy of equipment and servers. This addresses the familiar single-point-of-failure challenge for reliability. However, the NGN could experience broad disruptions as a result of single modes of failure, such as those associated with a logical protocol error or widespread logical software coding error. *See* Appendix G, Systematic Assessment of NGN Vulnerabilities. Other recommendations of the Task Force, such as providing priority to command and control communications, are intended to address the single mode of failure concern. This "Resilient Alternate Communications" recommendation specifically addresses the concern of a single point of failure at the access point.

power, and other emerging energy sources such as solar power, depending on needs.[25] The combination of multiple WPS providers within an incident area can add overall capacity to an affected area and provide for alternate access methods. Priority can help provide resiliency of communications, and the coalescence/convergence of WPS and Government Emergency Telecommunications System (GETS) into a coordinated end-to-end NS/EP priority treatment service (see sections 6.3 and 6.4) will add resilient, reliable, and consistent capabilities for NS/EP communications users. NGN services such as ENUM (IP address/landline number and device mapping) and alternate contact routing, will enhance communications infrastructure reliability and enhanced capabilities. Finally, over-provisioning[26] of capacity by infrastructure providers can add resilience should network congestion or loss of network links occur.

Applying *best practices* will further enhance the NGN for NS/EP services.[27] Diversity in routing critical links should be pursued, and steps taken to ensure true route diversity and not simply diversity of suppliers where the physical paths travel in the same cable sheaths or systems. Alternate communications access should also be provided at "sheltering" points. It is of paramount importance that Federal Emergency Management Agency (FEMA), National Guard, and local authorities have accessible alternate communications and resources for those who require them. For example, National Oceanic and Atmospheric Administration (NOAA) and portable AM/FM capabilities are used for alternate communications, the overall NS/EP communication mission between NS/EP users, and as outreach to the general population.

Ensuring constant communications reliability during every high-level crisis is an infeasible goal. Accordingly, NS/EP users must consider the full spectrum of possible disruptions in their contingency planning and develop solutions based on their own unique requirements. Fortunately, the likely convergence of most communications into a robust IP backbone will create far more resilience than exists, and most disruptions will be relatively easy to repair or work around. (It is important that avoiding single-points-of-failure be a design consideration for the NGN.) Conversely, a greater dependence on communications over the NGN also has the potential to create a single point of failure from a local access perspective. With applications and services converging into a common infrastructure, those who could not gain access to the NGN in a crisis situation would have few viable alternatives.

Therefore, incident managers should implement alternate communications that will provide multiple access options for reaching the NGN backbone or for local and regional communications. Examples include satellite phones, line-of-sight optical systems, digital broadcast satellite (DBS), devices with multi-access capabilities, mesh networks, metropolitan wide-area networks, such as IEEE 802.11(b) Wi-Fi (Wireless Fidelity) and IEEE 802.16Wi-MAX (Worldwide Interoperability for Microwave Access) networks, and many others. Currently, the NCC and other agencies use the SHAred RESources (SHARES) High Frequency

---

[25] Another NSTAC Task Force, the Telecommunications and Electric Power Interdependency Task Force is examining interdependencies between these two sectors.

[26] "Over-provisioning involves providing communications links the bandwidth of which "exceeds the expected traffic load by a certain margin, which is selected to ensure that the link can absorb both expected and unexpected traffic fluctuations." *See* Y. Huang and R. Guerin, "Does Over-Provisioning Become More or Less Efficient as Networks Grow Larger?[,]" http://csr.bu.edu/icnp2005/Papers/20_yhuang-Overprovision.pdf.

[27] *See e.g.*, Network Reliability and Interoperability Council best practices found at www.nric.org. Additional information on these best practices can be found at http://www.bell-labs.com/user/krauscher/nric/.

(HF) Emergency Radio program, which provides a single interagency emergency message handling system for the transmission of NS/EP information. The SHARES program brings together existing HF radio resources of Federal, State, and industry organizations when normal communications are destroyed, disrupted, or unavailable due to natural or manmade disasters.

OMB and DHS have significant oversight and planning requirements for ensuring resilient communications. Under the Federal Information Security Management Act of 2002 (FISMA), OMB must annually approve agency IT security programs. As part of this process, OMB could base approval of such programs on a focused plan for resilience. Further, OMB's FISMA reporting process could monitor agency progress in this area annually. OMB has already issued a memorandum directing each agency to review its telecommunications capabilities in the context of planning for contingencies and COOP situations;[28] such reviews should consider not only physical route diversity but also alternate communications mechanisms that could operate should a loss of access infrastructure occur. Finally, DHS's Federal Emergency Management Agency is updating Federal Policy Circular 65 (FPC65), which establishes IT communications requirements for COOP communications and could build NGN-specific requirements into the overall planning effort.

10.0 AGREEMENTS, STANDARDS, POLICY, AND REGULATIONS

Recommendation: The President should direct DHS, the Department of State, and DOC (including NIST and NTIA) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally-distributed NGN environment.

Arrangements and expected behaviors between entities are one of the basic building blocks of the communications infrastructure.[29] These include mutual agreements/Service Level Agreements (SLA), industry standards, accepted policies and Government regulations (collectively, ASPR). Whether between two entities or among hundreds, and whether among companies, Governments, or both, ASPRs have an essential role in ensuring NS/EP communications. Unlike the NS/EP capabilities of legacy networks, which were built on an existing framework, the NS/EP capabilities of the NGN will be developed as the NGN itself is being developed. This requires meticulous care in the establishment of supportive ASPR. To this end, one of the critical goals of the recommendation above, to establish a Common Operational Criteria development framework, is to foster the creation of effective ASPR.

---

28 OMB Memorandum M-05-16, Memorandum for the Heads of Departments and Agencies, June 30, 2005, issued pursuant to Section 414 of Treasury, Transportation, Independent Agencies, and General Government Appropriation Act, 2005 (Division H of P.L. 108-447).

29 *See* Appendix G– Systematic Assessment of NGN Vulnerabilities.

The intrinsic vulnerabilities of ASPR include:[30]

- Lack of ASPR;
- Conflicting ASPR;
- Outdated ASPR;
- Unimplemented ASPR (complete or partial);
- Interpretation of ASPR (mis- or multi-);
- Inability to implement ASPR;
- Enforcement limitations;
- Boundary limitations;
- Pace of development;
- Information leakage from ASPR processes;
- Inflexible regulation;
- Excessive regulation;
- Predictable behavior due to ASPR;
- ASPR dependence on misinformed guidance;
- ASPR ability to stress vulnerabilities;
- ASPR ability to infuse vulnerabilities; and
- Inappropriate interest influence in ASPR.

The intentional or unintentional exercise of any of these vulnerabilities by a threat can significantly impair NS/EP communications. For example, agreed upon standards that are not implemented fail to provide the defined capabilities. Similarly, information leakage through policy development processes and predictable behavior from known regulations can provide tactical advantages to an adversary.

Of course, implementation of this recommendation faces significant challenges. First, ASPR development lifecycles are often very time-consuming. Second, ASPR processes are often

[30] Ibid.

complex, require considerable technical, regulatory, and other expertise. Third, ASPR development often involves a large number of stakeholders and associated interests—including the broad international community. The Common Operational Criteria development framework must be designed to address the vulnerabilities presented by ASPR and the challenges associated with them.

Multiple international standards bodies and industry forums are developing NGN ASPR.[31] Regarding standards, industry vendors and operators are actively developing the requirements, architecture, and detailed protocols. However, Government involvement in these NGN activities is limited. With convergence, and the enhanced NS/EP services that the NGN will provide, an increasing number of standards will be of critical importance. Accordingly, the NGNTF previously recommended that:

- The President should direct his departments and agencies to participate more broadly and actively in the NGN standards process in partnership with the private sector in areas such as web services, directory services, data security, network security/management, and control systems, all of which will become increasingly important to NS/EP communications platforms.[32]

The Government must monitor development of standards that will affect NS/EP communications on the NGN; it must also actively participate and contribute in appropriate fora to influence the development process so that NS/EP needs are better met and new NGN capabilities are available for NS/EP communications. Additionally, the appropriate Government agencies and regulatory bodies must be active in defining NGN NS/EP requirements. Vendors and operators make the best effort possible to represent the governmental and regulatory positions. However, sometimes these positions are interpretations by the various companies of the Government wishes and mandates. It would be beneficial for the NGN standards process if Government representatives could be present during the development of the NS/EP NGN services and capabilities requirements to clarify the Government requirements and mandates.

This work includes such critical areas as resilient communications (see above) and first responder communications[33] needs, critical to support and enhance the end-to-end NS/EP mission. This work should be supported via appropriate private industry and Government resources and technical contributions.

Moreover, leadership in many areas of NGN standards, including some associated with NS/EP communications, resides in international and foreign regional bodies. See Appendix I. Some of these bodies have organizational rules that prevent the participation of companies from various regions of the world. For example, the European Telecommunications Standards Institute (ETSI)[34] TISPAN (Telecommunications and Internet Protocol Harmonization over Networks [TIPHON] and (Services and Protocols for Advanced Networks) [SPAN]) project is developing

31 *See* Appendix I, NGN and NS/EP ASPR Ecosystem

32 NGNTF Near Term Recommendations Working Group Report, March 2005.

33 These standards activities include ITU-R WP8A, Project MESA, and TIA TR-8.8, Broadband Data Systems.

34 ETSI has received repeated complaints about this organizational rule and is considering potential rule changes that would allow U.S.-based companies to participate. No specific changes have been incorporated yet.

sets of NGN-related standards that will probably be attempted to be applied globally. However, the current organizational rules require TISPAN meeting participants to be ETSI members. To be an ETSI member, the associated companies of the participants must have business offices or operating business divisions in Europe. Based on these organizational rules, many of the United States-based companies, including the largest wireless operator in the United States, are prevented from being active participants in the TISPAN activities and are prevented from having access to the members-only area of the TISPAN project that contains detailed contributions and discussion papers.[35] The United States' NS/EP interests could be adversely affected if the ability of its companies and Government to participate in standards development is impaired, and United States NS/EP requirements are not adequately represented.

11.0 INCIDENT MANAGEMENT ON THE NGN

Recommendation: The President should direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the NCC, for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

11.1 Introduction

NS/EP communications incident management has traditionally existed in the realm of the physical event, and a process is in place to manage those events, including how they affect wireline and wireless communications. The NCC has historically assisted in the NS/EP incident management function for communications providers.

However, the NGN environment includes numerous new technologies and new industry players who control key network elements but may not have relationships in place with industry and Government incident managers. Most new communications providers are not members of the NCC, and therefore, they are not as easily accessible during an incident, nor do they reap the benefits of membership, including building trusted relationships with industry and Government. Additionally, the network itself is becoming increasingly complex and global in nature, pushing incident management out beyond the realm of the territorial United States.

As new providers and technologies continue to enter the communications arena, management of cyber incidents and blended physical/cyber incidents has proven more improvisational. Unlike management of physical incidents, management of cyber incidents is associated with limited common terminology, few standard processes, and few established guidelines on how the situation should be handled. Federally funded cyber exercises have been conducted to pinpoint gaps, yet they have not reached the level of sophistication and standardization required. Future cyber exercises should approach the degree of professionalism attained by military exercises in

[35] One method to overcome this challenge is through the use of a trusted third party that meets the ETSI criteria to represent U.S. NS/EP interests. In addition, industry and standards development organizations are working to ensure U.S. requirements are addressed by groups like ETSI.

the areas of planning, organization and evaluation, and must include a feedback loop for discussion and implementation of lessons learned.

Meanwhile, communications providers are transforming their networks by branching out heavily into IP-based wireless and packet-switched communications. These architectures and the host of new providers and technologies create significant challenges for incident management in the NGN.

11.2 Unique NGN Incident Response Issues

The transition period to the NGN presents challenges for ensuring the security and availability of NS/EP communications, including in the broad areas of first responder communications, control systems, such as Supervisory Control and Data Acquisition (SCADA) systems, network gateway protection, Continuity of Operations (COOP), Continuity of Government (COG), and financial services transactions. In addition, new threats and vulnerabilities create complex risk scenarios for NS/EP communications in an NGN environment. A further challenge is the NGN's global nature, which will require that methods for managing incidents of national significance address international cooperation.

The time available to respond to or thwart a cyber attack on converging networks continues to decrease, making it more difficult for human mitigation of the attack. In the near future, automated mitigation efforts will be needed to effectively manage an incident, which only increases the complexity of the NGN environment and effectively removes incident control from human hands. With the reduced response time, incident managers have even less time to thwart cyber attacks and must focus their efforts on response and mitigation.

The open, layered architecture or nature of the NGN facilitates the offering of new services and services from new providers. Many new providers are unfamiliar with NS/EP incident response. Corporate "attitudes" may differ between the two entities on incident management priorities—for instance, NS/EP incident management often requires more information sharing and collaboration with Government entities than is normal for nontraditional providers. New providers existing in an unregulated environment are more hesitant to develop relationships with Government entities. The providers have created informal incident response networks that have been sufficient to respond to customer needs, and yet they may not be formal enough to ensure NS/EP communications will remain secure and available during an incident of national significance. Companies will need to develop a mutual understanding on how to meet customer expectations for service on the NGN while continuing to ensure that NS/EP capabilities, including priority treatment of communications, are available to the Government and other incident managers at appropriate times.

With increasing complexity, interdependencies (known and unknown) and the distributed nature of the network, management plans will need to remain flexible to account for numerous attack methods, recognizing the limitations of a one-size-fits-all approach. The key to NGN incident management will be to maintain the level of service expected today by consumers while balancing new threats.

11.3 Industry Involvement Throughout the Planning Process

Incident response must be a joint effort between industry and Government. As such, industry and Government must work jointly on strategic policy for incident management from its earliest stage of development. This would be a change from the current process in which Government produces a formal plan and industry is asked to comment in the plan's final stages. The private sector should be more active during planning and response, but as part of a collaborative process as an equal partner with Government.

DHS has published a variety of high-level plans, including the National Response Plan (NRP) and the National Incident Management System (NIMS). For the most part, these plans exist at a very high level, and are derived from a background of physical rather than cyber events. From an incident management perspective, the plans do not go into detailed processes for incident management and recovery; they are geared more toward offering high-level organizational principles for desired results. NIMS, for instance, is aimed at a very broad audience and is considered a "framework" for responders at all levels to use in working together. These plans, constructed by the Government with little input from industry, provide very little guidance for real-world mechanisms and processes for incident management in an NGN environment. For example, had industry been involved in the detail of the Homeland Security Operations Center (HSOC) approach, industry would likely have been more engaged in the Center's early activities.

11.4 Joint Coordination Center

A joint coordination center for industry and Government should be established. This would be a cross-sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies. Such a center would improve communications between industry and Government as well as among industry members, and would incorporate and be modeled on the NCC.

The center should be a Government-funded, appropriately equipped facility, manned jointly by experts from all key sectors. In a fully converged NGN environment, everything will be interconnected and interdependent to a greater degree, and thus means of coordinating among all key sectors must exist. Physically collocated, joint manning is vital to achieve the high level of interpersonal trust needed for sharing sensitive specific information and to achieve the level of mutual credibility required in a fast-paced decision-oriented environment.[36] It should provide the full set of planning, collaboration, and decision-making tools for those experts to work, whether together as a whole or in focused subgroups.

Industry is at times hesitant to share information with the Government because it is unsure of how the information will be used, and Government-to-industry information sharing should also

[36] "If the partnership between the federal government and private sector is to be successful, another key requirement is establishing a permanent physical location or forum so that critical and non-critical sectors can interface with one another and their federal counterparts. This is essential to developing and maintaining long-term collaborative relationships." A Review of the Top Officials 3 Exercise, DHS OIG Report OIG-06-07, p. 24 (Nov. 2005).

be improved.[37] DHS has a vision for how HSOC will function to improve information sharing; however, the HSOC's current operational interface to the private sector is nascent and needs further development. An environment of trust must be established. A joint operations center could play a key role in fostering that environment and in enhancing HSOC operations. In addition, appropriately cleared industry experts collocated in a joint coordination center with their Government counterparts could assist the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the DHS intelligence analysis arm, in performing its analytical and reporting functions, helping to ensure that HITRAC products are more complete, credible and useful.

11.5 Exchange Program

Incident response, including planning for response, requires a joint industry/Government effort, and each group must better understand the other's role. To this end, an exchange program should be instituted to foster understanding between industry and Government practitioners in network operations, security operations, and crisis management. The groundwork for this initiative has already been laid; an IT Exchange Program[38] (ITEP) has been established by the Office of Personnel Management but has not been implemented in the executive branch or at the Federal department or agency level.

11.6 Federal Incident Management Training Academy

A Federal training academy for incident managers should be established. NGN incident management operations would be improved if cross-sector industry training is available. Accordingly, the Government should set up an all-hazards intensive training center with specific attention played to NGN and cyber issues.

Experienced incident managers have repeatedly stated that having employees with the capability, knowledge, and authority to respond during an incident is far more important than having a detailed written plan. A training academy could immerse students from industry and Government in realistic and intense scenarios over a set period of time, such as a one-week session of round-the-clock incident management immersion.[39] This would also foster strong relationships among NGN incident responders in industry and Government, laying the groundwork for more effective communications during an actual incident.

11.7 Exercise Program

To further the capability, knowledge, and authority of incident managers, a formal exercise program for NS/EP communications incident response on the NGN should also be established. This program should be collaboratively developed, broadly participatory, and regularly evaluated. It could be developed in tandem with the training academy, and would be designed to

---

37 Both these observations were confirmed at the August 2005 NGN Incident Response Subject Matter Experts meetings. *See* Appendix D.

38 *See* http://www.opm.gov/fedregis/2004/69-011504-2311-a.htm.

39 Of interest, a bill has been introduced to establish a "National Homeland Security Academy" which would provide both coursework and hands-on training exercises. S. 2158, introduced Dec. 21, 2005.

fit into national strategic plans such as the NRP. The exercises themselves should be modeled on the level of detail and professionalism demonstrated by military programs. The key to the success of this program will be the implementation of lessons learned into future activities. Industry must be involved early on in the process and should be involved in the creation of the objectives for the exercise.

11.8 Increased Research and Development Funding

As historic methods for responding to incidents become outmoded, R&D funding related to incident management should increase. This investment could fund incident management research toward developing advanced monitoring, detection, decision making, and response capabilities. A concerted effort should be made to research human factors in incident management.

12.0 INTERNATIONAL POLICY

Recommendation: The President should direct his departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-U.S. companies in NS/EP incident response in the United States; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.

Protecting and promoting NS/EP communications requires international action. The NGN will be used globally. NGN communications will transit international borders. Finally, NS/EP services will be provisioned internationally (such as Domain Name System [DNS] services). It is simply not tenable to treat NS/EP communications as a domestic issue only.

Both private industry and Government have made progress in the pursuit of international cooperation and coordination. Industry is inherently international—many if not all NSTAC member companies have international operations—and must work with other international companies and Governments on key issues affecting NS/EP communications. Moreover, formal and informal industry coordination mechanisms operate internationally, and standards development organization have international membership.[40]

The State Department effectively represents the Government in international discussions regarding critical infrastructure protection. Those discussions have recently included the requirements for NS/EP communications. As the highly connected NGN reduces the effect of national borders on our networks, NS/EP communications will increasingly involve international issues. Accordingly, it is critical that upcoming international discussions on critical infrastructure protection include an NS/EP element.

[40] Government participation in international standards development in addressed in Section 10.0.

Many issues, however, remain, including how to handle incident response in a converged environment. See Section 11, above. In short, we have a good understanding of how to handle NS/EP incident response on the existing PSTN, but converged networks are far more likely to involve international players, with incidents first noticed abroad, participants affected abroad, services provided from abroad, or components (hardware/software) provided from abroad. The Federal Government will face difficult issues in deciding whether and how to involve international participants in a national security communications incident when those participants are outside of the United States. Similarly, international companies may have much to contribute to U.S. watch, warning, and incident response capabilities, including the Telecommunications and Information Technology Information Sharing and Analysis Centers (ISACs); however, it is unclear whether participation of international companies in these fora would adversely affect their partnership with the United States. The Federal Government should develop and communicate to industry a rational policy that balances the need for including the most critical companies with protecting the national security of the United States.

Outside the realm of incident response, it is possible that different governments could take contrary approaches to protecting NS/EP communications on the NGN. With widespread international interdependence, such conflicts could undercut the effectiveness of solutions inside and outside of the United States. Accordingly, in the international discussions referenced above, and in other international fora, the Federal Government should seek compatible approaches to NS/EP communications, consistent with the recommendations in this report.

13.0 FIRST RESPONDERS

Recommendation: The President should direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

When mature, the NGN will provide first responder and public safety organizations with much greater capabilities, such as transmission of data real-time along with voice. The NGN will also aid interoperability in cases where "operability" of first responder and public safety networks and the NGN itself are present. The connection or bridging of disparate networks to the NGN will allow communication between them via the underlying protocols of the NGN. *See* Figure 2. As noted in the NGNTF's Near Term Recommendations Report:

- The timely migration to newer digital, interoperable, and standardized solutions, backed by appropriate policy use for such systems, will help ensure that America's first responders are properly prepared, equipped, and able to coordinate their response to all-hazards and emergency situations.[41]

However, significant challenges also surround end-to-end NGN services for first responder and public safety organizations. First responder and public safety networks may be among the last to be upgraded to the NGN due to security and availability concerns arising from interconnection

41 NGNTF Near Term Recommendations Working Group Report, March 2005.

and because of the difficulty, particularly in terms of resources, to upgrade legacy systems. With regard to the former, this Report recommends critical steps to make the NGN an NS/EP-capable network. And with regard to the latter, the Federal Government can play a critical role in supporting the transition of first responders and public safety organizations to the NGN. As stated in the Near Term Report:

- Government agencies, such as [DHS Office of Interoperability and Compatibility[42]], should continue to enhance the capabilities of first responders via the following: providing needed levels of funding for digital equipment; supporting standards and policy development; allocating spectrum appropriately and in an expedited manner; broadening the deployment of WPS; and upgrading Public Safety Answering Points.[43]

14.0 CONCLUSION

The NGN can provide considerable benefits for NS/EP communications; however, to realize these benefits and speed the transition to the NGN, solutions that address NS/EP functional requirements are required, especially for security and availability. This is an end-to-end problem; on a packet-based network such as the NGN, information will travel over various networks and equipment, and a failure at a critical point absent mitigation, such as an alternate communications path, could impair the communication. For the NGN to broadly meet the essential NS/EP functional requirements in a consistent, continuous, and reliable end-to-end manner, a set of mechanisms needs to be promoted and adopted by those supplying network access, transport, and infrastructure services for this community, as well as NS/EP users. Accordingly, industry and the U.S. Government should enhance their partnership to achieve an elevated level of cooperation to implement these mechanisms, developing: organizational solutions for incident management and the partnership itself; cooperative frameworks supporting identification and end-to-end NS/EP communications; technical solutions that support the next generation of NS/EP-supporting technology on the NGN; and policy solutions that address the increasing diversity, complexity, rapidity of change, and international nature of the NGN itself. There is no silver bullet. Government and industry need to work cooperatively to implement a set of solutions that support NS/EP on the NGN.

[42] DHS' Office for Interoperability and Compatibility oversees the SAFECOM program, which "is a communications program that provides research, development, testing and evaluation, guidance and assistance for local, tribal, state, and federal public safety agencies working to improve public safety response through more effective and efficient interoperable wireless communications."

[43] NGNTF Near Term Recommendations Working Group Report, March 2005.