THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Next Generation Networks Task Force

Near Term Recommendations Working Group Report

March 2005

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As wireless and wireline networks converge and extend their interoperability, global Next Generation Networks (NGN) are forming. This convergence is changing how the Federal Government will meet its needs for national security and emergency preparedness (NS/EP) communications. One recent marketplace example of this convergence are phones that can now access an array of web-based services and communicate over Internet Protocol (IP) links to phones on the Public Switched Telephone Network (PSTN).

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 using 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.

At an initial NGNTF meeting of subject matter experts in August 2004, questions from Government stakeholders arose regarding how NS/EP communications would be affected by convergence and the move to the NGN. Of particular interest were efforts that could be taken immediately to preserve or enhance NS/EP communications for the future. To address stakeholder requests to explore those issues, the NGNTF formed the Near Term Recommendations Working Group (NTRWG) to examine near-term opportunities for using existing technology to improve the security and availability of NS/EP communications on converging networks. The NTRWG also looked at areas where Government involvement was needed in the near term because of the immediacy of events — such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs.

Based on the NTRWG's analysis of near-term opportunities to use existing technology, the NSTAC offers the following recommendations.

The NSTAC recommends that the President direct his departments and agencies to:

- Use existing and appropriate cross-government coordination mechanisms to track and coordinate cross-agency NGN activities and investment;

- Explore the use of Government (civilian and Department of Defense) networks as alternatives for critical NS/EP communications during times of national crisis;

- Use and test existing and leading-edge technologies and commercial capabilities to support NS/EP user requirements for security and availability;

- Support the development and use of identity management mechanisms, including strong authentication;

- Study and support industry efforts in areas that present the greatest NS/EP risks during the period of convergence, including: (1) gateways; (2) control systems; and (3) first responder communications systems;

- Review the value of satellite systems as a broad alternative transmission channel for NS/EP communications;

- Participate more broadly and actively in the NGN standards process in partnership with the private sector in the following areas: web services; directory services; data security; network security/management; and control systems; and

- Focus on developing cohesive domestic and international NS/EP communications policy and conduct inter-governmental discussions on NS/EP communications.

1.0 INTRODUCTION

The convergence of the Public Switched Telephone Network (PSTN), wireless networks, and Internet Protocol (IP) networks (including cable providers) into global Next Generation Networks (NGN) is changing how the Federal Government will meet its critical communications needs, such as those supporting national security and emergency preparedness (NS/EP). Although the complete process is expected to take many years, networks are already converging to form the NGN. Within 10 to 15 years, there will likely no longer be entirely separate telephone and data networks. They will be replaced with open and dynamic networks that provide end-users with greater capabilities.

The NGN is expected to carry voice, video, text, and data transparently to many types of end-user devices.[1] As one example, service providers offer phones that communicate over IP links to phones on the PSTN. These new phones access an array of new web-based services such as financial and consumer services, text messaging, graphics, navigation aids, and information services. In this new environment, telecommunications services include infrastructure and network applications and inherent features such as security, messaging, mediation, discovery, collaboration, storage, and other capabilities.

As indicated by previous reports of the President's National Security Telecommunications Advisory Committee (NSTAC), this convergence offers new capabilities to NS/EP[2] users and also presents new challenges. For example, NS/EP users will find the NGN offers significant improvements as bandwidth and software improve, such as delivery of building plans to a first responder in an emergency. The NGN can also provide greater robustness and resiliency via new mechanisms, such as the use of multiple communication mechanisms and redundancy of devices and servers. However, these enhanced capabilities also introduce new and sophisticated security concerns, including: (1) the heightened ability to manipulate the "control space" of communications networks due to the relatively open architecture of the Internet; (2) the increased exposure of signaling data to illicit modification, capture, disruption or falsification as a result of the NGN's use of in-band signaling; (3) a greater vulnerability to remote attacks resulting from the NGN's global interconnectivity; and (4) a potential increase in the amount of traffic lacking sufficient protection due to the NGN's expected shift of responsibility for securing communications from providers to users.

---

[1] The term "NGN" is not intended to represent any single configuration or architecture. Instead it represents the set of converged networks that is 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. More information about the NGN will be found in other reports being generated by the NSTAC NGNTF.

[2] Office of Science and Technology Policy (OSTP) and National Security Council (NSC) regulations 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 regulations 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]).

To address how the Government can meet its NS/EP requirements and address emerging threats on the NGN, the NSTAC Industry Executive Subcommittee (IES) created the Next Generation Networks Task Force (NGNTF) 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.

At an initial NGNTF meeting of subject matter experts in August 2004, Government stakeholders asked for recommendations that should or must be accomplished in the near term. Accordingly, the NSTAC NGNTF created the Near Term Recommendations Working Group (NTRWG) to examine near term opportunities to use existing technology to improve the security and availability of NS/EP communications on converging networks. The NTRWG also examined areas where Government involvement would be needed in the near term because of the immediacy of events — such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs. The full work of the NGNTF continues, and it will produce a report with a completed set of recommendations later in 2005.

2.0 ASSUMPTIONS

The following assumptions apply to the recommendations presented in this report:

- The PSTN and other networks similar to the Internet are already partly converged and a migration to the NGN may involve a period of coexistence;
- The Government can apply the same technologies that are available to industry to NS/EP communications; and
- Response to international emergencies and domestic NS/EP communications, in general, will depend on or be affected by international communications and standards.

3.0 DISCUSSION

The following presents a discussion of the leading near term issues that require Presidential attention as a result of the transition to the NGN.

3.1 Next Generation Networks Activity Coordination

Coordination is needed within the Federal Government to prepare for the transition to the NGN. The following presents a discussion of near term coordination efforts that could assist the Federal Government in proactively managing the transition.

- Coordination and information sharing must occur in the Federal Government regarding NGN activities to save resources, speed implementation of new technologies, and avoid technical, policy, or operational conflicts. For instance, new terms and concepts are currently developing within different groups that must be synthesized to avoid future inter-organizational communication problems. Accordingly, both the Presidential Coordinating Committees and the National Communications System (NCS) should begin to compile common taxonomies and frameworks that leverage these current efforts.

- Enhanced coordination should involve the inclusion of national requirements for NS/EP communications in Federal and Federally-funded NGN initiatives, and should also address requirements such as fostering national economic competitiveness. These issues are complex and should also involve coordination with industry and regulatory agencies. The international nature of the NGN also means that economic issues should involve diplomatic considerations.

- The following scenario is one example of how cross-government coordination could help meet critical NS/EP needs. A disaster could occur at a time when military demands on the Department of Defense's (DoD) still evolving Global Information Grid (GIG) are at near normal levels, while the public and civilian infrastructure is experiencing severe strain. Accordingly, remaining available capacity of the GIG could be allocated to meet critical infrastructure needs. This rapid non-military use of the GIG would only occur with prior policy, coordination, investment, and training undertaken by all relative stakeholders. Similarly, during a widespread emergency affecting critical NS/EP communications, first responders might rely upon Federal network capabilities obtained via the General Services Administration's (GSA) future Networx program to obtain needed capacity or access.

- Certain critical NS/EP issues need urgent attention and coordination. For example, communications used by first responders and relied on by the highest priority public critical infrastructures (such as, finance and energy) are migrating to the NGN and its extended capabilities. Should a catastrophic disaster occur, these communications could be lost or deliberately targeted by adversaries. Although programs and initiatives exist in the Federal Government to address these issues (e.g., Project SAFECOM for first responders' communications), further coordination across agencies and programs is necessary to ensure that such programs and initiatives are complimentary and mutually reinforcing.

- The Federal Government has established a variety of cross-agency coordinating mechanisms, including the Presidential Coordinating Committees, that should be used or revitalized as appropriate to address the issues raised in this and the final report of the NSTAC NGNTF. In addition, the Manager of the NCS should also be charged with addressing the issues described in this report, such as coordinating Federal telecommunications standards.

In light of the above discussion, the NSTAC offers the following recommendations:

- The President should direct his departments and agencies to use existing and appropriate cross-government coordination mechanisms to track and coordinate cross-agency NGN activities and investment; and

- The President should also direct his departments and agencies to explore the use of Government (civilian and DoD) networks as alternatives for critical NS/EP communications during times of national crisis.

3.2 Existing Technologies for Security and Availability

Many existing technologies can help secure and keep NS/EP communications available on converging networks. Often, these technologies are already being used in the private sector for similar purposes. Existing commercial technology can support NS/EP user requirements for prioritization, security, and availability as networks continue to converge. Where such technologies can meet Government NS/EP needs during the transition to the NGN, the Government should use these technologies in place of initiatives focusing on the creation of dedicated capabilities for Government. Where possible, the Federal Government should become a participant in or sponsor of technological trials to test the extent to which the following technologies will meet the needs of the NS/EP community.

Existing technologies that the Government can utilize to support NS/EP needs more effectively are described below.

- **Private IP networks.** Public IP services are exposed to risk from worms and viruses, and exposure to malicious actors, foreign and domestic, who have the time, talent, and motivation to disrupt service. Use of private IP networks can segregate and isolate traffic from denial of service (DOS) or malicious degradation of service attacks. These private IP networks employ the full functionality and features of IP networks without routing or exposure to the public IP network. Network-based Virtual Private Networks (VPN) also provide many of the advantages of private IP networks while distributing many of the costs associated with private communications links.

- **Virtual Private Networks and protocol capabilities**. VPNs enable encrypted, encapsulated packet switching to avoid message theft, recording, or interception. Similar functionality is provided by Internet Protocol Security (IPsec), a set of Internet Engineering Task Force (IETF) standards, for secure communication between single or groups of hosts communicating over Internet Protocol version 4 (IPv4) (for more information see

http://www.ietf.org/html.charters/ipsec-charter.html). Widely implemented by numerous vendors, IPsec adds capabilities that were designed into the next generation Internet Protocol version 6 (IPv6). IPsec is said to operate at "Layer 3," making its use completely transparent to the application in the ideal case (difficulties can emerge in implementation, however). Once two networks establish communication over IPsec, all applications benefit from site-to-site authentication, integrity, and confidentiality.

- **Use of multiple communications paths.** In addition to, or as an alternative to, priority services for communications, attaching a communications device to multiple networks can enhance the resiliency of communications during an incident or attack affecting not all of those networks. For example, a computer device used for NS/EP communications could be homed on two independent IP networks, or on a wireline IP network and a wireless broadband network, such as the 1xEV-Dx, Universal Mobile Telecommunications System network. Border Gateway Protocol (BGP) allows routers to effectively support multi-homing. Moreover, the Stream Control Transmission Protocol (SCTP) is a reliable IETF standard track transport protocol [defined in Request for Comment (RFC) 2960] that supports session continuity for multi-homed hosts and mitigates vulnerabilities inherent in the Transmission Control Protocol (TCP). It should be noted that connecting a device to multiple networks also opens up multiple points of attack; this additional risk must be properly mitigated by existing technologies.

- **Use of existing protocol capabilities.** The IETF has enhanced the Session Initiation Protocol (SIP) for marking a session as requiring preference (priority treatment) and for communicating that indication to subsequent networks. The indication is carried in the optional Resource Priority field [IETF RFC 3487]; and the current proposal supports two Name Spaces so that neither, either, or both an Emergency Telecommunications Service (ETS) indicator and a priority level indicator may be sent. Use of this field by authorized users would allow them to have ubiquitous conductivity for priority communications pending resolution of how to handle NS/EP communications on the NGN. Security measures would need to be created, including a mechanism to limit the use of the Resource Priority field to authorized users, to restrict the effect of DOS attacks exploiting priority service.

- **Peer-to-Peer.** Peer-to-peer software and devices can be used to improve throughput and performance via collaboration among communicating devices that improve robustness and remove single-points-of-weakness. Peer-to-peer computing may also serve as a backup or supplement for primary communications technology, with fewer dependencies on the telecommunications infrastructure.

- **Encryption.** Malicious agents can intercept clear-text communications. Once these communications are intercepted, confidential information can be obtained and subsequently used to degrade or disrupt NS/EP operations. Many application-aware, peer-reviewed, and standards-based encryption techniques such as Secure Shell (SSH), Secure Sockets Layer (SSL), and Transaction Layer Security (TLS) are available to mitigate these threats. The Government should employ these tools for NS/EP users, using appropriate levels of encryption based on the application.

- **Firewalls and intrusion detection systems /intrusion prevention systems.** IP-networks enable global connectivity that challenges service providers to allow only authorized users access to portions of the network while also keeping malicious parties from both accessing networks and executing DOS attacks. An essential network security tool at present is a firewall. A firewall allows the network operator to establish rules to determine what traffic should be allowed in or out of the network. Ideally, a firewall would be able to filter packets at line (optical) rates and might be coupled with intrusion detection systems (IDSs) — which typically have lists of known malicious attacks, or signatures — or intrusion prevention systems (IPSs).

- **Secure techniques for maintenance of network elements**. Effective security is more than installing a single technology or adhering to a distinct process. The network should be maintained by security professionals with appropriate training, certification, and ongoing education. Communication with the network and its supporting elements should be done in a secure mode, using encrypted management tunnels, strong authentication, and limited need-to-know access for individuals. Regular audits of access and modification of elements should be conducted to determine compliance. If out-of-band management via modems is used, available secure mechanisms, including encrypted modems that support strong authentication and call back to authorized locations, should also be used.

- **Enterprise-level scanning, administration, and remediation (including patch management) tools.** Networks can be affected by excessive traffic created by self-propagating viruses, worms, and other attacks. This traffic can degrade or collapse services necessary for NS/EP communications. The network and all supporting elements should sustain standard, enterprise-level network tools (including automated configuration control and patch management) to identify and remediate security vulnerabilities (including patch management tools) in network elements, communications devices, and servers essential for the delivery of NS/EP services.

- **Resiliency and robustness for critical services.** Networks should be constructed to ensure service during intentional DOS network attacks that may be orchestrated in concert with physical events. Servers hosting critical NS/EP services should be secured using appropriate best practices, including configuration and patch management and availability of backup power/cooling. Such servers, or servers under attack, can also be massively, and perhaps dynamically, replicated. For example, application load-balancing techniques that use routers to distribute traffic are available today. Anycast is a developing technique in which two or more devices offering equivalent service share the same IP address but often in different locations within the same or different autonomous systems. The technique is applicable to both IPv4 and IPv6 and is described in several informational RFCs.[3] Anycast can provide fast, application-independent redundancy to a set of critical services such as Domain Name System (DNS) or other directories.

[3] *See* http://www.ietf.org/.

- **Network-Based Availability Techniques.** DOS attacks and vulnerabilities of routing protocols are subjects of increasing concern. Along with route and packet filtering, other defenses may limit the effectiveness of DOS attacks.

  – Accordingly, the NGNTF believes that the Government should support the further development and usage of the following network-based availability techniques:

    ·· Packet filtering at the edge of Internet Service Provider (ISP) or carrier networks to reduce the effect of DOS attacks, which often rely on false source addresses;

    ·· The filtering of routing advertisements to significantly reduce the hijacking of routes; and

    ·· Appropriate detection (including distributed sensors) and filtering technology to allow carriers to monitor, profile, and filter attacks in real time.

  – Filtering at the national border has been suggested by some but would need to be examined in detail because of possible collateral effects, given the interdependence of the communications infrastructure (private and public), the need for international Government and business communications, and so forth. It is imperative that filtering not impair critical network communications, such as NS/EP communications, encrypted communications,[4] and critical network services. It must be recognized that filtering can become a vector for a self-DOS attack, unless it is properly tailored.

  – It should also be noted that primary responsibility for implementing network-based availability techniques lies with the private sector. Federal agencies, however, should implement such techniques as appropriate and support the private sector's efforts to implement such techniques.

In light of the above discussion, the NSTAC offers the following recommendations and findings:

- The President should direct his departments and agencies to use and test existing and leading-edge technologies and commercial capabilities to support NS/EP user requirements for security and availability. Where such technologies can meet Government NS/EP needs during the transition to the NGN, they should be used in place of initiatives focusing on the creation of dedicated capabilities for Government;

- The NCS should continue to monitor private sector implementation of existing commercial technologies to determine their effects on the resiliency of public IP networks and their effects on NS/EP communications; and

[4] Because the NGN will be composed of devices with powerful computational capabilities, it is infeasible to prevent end users from encrypting their own content and transmitting it across the network. Nothing in the NGN should be built under the assumption that NGN providers will be able to decrypt all communications flowing across their network.

- The NCS should also examine opportunities to participate in technical trials to test the effectiveness of existing commercial technologies to meet NS/EP needs.

3.3 Identity Management

In an NGN environment, with an array of diverse networks, applications, terminals, and access points worldwide, the ability to identify an individual user or communicating entity in a trusted fashion becomes a significant challenge. Accordingly, strong authentication (and determination of authorization) is critical for NS/EP applications and services and the ability to meet other Government requirements.[5] The following points serve to expand on the issue of identity management.

- During the transition to the NGN, strong identification for devices, applications, and sensors will become increasingly important and necessary. For example, communications from sensors for critical Supervisory Control and Data Acquisition (SCADA) systems qualify as NS/EP communications.

- The existing, controlled-access PSTN and services offered on it have long had the technical capabilities, business incentives, and regulatory requirements that resulted in secure, authenticated standardized directories that are shared by authorized providers and Government authorities. These directories are used for various purposes, ranging from fraud management to calling name, and including prioritization use during national emergencies.

- Alternately, general trusted user identification requirements do not exist today in the IP-enabled services environment where a user or service provider can essentially operate anonymously. Trusted user identification can be and is performed on a service-by-service basis (e.g., Internet banking). As NGN capabilities evolve, additional trusted user identification services and secure directories could be introduced as value-added services conforming to security standards.

- Authentication and the sharing of authentication information through directories or other routes may be of increased importance on IP networks, which are similar to the Internet in their open, diverse, and anonymous nature. Directories can and will be managed by enterprises, and may work along with more distributed authentication mechanisms to provide authentication solutions on the NGN.

- The NGN infrastructure encompasses inherently the integration of multiple network platforms and service capabilities. NS/EP needs in the NGN environment will depend highly on seamless interoperability that allows access to the same information and capabilities, irrespective of the access point or application.

[5] This is not to say that all access will be authenticated, which is impractical in the near term and probably undesirable in the long term. Certain uses of the NGN will probably remain anonymous, perhaps including reporting of public health information to widespread, anonymous users. We should not assume authenticated access will be required for all NS/EP uses.

- A variety of cryptographic key and biometric tools and applications exist to help identify users, instantiate identification in trusted directories as appropriate, and subsequently verify a user invoking network communications capabilities. Indeed, the computing power and versatility of end-user devices on IP networks permits greater assurance at a lower cost than is available on the PSTN. IP networks readily support strong authentication (e.g., well-designed two-factor authentication regimes using both a password and a token), whereas Government Emergency Telecommunications Service (GETS) is based on a static, numeric password only.

- Establishing requirements for NS/EP user authentication and/or directory storage is highly desirable. Taking such near term action in a uniform fashion — particularly on a global basis — could benefit the NS/EP community, including lowering the administrative burden of authentication management.

- To define a standards mechanism for Internet directories, in 2002, the IETF created the Cross Registry Information Service Protocol (CRISP) working group.[6] The intent of this working group was directed at providing secure, authenticated directory capabilities in an IP-enabled services world.

- The CRISP working group has thus far produced a generic Internet Registry Information Service (IRIS) specification, including three specific Extensible Mark-Up Language (XML) schema for signaling services: Electronic Number, DNS, and reverse DNS.[7]

- Federal enterprise efforts to enhance identity management are occurring as part of the e-Authentication Initiative,[8] through the Federal Identity Credentialing Committee (FICC),[9] and through development by the National Institute of Standards and Technology (NIST) of a Personal Identity Verification standard pursuant to Homeland Security Presidential Directive – 12.[10]

---

[6] *See 2.1.1 Cross Registry Information Service Protocol (crisp),* Proceedings of the Fifty-Fourth Internet Engineering Task Force, Yokohama, Japan, 14-19 Jul 2002, http://www.ietf.org/proceedings/02jul/106.htm.

[7] The core protocol is IRIS. *See IRIS - The Internet Registry Information Service (IRIS) Core Protocol*, draft-ietf-crisp-iris-core-07, 13 Jul 2004, http://www.ietf.org/internet-drafts/draft-ietf-crisp-iris-dreg-07.txt. The IP Address directory service is supported by an XML schema designated AREG. *See IRIS - An Address Registry (areg) Type for the Internet Registry Information Service*, draft-ietf-crisp-iris-areg-06, 5 Aug 2004, http://www.ietf.org/internet-drafts/draft-ietf-crisp-iris-areg-06.txt. The DNS name directory service is supported by DREG. *See IRIS - A Domain Registry (dreg) Type for the Internet Registry Information Service*, draft-ietf-crisp-iris-dreg-07, 13 Jul 2004, http://www.ietf.org/internet-drafts/draft-ietf-crisp-iris-dreg-07.txt.

[8] *See* http://www.cio.gov/eauthentication, and OMB memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* (December 16, 2003).

[9] *See* http://www.cio.gov/ficc. The FICC is chartered to make policy recommendations and develop the federal identity credentialing component of the Federal Enterprise Architecture. *See* http://www.cio.gov/ficc/documents/ficccharter.htm.

[10] *See* http://csrc.nist.gov/piv-project/index.html.

- Authorization, as distinct from authentication, remains a critical challenge. Authentication is the process of establishing user identity, while authorization is the process of assigning rights and privileges to an identified user. Authentication information can be provided through NGN-accessible directories, but authorization information cannot be provided to the same extent as it is a local decision. The PSTN was designed in an environment where the differences between authentication and authorization were small. Conversely, in the NGN, the differences will be significant. The challenge of effectively managing authorization information in a distributed environment requires further study.

In light of the above discussion, the NSTAC offers the following recommendations and findings:

- The President should direct his departments and agencies to support the development and use of identity management mechanisms that are more effective than those currently in place on the PSTN, including strong authentication;

- Federal use of more secure commercially-available identity management mechanisms for NS/EP could create incentives for the development or use of infrastructure to support those mechanisms, leading to overall security improvement on IP networks. The Federal Government should examine use of secure, authenticated, and standards-based directory services and/or strong authentication in appropriate applications; and

- NS/EP needs and requirements in identity management should be addressed specifically in a coordinated and unified fashion by the relevant fora, with NCS participation. For this effort to be most effective, the relevant entities, including NCS and the FICC, must also work with the private sector to avoid conflicting solutions, encourage the use of existing mechanisms, and coordinate with other standards bodies.

3.4 Areas of Critical Risk

The following presents three areas of critical risk to NS/EP communications that have emerged as communications networks begin their transition to the NGN. They include gateways, control systems, and first responder communications.

3.4.1 Gateways

The security of gateways between networks is critical, especially as different networks that are converging may employ diverse security models or have different vulnerability and threat exposure. For example, because the Internet, and likely the NGN, are open architectures that do not assume authorization from access to the "control space" (whereas authorization was assumed in the controlled-access PSTN control space), non-secure gateways can allow malefactors to access the PSTN control space, where authorization may be assumed and where greater damage could be wrought.

In response, the NSTAC offers the following finding:

- The Federal Government should continue to support the private sector as it seeks to ensure the security of gateways between networks during the transition to the NGN, using in part the technologies identified in this report.

3.4.2 Control Systems

A major challenge in securing control systems — SCADA, Digital Control Systems (DCS), Process Control Systems (PCS) — is educating industry, including both users and developers/vendors, as to the importance and scale of the challenges these infrastructures face (e.g., secure design, development, and delivery). Information Technology (IT) and control systems specialists have historically had very different backgrounds with different assumptions and approaches to security for such systems. Recent efforts in the Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection (IAIP) Directorate are making inroads in this area, and vendor education should begin to emerge through work at the Idaho National Laboratory (INEEL) and Sandia National Laboratory. Optimally, DHS should concentrate on initiatives that have broad benefits across sectors. The following points serve to expand on the issue of control systems.

- Users of control systems find it difficult to determine if critical, dedicated, or even redundant links are actually robust for a given control center link. To assist with this, the NCS' Network Design and Analysis Capability (NDAC) has amassed a set of data, tools, and models that characterize various aspects of communications; additionally, other resources are available.[11] Accordingly, the capabilities of the NDAC, with the assistance of control systems experts, can be applied to challenges within the control system domain.

- Securing control systems is particularly difficult because they have a long capital equipment life and slow upgrade paths. Severing control systems links to the Internet/NGN is no longer possible or efficient in many cases. Existing solutions, such as those described in this report, will need to be applied to address security during migration to the NGN even though end-to-end security and complete authentication will not be possible on many of these systems' links due to performance limitations of end-computing devices and real-time control constraints.

- DHS has emphasized the need to improve the security of control systems and is working to develop a Control Systems Center, a Control Systems Security and Test Center, and a Control Systems gap analysis.

[11] Operators can examine the work of the Alliance for Telecommunications Industry Solutions (ATIS) on diversity of communications links, and, more generally, resources available at the Center for SCADA Security (http://www.sandia.gov/scada/home.htm) and NIST (the Process Control Security Requirements Forum (http://www.isd.mel.nist.gov/projects/processcontrol/)).

In light of the above discussion, the NSTAC offers the following finding:

- The Government should continue to encourage efforts to secure control systems, using in part the technologies identified in this report. The Government should also encourage efforts to understand the security issues that arise in control systems as networks continue to converge.

3.4.3 First Responders

The Nation's Federal, State, and local first responder agencies have historically depended on their own radio systems. These systems are often incompatible with those belonging to other agencies with whom they work. Additional funding to meet first responders' interoperable communications needs is of paramount importance to ensure the necessary exchange of information occurs during critical day-to-day operations and in peak times of emergencies. To coordinate their response, different jurisdictions and agencies must be able to effectively communicate with one another in real-time. 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. The following points serve to expand on this issue.

- During the September 11, 2001 attacks, fire and rescue units from a multitude of jurisdictions could not communicate because their equipment was tuned to different radio bands. Increasing the amount of available and coordinated spectrum will assist first responders during national and local emergencies and will increase their ability to facilitate joint responses across jurisdictions. Additionally, expedited allocation of increased appropriate spectrum will allow operators and vendors to plan for service deployments. The full value of interoperability across public safety jurisdictions will be obtained if all the jurisdictions complete the transition to the NGN as near in time to one another as is practical.

- Wireless Priority Service (WPS) is available only to designated individuals at the following Government levels: national security, emergency responders, and private sector critical infrastructure leaders and decision makers. WPS was approved by the Federal Communications Commission (FCC) for NS/EP requirements on a call-by-call priority basis. When trying to make a call in times of an emergency, approved WPS users will have the ability to gain priority access to the next available cellular channel to place their call. This service will greatly enhance their ability to complete wireless calls during critical times and communicate vital decisions and reports during emergency situations. The value of such critical NS/EP services would be enhanced by increased Federal funding for and ubiquitous deployment of WPS across all NCS identified wireless platforms and deployed infrastructures. This funding would also speed implementation of this capability, which would be useful in addressing the threat of terror and natural disasters.

- As networks migrate to the NGN, the need for upgrading Public Service Answering Points — which are responsible for responding to emergency calls from the public — becomes

urgent, as these points could become the bottleneck to deployment and use of advanced capabilities possible with the NGN.

- DHS has emphasized the importance of first responder communications through the SAFECOM initiative and the creation of the Office of Interoperability and Compatibility (OIC).

In light of the above discussion, the NSTAC offers the following finding:

- Government agencies, such as OIC, 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.

3.4.4 Critical Areas—Conclusion

To conclude discussion of the critical areas set forth above, the NSTAC offers these final recommendations and findings:

- The President should direct his departments and agencies to study and support industry efforts in areas that present the greatest NS/EP risks during the period of convergence, including: (1) gateways that allow access to the control space of the PSTN; (2) control systems that were not designed to operate in or communicate using NGN's open communications environment; and (3) first responder communications systems, which are frequently under-funded, outfitted with outmoded technology, and may face heightened threats; and

- DHS should also continue to monitor progress in each of these areas and ensure that they are appropriately addressed in its strategic plans and in the plans of its various components.

3.5 Satellites

Satellite technology is poised to become an important component of the redundancy of the NGN. Thus, steps should be taken in the near term to ensure the future availability and reliability of satellite systems for NS/EP communications on the NGN. The following points serve to expand on this issue.

- New satellite services with potential value to NS/EP NGNs continue to be developed, including satellite-digital audio radio, Ka-band systems for wireless broadband, aeronautical broadband services, modifications to direct broadcast satellite systems, and the Broadband Global Area Network service.

- Concurrently, although IP communications are already transmitted over satellite links, IP and networking standards may not account for larger latencies as experienced by satellites that can result in unnecessarily poor application performance across those links, especially with voice, video, and SCADA-related applications. Moving forward, these issues must be addressed.

In light of the above discussion, the NSTAC offers the following recommendations and findings:

- The President should direct his departments and agencies to review the value of satellite systems as a broad alternative transmission channel for NS/EP communications and advocate or contract for the inclusion of appropriate capabilities in such systems; and

- The NCS should undertake a survey of satellite systems in development, determine their value for NS/EP communications, and propose mechanisms for best use of such systems. NCS should coordinate with DoD's Strategic Command and the Defense Information Systems Agency (DISA) to leverage their expertise and work with satellite vendors.

3.6 Standards

The NSTAC has frequently recommended that the Government continue to communicate NS/EP needs to the standards community. With convergence, and the enhanced NS/EP services that the NGN will provide, additional standards will be of critical importance. The following points serve to expand on this issue.

- In particular, NS/EP users need to be concerned not only about the communications transport infrastructure, but also the NS/EP services that will ride on top of that infrastructure (e.g., the ability of a first responder to download a building plan from a Government server, which may pull data from other remote servers). Accordingly, NS/EP requirements must be considered both in traditional telecommunications and networking standards bodies — including the International Telecommunication Union (ITU), ATIS, the Telecommunications Industry Association and the FCC's Network Reliability and Interoperability Council (NRIC), among many others — and in nontraditional standards being set for identity management and web services.

- For example, the Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business and web services standards and is developing standards addressing emergency services, Public Key Infrastructure (PKI), security, reliable messaging, etc.

- Also, the IETF has developed an initial ensemble of IRIS standards, but these IRIS standards have not found their way into national NGN standards bodies, nor have secure, authenticated directory services been implemented into standards in most countries.

- Other areas in which standards are being set and where NS/EP requirements may be important to include are: definitions and representations of the secured and managed objects in the computing environment; policy-based security and management (e.g., Distributed Management Task Force; NGN signaling services; and IP-based instrumentation for application, information (data), network, and device security and management interfaces using current and emerging technology including Simple Object Access Protocol (SOAP) and web services.

- In addition, although there is some work on control systems (SCADA/DCS/PCS) protocols to add stronger message authentication, encryption, and intrusion detection/protection, etc., many of the control protocols that will sit on top of the NGN may not take advantage of proposed NGN security mechanisms and methodologies.

- NCS has been broadly involved in traditional telecommunications standards bodies, as well as work by other standards bodies on standards and protocols that are specifically associated with voice communications. However, NCS has not been resourced to participate in relevant standards efforts associated with IP transport, applications, etc.

- Government participation in such efforts should continue to be centrally coordinated by the NCS. The agency must be funded adequately to allow participation in the broader array of standards groups to ensure that rapid cross-organizational coordination occurs and to ensure that existing or evolving commercial, national, and international standards are used when possible.[12]

- Further, the Federal Government can be a participant in or sponsor of technological trials that follow the development of many standards to determine whether they meet the needs of the NS/EP community.

In light of the above discussion, the NSTAC offers the following recommendations and findings:

- 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;

- The NCS should continue to provide central coordination for NS/EP standards activities, using existing or evolving commercial, national, and international standards where feasible. Moreover, funding must be available for Federal Government participation in and coordination of standards activities; and

[12] Executive Order 12472 provides that the Manager of the NCS shall, "[p]ursuant to the Federal Standardization Program of the General Services Administration, and in consultation with other appropriate entities of the Federal Government including the NCS Committee of Principals (COP), manage the Federal Telecommunications Standards Program, ensuring wherever feasible that existing or evolving industry, national, and international standards are used as the basis for federal telecommunications standards."

- The NCS should also examine opportunities to participate in technical trials to test the effectiveness of current or developing standards to meet NS/EP needs.

3.7 International

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 DNS services). The following points serve to expand on this issue.

- It is important to use existing capabilities when considering the use of NS/EP services in the NGN's international environment. The ITU — Telecommunication Standardization Sector has developed a protocol to permit international priority calls, an International Emergency Preference Scheme call, but this protocol is not implemented due to lack of a policy on its use.

- The United States Government must also continue to enhance international cooperation to ensure NS/EP issues are adequately addressed. 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.

In light of the above discussion, the NSTAC offers the following recommendations and findings:

- The President should direct his departments and agencies to focus on developing cohesive domestic and international NS/EP communications policy and to conduct inter-governmental discussions on NS/EP communications;

- The NCS should develop policy regarding international emergency calls and transmissions entering or exiting the domestic PSTN; and

- The Department of State and other Government agencies should continue to raise issues related to NS/EP communications in international discussions regarding critical infrastructure protection.

4.0 RECOMMENDATIONS TO THE PRESIDENT

The NSTAC recommends that the President direct his departments and agencies to:

- Use existing and appropriate cross-government coordination mechanisms to track and coordinate cross-agency NGN activities and investment;
- Explore the use of Government (civilian and DoD) networks as alternatives for critical NS/EP communications during times of national crisis;
- Use and test existing and leading-edge technologies and commercial capabilities to support NS/EP user requirements for security and availability;
- Support the development and use of identity management mechanisms, including strong authentication;
- Study and support industry efforts in areas that present the greatest NS/EP risks during the period of convergence, including: (1) gateways; (2) control systems; and (3) first responder communications systems;
- Review the value of satellite systems as a broad alternative transmission channel for NS/EP communications;
- Participate more broadly and actively in the NGN standards process in partnership with the private sector in the following areas: web services; directory services; data security; network security/management; and control systems; and
- Focus on developing cohesive domestic and international NS/EP communications policy and conduct inter-governmental discussions on NS/EP communications.

5.0 OTHER FINDINGS

In addition to the above, the NSTAC finds that Federal departments and agencies will profit from the following actions:

- The NCS should continue to monitor private sector implementation of existing commercial technologies to determine their effects on resiliency of public IP networks and their effects on NS/EP communications;
- The NCS should examine opportunities to participate in technical trials to test the effectiveness of existing commercial technologies to meet NS/EP needs.
- Federal use of more secure commercially-available identity management mechanisms for NS/EP could create incentives for the development or use of infrastructure to support

those mechanisms, leading to overall security improvement on IP networks. The Federal Government should examine use of secure, authenticated, and standards-based directory services and/or strong authentication in appropriate applications;

- NS/EP needs and requirements in identity management should be addressed specifically in a coordinated and unified fashion by the relevant fora, with NCS participation. For this effort to be most effective, the relevant entities, including NCS and the FICC, must also work with the private sector to avoid conflicting solutions, encourage use of existing mechanisms, and coordinate with other standards bodies;

- The Federal Government should continue to support the private sector as it seeks to ensure the security of gateways between networks during the transition to the NGN, using in part the technologies identified in this report;

- The Government should continue to encourage efforts to secure control systems, using in part the technologies identified in this report. The Government should also encourage efforts to understand the security issues that arise in control systems as networks continue to converge;

- Government agencies, such as OIC, 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;

- DHS should continue to monitor progress in such critical areas as gateways, control systems, and first responder communications systems, and ensure that these devices and systems are appropriately addressed in DHS' strategic plans and in the plans of its various components;

- NCS should undertake a survey of satellite systems in development, determine their value for NS/EP communications, and propose mechanisms for best use of such systems. NCS should coordinate with DoD's Strategic Command and the DISA to leverage their expertise and work with satellite vendors;

- The NCS should continue to provide central coordination for NS/EP standards activities, using existing or evolving commercial, national, and international standards where feasible. Moreover, funding must be available for Federal Government participation in and coordination of standards activities;

- The NCS should examine opportunities to participate in technical trials to test the effectiveness of current or developing standards to meet NS/EP needs;

- NCS should develop policy regarding international emergency calls and transmissions entering or exiting the domestic PSTN;

- The Department of State and other Government agencies should continue to raise issues related to NS/EP communications in international discussions regarding critical infrastructure protection; and

- Within six months after issuance of this report, representatives from the NSTAC should meet with the NCS's COP and other stakeholders to review this report and the actions taken regarding it. Before that meeting, the NCS should prepare a report summarizing actions taken with regard to each recommendation. If appropriate, subsequent reviews should be scheduled at that time.

APPENDIX A: TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER INDUSTRY WORKING GROUP MEMBERS

NSTAC TASK FORCE MEMBERS

BellSouth	Mr. David Barron, Co-Champion
Microsoft	Mr. Philip Reitinger, Co-Champion
Raytheon	Mr. James Craft, Co-Champion
Boeing	Mr. Robert Steele
Computer Science Corporation	Mr. Guy Copeland
SAIC	Mr. Hank Kluepfel

OTHER INDUSTRY WORKING GROUP MEMBERS

Bechtel	Mr. Fred Wettling
Cingular	Mr. Richard Tam
Global Internetworking	Mr. Gary Hale
Idaho National Laboratory	Mr. Wayne Austed
Juniper	Mr. Martin Schulman
Lucent Bell Labs	Mr. Stuart Goldman
Motorola	Mr. Dragan Boscovic
Raytheon	Mr. Michael Daly
Sprint	Mr. Stephen Gillian
Sprint	Mr. Brad McManus
Telcordia	Mr. Robert Lesnewich
Telecommunications Industry Association	Mr. David Thompson
VeriSign	Mr. Anthony Rutkowski

GOVERNMENT PARTICIPANTS

Department of Transportation	Mr. Everett Dowd
Department of Transportation	Ms. Hollace Twining
National Institute of Standards and Technology	Mr. David Su

APPENDIX B: ACRONYM LIST

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

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