NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

March 12, 2009

The Honorable Barack H. Obama
The White House
Washington, DC 20500

Dear Mr. President:

Your National Security Telecommunications Advisory Committee (NSTAC) has been asked to provide input to Dr. Melissa Hathaway's *Sixty-Day Cyber Study Group* by answering four specific questions. We are pleased to have the opportunity to support this important work and feel we can provide valuable insight given our focus national security.

In approaching this work we reviewed a considerable body of previous NSTAC work that has lead to the responses in the attached document. We have also included some broader policy issues not previously addressed by your NSTAC that may warrant additional exploration as your Administration sets its cybersecurity agenda.

It is important to note that several themes continue to emerge that we believe are of particular significance:

- Integration of Federal cybersecurity activities under a single, central organizing governance structure. This is foundational to making meaningful progress.
- Collaboration with industry in the development of a legal framework to protect the nation's critical infrastructure from cyber threats.
- Continued commitment to foster a strong public/private partnership in order to strengthen our national cybersecurity posture.

On behalf of the NSTAC Principals, thank you for this opportunity and we look forward to our continued work with you and your Administration on this and other issues critical to our national security.

Sincerely,

Edward A. Mueller
NSTAC Chair

Attachment:
NSTAC Response to the White House Cyber Review Questions

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Response to the Sixty-Day Cyber Study Group

March 12, 2009

1.0 INTRODUCTION

The President's National Security Telecommunications Advisory Committee (NSTAC) is pleased to know that the Obama Administration understands that cyberspace is a strategic asset and that its protection should be considered a national security priority. The NSTAC agrees with this posture and has examined issues pertaining to national security and emergency preparedness (NS/EP) communications in a converged environment for many years.[1]

The NSTAC is aware that a significant amount of work is being done across the Federal Government and within a number of advisory committees and industry organizations. The NSTAC appreciates the opportunity to provide input to the Executive Office of the President's (EOP) cybersecurity review and believes it is well positioned to offer a unique insight given its national security focus. The Government, inclusive of State and local authorities responsible for protecting critical infrastructure from physical threats, and the private sector share the responsibility for securing cyber space and the Nation's critical communications infrastructure. This responsibility benefits from complementary skills sets and resources possessed by both Government and industry to address cyber threats and threats to the physical infrastructure. In moving forward, it is essential the Government and the private sector adopt a coordinated approach to achieving joint goals in a manner that is consistent with the Constitution and laws of the United States, as well as principals of effective governmental and commercial enterprise management. While many of the NSTAC's past recommendations address the Government's role in the protection of the physical networks or specific assets, many of the same concepts apply to protecting logical network assets through cybersecurity. The eight specific recommendations in response to the fourth question set forth a wide range of ideas and priorities that industry and Government must work on collaboratively.

The NSTAC responses to the four questions posed by the White House are contained in the sections that follow. In the interest of developing a logical flow, the NSTAC has responded to the questions in the following order:

- What should be the Government's role(s) in securing/protecting the critical infrastructures and private sector networks from attack/damage, etc. (from nation states, natural disasters, and catastrophic vulnerabilities)?
- What organizational structures are necessary to support national security/emergency preparedness communications needs in a converged environment?
- What gaps exist in federal authorities (laws/regulations/policies)?
- Based on your experience and expertise and your previous recommendations in this area, please provide us with a prioritized list of ten areas that require immediate attention?

[1] See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force*. October 1990; *NSTAC Network Security Task Force Report.* July 1996; *Next Generation Networks Task Force Near Term Recommendations Working Group Report*. March 2005; *NSTAC Next Generation Networks Task Force Report*. March 2006; and the NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President. November 2008.

2.0 ROLE OF THE GOVERNMENT

What is the Government's role(s) in securing/protecting the critical infrastructures and private sector networks from attack/damage, etc. (from nation states, natural disasters, and catastrophic vulnerabilities)?

Today's threat environment extends well beyond unauthorized entry into buildings or simple penetration into the critical communications infrastructure. The environment now includes largely unpredictable cyber threats that extend from often unknown actors in unknown locations. There are still many unresolved questions pertaining to cyber attacks, such as whether or not businesses and organizations can survive an attack; how one detects and prosecutes criminals in a borderless environment; and how one distinguishes a criminal, terrorist, and/or state-sponsored threat when many attacks are undetected, unchecked, and contain no markings that easily provide attribution. The Federal Government is responsible for ensuring the safety and security not only of its citizens, but also of its own infrastructure and communications requirements. The integration of Federal cybersecurity efforts under a centralized Federal structure will promote information sharing and provide the situational awareness critical to address cyber incident management and improve interagency coordination.

The following issues are broad areas of policy and practice where the Government can take a lead cybersecurity role in its partnership with the private sector.

2.1 Information Sharing

The Government can provide support to industry by examining the need to further strengthen critical information sharing mechanisms between industry and Government and advancing operational measures to ensure cybersecurity.

Due to the interconnected and interdependent nature of communications networks, global service providers have fostered crucial information sharing and cooperative response and recovery relationships for decades, recognizing that a single network anomaly will generally affect multiple provider-owned and -operated networks. In support of the country's national security telecommunications agenda, the Government created the National Coordinating Center (NCC) in 1984, followed by the Network Security Information Exchange in 1991. These two joint information sharing mechanisms remain valuable today both for physical and digital coordination. However, in order to provide a more complete picture of information sharing, network operators must receive actionable intelligence and threat information.

In cyberspace, just as in physical space, there is a joint need for Government and the private sector to work together in preventing unauthorized access to systems or property. Information sharing should be viewed as having two major elements: (1) monitoring and early warning; and (2) real time information sharing. The policy of the U.S. Government should be to: (1) share information, both classified and unclassified, that could affect the security practices that industry employs regarding network operation centers with U.S. service providers; and (2) undertake an

information sharing process review to determine that the U.S. Government has the appropriate mechanisms, responsibility designations, and directives in place that allow for the sharing of such information.[2] Further, information sharing must take place in an environment that protects trade secrets and proprietary information, and mitigates anti-trust concerns.

2.2 Lead By Example

In the defense of cyberspace, it is important that Government, in collaboration with industry, lead by example by properly securing its infrastructure, including Government-owned computer networks and equipment. Examples of Government progress in this area include the reduction of points of network ingress/egress and increased monitoring of Federal agency networks. Businesses, organizations, and citizens should be able to look to Government for ways to foster information security in the digital age. Government should also demonstrate best practices and share lessons learned with private citizens and organizations, rather than mandating particular methods or approaches to securing computer systems and networks. It is imperative that the Government make its accumulated body of knowledge available to the public for use, as needed. The Government's ability to provide best practices and guidance to those unable to develop or access them on their own is especially important.[3]

In recent reports, the NSTAC made a number of recommendations in the areas of critical mission identification, improvements in contingency planning, and amending Government Internet protocol (IP) traffic management and procurement policies, which might enhance not only the Government's security and resiliency, but also set an example for other organizations in similar positions. Representative excerpts from those recommendations are described in the following sections on critical mission identification and Government essential missions, improvements in contingency planning, enhancement of IP traffic management practices, and procurement.

Critical Mission Identification and Government Essential Missions:
To diminish the likelihood of single points of failure occurrences impacting NS/EP and mission critical operations, the Government should identify its essential services and infrastructure, gaps in coordinated protective initiatives such as the Telecommunications Service Priority (TSP) program, and service level agreements with the private sector that fall short of identified protective requirements. Several actions are needed:

- Extend National Communications System Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, to direct all Federal agencies to conduct agency specific mission reviews to identify the services and infrastructures that are essential to their missions.
- Direct the Department of Homeland Security (DHS) to amend any critical infrastructure protection approaches and criteria to include content and service dependencies.
- Undertake Government-focused, risk-based assessments of NS/EP and mission-essential Governmental functions and their reliance and dependence on new and emerging core network elements, such as the domain name servers (DNS), certificate authorities (CA), and search and

[2] *NSTAC Report to the President on Network Operations Centers.* August 2008. Page 13.
[3] *NSTAC Report to the President on the Physical Assurance of the Core Network.* November 2008. Page 15-16.

geospatial mapping services; and direct key agencies, such as the Department of Homeland Security (DHS) and the Department of Defense, to align their infrastructure categorization, classification, and protection activities more consistently with the equivalent private sector activities where appropriate.

- Direct key agencies to conduct risk-based assessments of content and services applications on the criticality of DNS, CAs, and search and geospatial mapping services to mission essential and NS/EP functions, communicate those requirements, and develop the appropriate service level agreements, programs, or market-driven incentives to foster enhanced industry resilience.
- Direct DHS and other key agencies to categorize and prioritize efforts to reflect similar or aligned approaches to risk assessment efforts in the communications and information technology sectors.[4]

Improvements in Contingency Planning:
The Government should improve planning for national contingencies by integrating guidance on global infrastructure facilities into the national policy on the continuity of U.S. Government structures and operations established by National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*. To meet the policy goals of the directive, issue guidance for the development of a national response capability/contingency plan with Government that directs appropriate departments and agencies to develop a contingency plan to sustain critical NS/EP communications during a catastrophic event.[5]

Enhancement of IP Traffic Management Policies:
The Government should establish a policy that requires Federal departments and agencies to: (1) ensure their enterprise networks are properly designed and engineered to handle high traffic volume; (2) manage traffic through quality of service programming in its routers to prioritize traffic, including NS/EP traffic; and (3) expand the use of managed service agreements to provision NS/EP services within the new IP-based environment.[6]

Enhanced Procurement Practices:
The Government is one of the largest single purchasers of software, hardware, and support services and is in the position to influence cybersecurity products and services, and the overall health of networks, by specifying security requirements in their contract mechanisms. Current Federal and State acquisition policies should stipulate cybersecurity requirements in leveraging the use of public funds.[7] Collaboration with stakeholders, including industry, is essential in defining security requirements.

International Coordination:
The Government is also responsible for representing the citizens of the United States in international technical, legal, and diplomatic forums and debates. While the Internet is certainly a shared resource between the public and private sectors, the Government has a unique role in

[4] *NSTAC Report to the President on Physical Assurance of the Core Network*. November 2008. Page 47.
[5] Ibid.
[6] *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic.* August 2008. Page 16.
[7] *NSTAC Report to the President on Physical Assurance of the Core Network*. November 2008. Page 25-26.

diplomacy, international law, and global politics that cannot be delegated to the private sector. It is imperative that the Government engage other countries and become a leader in the international debates over the future of the Internet and its impact on the global economy and global security.[8] International coordination should extend to the diplomatic and international law domains, but also into the coordination of the policies required to support next generational NS/EP capabilities in a globally distributed next generation network (NGN) environment.[9] This is particularly important when the United States is engaged with domestic and international policy and standards entities to develop a more consistent, unified U.S. strategy to enhance current agency activities.[10]

3.0 ORGANIZATIONAL STRUCTURE

What organizational structures are necessary to support national security/emergency preparedness communications needs in a converged environment?

Industry recognizes that protection of cyberspace and its related infrastructures, as well as the sharing of sensitive information, poses unique challenges to the Government. One significant challenge associated with cybersecurity is that an attack occurring at any instance in time may be over before any analysis, response, or mitigation can occur. While information sharing will remain a key tenet of any effective and successful cyberspace defense effort, decision processes now need to occur in milliseconds.[11] The NSTAC has previously examined several issues that need to be addressed in order to accommodate this new trend, including the organizational structures to provide indications, warning, and analysis in collaboration with the private sector and the creation of protocols and standard operating procedures among and between the private sector, Government, and international partners. To further protect the Nation, Federal Government efforts related to cybersecurity should emanate from a single, organizationally and topically-comprehensive governance structure. Such an organizational structure will allow the Government to engage in improved planning and program coordination, increased intergovernmental coordination, and improved interagency coordination of NS/EP communications policy requirements and related activities. Previous NSTAC recommendations in this area are discussed in the sections below.

3.1 Government Indications Warning and Analysis Capability

As the Government examines its role in the common defense of cyberspace, it is critical that the necessary monitoring and early warning capabilities exist, especially against nation state threats. Through the Government's monitoring process of receiving reliable threat data or the development of new capabilities by an adversary, Government must share this information with industry so that all are aware that an adversary is planning an attack and what assets are in

[8] *NSTAC Report to the President on International Communications*, August 2007. Page 12.
[9] *NSTAC Next Generation Networks Task Force Report.* March 2006. Page 29.
[10] NSTAC Next Generation Network Implementation Annex Working Group Letter to the President. November 2008. Page A-3.
[11] *NSTAC Report to the President on the Physical Assurance of the Core Network.* November 2008. Page 46.

danger to ensure that the appropriate resources are available when needed. These efforts will help prevent successful attacks or allow for faster response time to a threat that is still developing. When industry is provided with early warning data, e.g. potential threats, it can institute protective measures to ward off potential damage to infrastructure, therefore limiting the negative effects experienced by customers.

The NSTAC recently recommended that to strengthen the threat and warning architecture, the role of the private sector should be elevated to be both a protected source and recipient of critical and time-sensitive threat information.[12] Specifically, the NSTAC recommended that appropriate "Federal departments and agencies should:

- Prioritize Government efforts to complete the design and build-out of the intended threat warning architecture to include structured, real-time sharing of relevant information between such centers and counterpart facilities in industry.
- Ensure that linkages to private sector entities are included in the architecture, in particular, the "millisecond" critical infrastructure/key resource sectors such as telecommunications, information technology, finance, and power that arguably might have greater need for access to the Government's threat warning architecture.
- Further strengthen the threat and warning architecture by advancing the role of the private sector through—
  - Establishing contracts with [key] specific industry member companies to: (1) implement clearances for responsible individuals to work on protection issues; and (2) receive open source and classified threat briefings, and access to Government secure telecommunications and document storage.
- Sharing information and actionable intelligence with key telecommunications providers in a timely manner to evaluate and prepare for threats and better protect systems."[13]

A warning and analysis function/capability for both industry and Government is critical to protecting cyber communications. Traditionally, this has fallen to intelligence functions working in an organized collaboration with other Government organizations, but other entities, including private sector members and international partners, may be able to contribute to this national capability. Executive leadership, working in concert with both the public, legal, and legislative entities, must collaborate to fashion an environment permitting and safeguarding advanced information sharing and analysis regimes necessary to allow the Government and private sector to secure their communications infrastructure and assets in this critical mission.

Due to the time constraints associated with this tasking, the NSTAC is unable to provide a complete analysis of the characteristics of the necessary capabilities and organizational structures at this time. However, the NSTAC's Cybersecurity Collaboration Task Force (CCTF) has been tasked to examine the formation of a joint, public-private sector, 24/7 cybersecurity capability designed to detect, prevent, mitigate, and respond to cyber threats. The NSTAC Principals have been actively involved in this effort, which is scheduled for completion in advance of the May 21, 2009, NSTAC Meeting. During the meeting, the NSTAC Principals will discuss the

[12] *NSTAC Report to the President on Physical Assurance of the Core Network*. November 2008. Page 46.
[13] Ibid.

findings and recommendations and vote on the *NSTAC Report to the President on Cybersecurity Collaboration*.

3.2 Rationalize Protocols for Greater Integration Among and Between Joint Operations Centers

There are currently several cyber collaboration centers that interact across the Federal Government space to help disseminate information on security threats, including the U.S. Computer Emergency Readiness Team (US-CERT), National Cybersecurity Center, Joint Task Force- Global Network Operations, the National Cyber Investigative Joint Task Force, the Intelligence Community Incident Response Center, the National Security Agency Threat Operations Center, and the Defense Cyber Crime Center. The exact interactions and roles of each, however, remain unclear. In addition, there are numerous private sector collaboration centers, which also need to be considered as part of our defensive strategy.

In recent recommendations, the NSTAC reinforced the need to establish an incident response capability for all key sectors, with supporting mechanisms such as a training academy, exercise program, and a research and development (R&D) program, and recommended undertaking the following enhancements to current agency activities:

- Increase intergovernmental coordination to address incident management, including the development of standard operating procedures and greater interaction between cyber centers, private industry, and international entities, especially on cybersecurity issues.
- Further promote private industry and Government collaboration by establishing a protocol for routine engagement between the US-CERT and information technology and communications industry representatives; add explicit linkages for industry interaction during times of crisis to the standard operating procedures of the National Cyber Response Coordination Group; and involve industry participation in the establishment of the National Cybersecurity Center.
- Investigate the existence of additional technologies, tools, and capabilities available to help strengthen joint Federal, State, local and industry NGN incident response.[14] NS/EP communications services that were developed for use in a voice-only environment, such as the Government Emergency Telecommunications Service and Wireless Priority Service, are becoming less effective with the increased use of data applications in a converged world. The Government should also ensure that tools used to operate in a converged environment are funded at high levels to ensure maximum operating capacity and efficiency. The 2008 NSTAC Priorities Letter to the President reiterated this point.

Again, much of the input associated with the private sector approach to accomplishing these operational goals will be provided as an output to the NSTAC CCTF initiative.

[14] NSTAC Next Generation Network Implementation Annex Working Group Letter to the President. November 2008. Page A-3.

3.3 Expand International Cooperation on Cyber Incident Response and Coordination

Cyber threats to global infrastructures may originate from international sources beyond the jurisdiction of U.S. and allied authorities. These types of threats raise significant concerns about the security and availability of domestic NS/EP communications and the global communications on which many key U.S. functions and economic interests rely. The sophistication and reach of the global communications infrastructure increase the complexity of the threat, whereas the adversary's barrier to entry is low as a result of anonymity, connectivity, and widespread availability of tools for creating disruptions.

The U.S. Government's international NS/EP strategies, policies, and operational response frameworks are not sufficient to keep pace with globalization and technological convergence of public and private sector networks, nor do they adequately include private sector participation in these processes. DHS should coordinate international planning and development with the appropriate Federal agencies for adoption of a global framework incorporating operational protocols and response strategies.[15]

Thus, Federal agencies should expand relationships and response coordination using formal and reciprocal agreements with Allied governments to include participation from selected international service providers and other stakeholders into existing joint U.S. Government and private sector response and coordination processes and entities, such as the US-CERT and the NCC.[16]

3.4 Identity Management Considerations

Identity Management (IdM) of people, software, and other entities is a key underpinning of security for NS/EP communications on the Internet. Moreover, given the breadth of the NGN, interoperability among IdM mechanisms is critical; federation is essential. Government must leverage new and existing technologies in implementing its IdM processes. Federal department and agency support for the prompt development and use of IdM mechanisms, including strong authentication, could accelerate the implementation of more secure systems than currently exist. 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. There is currently no cohesive effort to ensure that NS/EP requirements are addressed in IdM protocols and standards.

The converged networks that make up the Internet provide open access to a broad array of communications, data, and services which interconnect 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 linked directly to the service. Without the ability to identify NS/EP users in the open

[15] *NSTAC Report to the President on International Communications*. August 2007. Page 17.
[16] Ibid.

Internet environment, NS/EP privileges cannot be properly assigned. Strong authentication for users, devices, and processes is a prerequisite for authorizing a user's access level by role or responsibility. Additionally, if NS/EP services are not reserved for authorized personnel, it could impede public and private sector responses to natural disasters, terrorist attacks, or national security threats.

The NSTAC recognizes the importance of IdM issues and is currently examining several IdM topics. Recommendations from the NSTAC Identity Issues Task Force are also scheduled for review by the NSTAC Principals at the May 21, 2009, NSTAC Meeting. These recommendations will address the necessary organizational IdM structures.

3.5 Information Systems Security Board

Advanced technology has offered an enormous benefit to the Nation, however, the convergence of computing and telecommunications has made weak or insecure information systems attractive targets that can be exploited by malicious actors. Vulnerabilities to commercial and military information systems raise significant national security concerns and threaten economic stability due to potential losses of billions of dollars. The state of cybersecurity today reflects the piecemeal, uncoordinated application of a huge variety of standards and practices to varying degrees without careful consideration of the holistic and systemic effects.

In a previous report, the NSTAC proposed an entity intended to improve the state of practice for implementing information systems' security: the Information Systems Security Board (ISSB).[17] The ISSB model may be worthy of reconsideration and update as a joint Government/industry entity given the current cybersecurity environment. The NSTAC stands ready to reexamine the ISSB concept, if requested.

The originally proposed functions of the ISSB were modeled loosely on the Financial Accounting Standards Board and would:

- Evaluate and endorse information systems security standards and develop testing criteria.
- Develop and maintain information systems security principles and guidelines for security environments.
- Develop rating criteria and guidelines for applying them to identify various levels of security tied to varying levels of application or data sensitivity.
- License testing laboratories and auditing organizations to evaluate everything from products and services to complex, enterprise-wide systems for compliance with ISSB criteria and guidelines.
- Issue technical notes to license holders, product developers, and the standards community.
- Establish a process to adjudicate ISSB rules, testing results, and auditing determination appeals.

[17] NSTAC *Information Systems Security Board Concept Paper*. July 1996.

4.0 LEGAL CONSIDERATIONS

What gaps exist in Federal authorities (laws/regulations/policies)?

The following sections offer a brief synopsis of the most pertinent NSTAC recommendations regarding gaps in Federal authorities.

4.1 Need for Federal Communications Commission Action on IP-Based NS/EP Services

In the 2008, the NSTAC recommended that the President petition the Federal Communications Commission (FCC) for a declaratory ruling to confirm that network service providers may lawfully provide IP-based priority access services to authorized NS/EP users.[18]

In 2000, the FCC issued an order establishing that the priority services offered to NS/EP authorized users were *prima facie* lawful under the *Communications Act of 1934,* as amended, and not an unreasonable preference or discrimination in contravention of Section 202(a) of the Act.[19] The authority contained in this FCC precedent must be maintained to ensure networks are capable of providing priority communications for NS/EP authorized users in the future. As IP technology becomes more widespread and plays an increasingly important role in supporting NS/EP services, those services—and the network management techniques that make them possible—must be permitted to evolve in an IP-based environment. For that evolution to occur, the proper legal and regulatory policies must be in place to ensure NS/EP traffic continues to have priority treatment on IP-based networks. Consistent with its ruling that priority access services offered by carriers to NS/EP authorized users are "*prima facie* lawful" under the *Communications Act* and do not constitute "unreasonable discrimination" under section 202 of the Act, the FCC should specifically confirm that the same is true with regard to IP-based priority access services offered by IP-based providers to NS/EP users.

4.2 Improvements to the Regulatory Environment Surrounding Cable Construction

Undersea cable systems are currently subject to a myriad of regulations and rules regarding placement and service. For example, the pre-construction/repair review process can be lengthy, have indeterminate requirements, require monetary compensation to both authorities and commercial fishermen, and subject systems of national importance to the decisions of various Federal, State, local, and county officials. The result is that cable owners may be forced to delay the installation or repair of the cable and to accept less than ideal placement of the cable.

[18] *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic.* November 2008. Page 13.

[19] *In the Matter of The Development of Operational, Technical and Spectrum Requirements For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010; Establishment of Rules and Requirements For Priority Access Service* (WT Docket No. 96-86). 15 FCC Rcd 16720 (2000).

Previous recommendations made to the U.S. Commission on Ocean Policy continue to be relevant today.

In the *NSTAC Report to the President on Physical Assurance of the Core Network*, the NSTAC recommended that the Government should strengthen and improve the regulatory environment for cable construction and licensing by developing a new undersea cable construction regulatory regime potentially modeled after Section VII of the *Natural Gas Act* or the *Deep Water Port Act*, which balances Federal and State interests to facilitate projects of national significance. The goal would be to establish a clearly defined, Federally managed permitting process to avoid current vagaries.[20]

4.3 Ratification of the Law of the Sea Treaty

As captured in the *NSTAC Report to the President on Physical Assurance of the Core Network*, the United States is one of a handful of countries that have signed, but not ratified, the Law of the Sea Convention (formerly known as the United Nations' Convention on the Law of the Sea, or UNCLOS), which entered into force in 1994 and currently has 153 nations as parties.[21] Working in conjunction with industry, the Government must seek ways to streamline Federal rules and regulations pertinent to undersea cable system design, construction, management, and security. Sufficient concerns about the implications for U.S. national security and U.S. environmental policy exist that opponents of UNCLOS assert "…the United States should be wary of acceding to the Law of the Sea Treaty." Such apprehension seems to be the rationale given for the Senate not ratifying the treaty to date. The NSTAC recognizes that there may be concerns that make ratification controversial, but from the point of view of undersea cable facilities, consideration must be given where the infrastructure provides NS/EP services to the Federal Government as an advantage derived from ratification. The Administration and Senate should balance these concerns and re-consider seeking Senate advice and consent to ratify the Treaty.

4.4 Codify the Definition of Essential Service Providers and Modify the *Stafford Act*

The Federal Government recognizes the significance of the telecommunications infrastructure in providing essential communications during and after a natural disaster or terrorist attack.[22] Communication is at the foundation of the Nation's ability to respond to a catastrophic event because the stability of the telecommunications infrastructure helps to ensure the protection and restoration of other infrastructures. Therefore, the NSTAC has repeatedly recommended that the Federal Government include telecommunications repair personnel in the definition of essential service providers (ESP).

[20] *NSTAC Report to the President on the Physical Assurance of the Core Network.* November 2008. Page 49.
[21] Addendum to the *NSTAC Report to the President on Physical Assurance of the Core Network.* February 2009. Page A-1.
[22] *Letter and Report to President George W. Bush on Federal Support to Telecommunications Infrastructure Providers During National Emergencies, Designation as Emergency Responders.* January 2006. Page 1.

In November 2008, the NSTAC Priorities Letter to the President and the *NSTAC Report to the President on Physical Assurance of the Core Network* reiterated this recommendation, calling out specific modifications to the National Response Framework, the National Incident Management System, the *Warning Alert and Response Network Act*, and the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, as amended, to ensure that the definition of ESP is applied uniformly throughout Federal, State, and local governments. The *NSTAC Report to the President on Physical Assurance of the Core Network* also recommended that the President direct DHS, including the Federal Emergency Management Agency, to provide Essential Service Function-2 companies, organizations, and personnel access to the area affected by a crisis or event.

Additionally, the NSTAC recommended that the *Stafford Act* be modified to provide Federal assistance including fuel, billeting, and security during natural disasters and incidents of national significance to help ensure restoration and reconstitution of private sector infrastructure and services in the aftermath of a natural disaster or incident of national significance.[23] Furthermore, in its 2006 *NSTAC Legislative and Regulatory Task Force (LRTF) Report, Federal Support to Telecommunications Infrastructure Providers in National Emergencies Designation as "Emergency Responders (Private Sector),"* the NSTAC recommended that the President:

- Issue appropriate Presidential guidance to define "Emergency Responders (Private Sector)" under the *Stafford Act* and other authorities as appropriate, to align with the broadened definition of "national defense" in the 2003 amendments to the *Defense Production Act (DPA) of 1950*. Specifically, the guidance should make clear that key response personnel of critical telecommunications infrastructure owners and operators should be defined as "Emergency Responders (Private Sector)" and should receive non-monetary Federal assistance under the *Stafford Act*.
- Direct the Secretary of Homeland Security to work with Congress to align the *Stafford Act* and other appropriate legislative authorities with the DPA by codifying the designation of private sector telecommunications infrastructure providers (TIP) as "Emergency Responders (Private Sector)" and by codifying the official interpretation that for-profit TIPs should receive Federal assistance.[24]

4.5 Potential NSTAC / Government Issues for Study

While compiling its response, the NSTAC identified a number of broader policy issues, which may warrant additional exploration as the Administration sets its agenda associated with cybersecurity. An appropriate goal would be to ensure that the legal framework for any cybersecurity initiatives assures adequate provisions for private sector protection, detection, deterrence, prevention, and maintains a clear understanding of international and export laws and the legal platforms through which industry interacts with foreign governments and organizations. The NSTAC stands ready to assist the Administration as it explores the appropriate policies and

[23] *Letter and Report to President George W. Bush on Federal Support to Telecommunications Infrastructure Providers During National Emergencies, Designation as Emergency Responders.* January 2006. Page 15.
[24] Ibid.

changes to our legal and regulatory framework, both domestic and international, to help the public and private sectors address the growing cyber threat.

The major areas that may need additional gap analysis are addressed below.

Potential New Roles for Government:
The Government may consider acquiring new roles not currently implemented or previously defined to deal with cyber threats. As the Administration considers its' next steps, NSTAC is prepared to counsel and advise of any impediments or further considerations associated with those undertakings.

Review of Foundational Law:
A significant issue regarding Federal cyber law is the legal regime is too complex. Federal Governmental agencies regularly seek to obtain information from private entities in order to execute what they perceive as their duties to gain visibility into what is happening in cyberspace, and, where appropriate, to conduct cyber operations. Numerous Federal, State and foreign laws, however, regulate the exchange of such information—both content and metadata—with governmental entities. These laws include Title III of the *Omnibus Crime Control and Safe Streets Act* of 1968, the *Electronic Communications Privacy Act* of 1986 (which includes the Stored Communications Act and the Pen Register Statute), and the *Foreign Intelligence Surveillance (FISA) Act of 1978*, as amended by the *FISA Amendments Act of 2008*. State laws also govern the disclosure of such information with the Government (as well as consumer disclosure rules) and are far from uniform in application. For private entities that operate overseas, they must ensure that they also comply with the laws of applicable foreign jurisdictions.

These laws overlap in significant ways, are exceedingly complex, employ vague and outdated terms and concepts, and, in some instances, do not adequately protect the legitimate privacy interests of communicants. Moreover, in many instances, they provide for criminal and/or civil sanctions for violations of their terms. This legal regime is flawed because it may cause Government and private entities to hesitate to act unnecessarily because they cannot be certain of how the law should be applied, and, for the same reason, they may inadvertently violate legal prohibitions.

In addition, current law is ineffective in countering the rapidly evolving nature of cyber threats, such as BOTNETS. The passage of cyber crime legislation, *Identity Theft Enforcement and Restitution Act of 2008*[25], last year was a significant step forward on the prosecution side of this issue. However, other legal reform measures, including liability protections, should be examined to support actions taken by service providers and vendors to thwart network attacks.

As the Administration moves forwards with its' cybersecurity initiatives, it may be prudent to establish a working group of experts from the Government, the business sector, and civil liberties

[25] Title II of P.L. 110-326, *To amend Title 18, United States Code, to provide secret service protection to former Vice Presidents, and for other purposes*. Signed September 26, 2008

and privacy advocates to immediately review the legal regime that governs cyber space in the United States, and recommend legislative changes to simplify and modernize federal cyber law.

Governance During Times of National Crisis:
With a shared infrastructure, decision-making authority, attribution and response, and reconstitution roles are unclear. Command and Control for National Security Missions is essential to ensure priority is given to missions which need the network most. During times of National Crisis, the U.S. Government will influence key decisions regarding the security and stability of shared Information Infrastructures, including governance, authentication, technological innovation, standards, mitigations, and operational issues. We must improve awareness of shared risk, consequence, dependencies, and cascade effects; and National level impacts of risk management tradeoff decisions related to National security missions. The outcome is clear guidance and an enhanced ability to rapidly execute National level decisions for response options to sophisticated attack against our shared information infrastructure resulting in loss of mission assurance.

Gaps in Cyber Incident and Response Policies:
In the aftermath of the 2007 distributed denial-of-service attacks against Estonian government networks, the NSTAC's LRTF explored questions regarding the impact of cyber incidents and conflicts on private sector critical infrastructure owners and operators. The LRTF found that there did not appear to be a single Government entity with the authority to differentiate between different types of cyber threats and the necessary response (i.e., law enforcement or national security).

5.0 PRIORITY NSTAC RECOMMENDATIONS

Based on your experience and expertise and your previous recommendations in this area, please provide us with a prioritized list of ten areas that require immediate attention.

While there are literally hundreds of prior NSTAC recommendations addressing the topics contained in this response, it is possible to identify themes and clusters that have been refined over time as process, policy, and technology have developed. Taken together, these form a basis for holistically depicting NS/EP. Through that understanding, one may elicit high-level needs and priorities across the entire NS/EP system.

Each of the eight stated recommendations below combines multiple recommendations from various NSTAC reports and studies. At the same time, each stated priority recommendation includes a list of references to previous work, where related requirements are described and developed in greater detail.[26]

[26] The nomenclature used to denote Priority NSTAC Recommendations follows the format used by Office of the Manager, National Communications System, detailing the NSTAC task force, year of approval, and recommendation number as it is presented in the report. The following list details the NSTAC work referenced in this document:
CATF: *NSTAC Report to the President on Physical Assurance of the Core Network*

The following chart graphically depicts the organizing principle around which the recommended needs, numbered in priority order, are structured. The entire cybersecurity system is bedded in needed Federal organizational initiatives to optimally approach the full scope of cybersecurity within Government purview. As such, Federal organization is the highest-priority cybersecurity need and is foundational to making meaningful progress on all other identified priorities. After that, the four highest-priority needs are characterized as "universal issues", specifically information sharing, identity management, standards and legal/policy considerations. These are deemed to be foundational to practically all other NS/EP considerations, and by their nature, cut across topically-specific efforts throughout cybersecurity. Remaining "topically-specific" activities are defined by their emphasis, namely technology, work processes, international organization and international diplomacy.

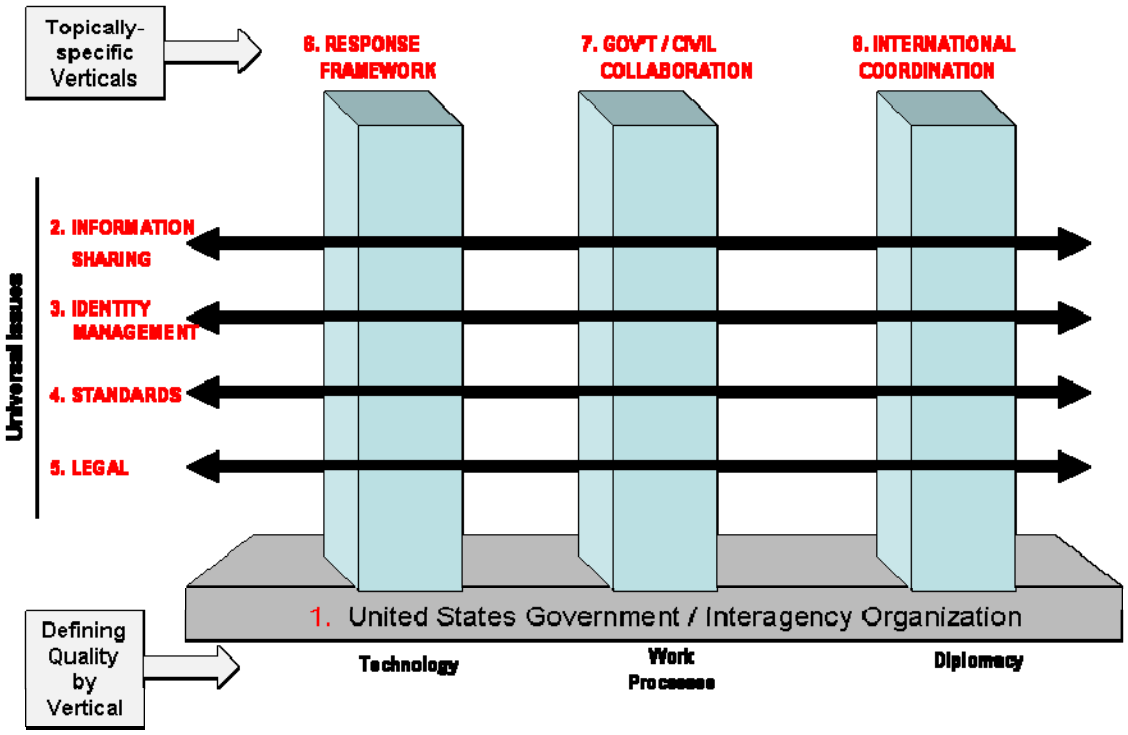

Figure 1. Depiction of Priority Recommendations

CATF Addendum = Addendum to the *NSTAC Report to the President on Physical Assurance of the Core Network*
ECITF = Emergency Communications and Interoperability Task Force Letter to the President
GIRWG-2006 = *NSTAC Report to the President on Global Infrastructure Resiliency*
GIRTF-IP = *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*
ITF = *NSTAC Report to the President on International Communications*
NCCTF = *NSTAC Report to the President on the National Coordinating Center*
NGN-2005 = *Next Generation Networks Task Force Near Term Recommendations Working Group Report*
NGN-2006 = *NSTAC Next Generation Task Force Report*
NGN IAWG = NSTAC Next Generation Network Implementation Annex Working Group Letter to the President
NOTF = NSTAC Outreach Task Force Letter to the President
TATF = *NSTAC Trusted Access Task Force: Screening, Credentialing, and Perimeter Access Controls Report*
TEPITF = *NSTAC Report to the President on Telecommunications and Electric Power Interdependencies: The Implications of Long-Term Outages*

5.1 United States Government / Interagency Organization

Recommendation:
Integrate Federal cybersecurity activities under a single, central, organizationally and topically-comprehensive governance structure. This will permit improved planning and program coordination, increased intergovernmental coordination to address cyber incident management, and improved interagency coordination of NS/EP communications policy requirements and activities across the Federal Government.

Background:
The National Strategy to Secure Cyberspace charges the Department of State (DOS) to enhance cooperation among international parties. In this capacity, DOS collaborates with other agencies, including DHS and the Department of Justice, to increase international cybersecurity cooperation by working with existing international organizations to establish a "culture of security." As set out in Homeland Security Presidential Directives 5 and 7, DHS retains much of the responsibility for U.S. Government policy direction in network security. Within DHS, the National Communications System and National Cybersecurity Division are involved in U.S. Government efforts on international NS/EP in the communications and information technology sectors.

Numerous departments and agencies are actively addressing NGN transition issues. 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, the new terms and concepts that different groups are currently developing must be harmonized to preserve clarity of meaning and consistency of policy and program execution.

References:

- R&D Coordination: NGN-2006-3
- Interagency Coordination: NGN IAWG-2008-8
- Fund Priority Programs: NOTF-2008-1; ECITF-2006-1; NGN IAWG-2008-7
- Inter-Governmental SOPs: GIRTF-IP-2008-1; ITF-2007-1; NGN-2005-8
- Inter-Governmental Discussions on NS/EP: NGN-2006-8
- Communications Policy: NGN IAWG-2008-6

5.2 Information Sharing

Recommendation:
Create structures for timely and secure sharing of cybersecurity threat and response information between government and industry, and between/among critical infrastructure sectors in a trusted collaborative environment.

Background:
The interconnected and interdependent nature of networks has fostered crucial information sharing and cooperative response and recovery relationships among global service providers and infrastructure sectors. These are needed to counter ever increasing cyber threats. 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.

Concern often arises about sharing proprietary data between and among private sector companies and the Federal Government. If industry and Government can agree on the data structures and tools for portraying the situation, a unified picture may emerge while protecting underlying proprietary data.

References:

- Information Sharing: GIRTF-2008-1; GIRTF-2008-2; CATF-2008-3; NCCTF-2006-4; TEPITF-2006-4; TEPITF-2008-2; NGN IAWG-2008-8; ECITF-2006-1; NCCTF-2006-1; NCCTF-2006-4; NGN IAWG-2008-7; NGN IAWG-2008-8
- Millisecond Sectors (Communications, IT, Finance, Power): CATF-2008-3
- Company-Company and Government-Industry Information Sharing: NCCTF-2006-1
- Information Sharing at the Local / Regional Level: TEPITF-2006-4
- NSTAC Status Report on National Coordinating Center Roadmap for the Future 2007

5.3 Identity Management

Recommendation:
In partnership with the private sector, create a secure, responsive, and extensible Identity management (IdM) framework to support cyber-based identity processes and applications and ensure emergency response access to critical infrastructure in support of disaster recovery.

Background:
IdM is a key underpinning of security for NS/EP communications on the Internet. Moreover, given the breadth of the NGN, interoperability among IdM mechanisms is critical; federation is essential. Government must leverage new and existing technologies in implementing its IdM processes. Federal department and agency support for the prompt development and use of IdM mechanisms, including strong authentication, could accelerate the implementation of more secure systems than currently exist. Coordinated agency efforts would also 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. There is currently no cohesive effort to ensure that NS/EP requirements are addressed in identity management protocols and standards.

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 linked directly to the

service. Without the ability to identify NS/EP providers and users in the open NGN environment, NS/EP privileges cannot be properly assigned. Strong authentication for users, devices, and processes is a prerequisite for authorizing a user's access level by role or responsibility. Additionally, if NS/EP services are not reserved for authorized personnel, it could impede Federal and private sector responses to natural disasters, terrorist attacks, or national security threats.

References:

- IdM: NGN IAWG-2008-1; ITF-2007-1; ITF-2007-2; NGN-2006-1-C
- IdM Mechanisms-Strong Authentication: NGN-2005-4

5.4 Standards

Recommendation:
Encourage broad participation and place increased emphasis on U.S. representation in technology standards activity, embracing federal and commercial collaboration in pursuit of national objectives. Consolidate Federal leadership and oversight of NS/EP related efforts.

Background:
The United States has an opportunity to influence the work of global standards bodies by actively participating in and leading the standards development process. At a time of increased global attention to the standard-setting process, it is important that the United States commit appropriate resources to maintain a leadership position. NS/EP requirements must be considered in traditional telecommunications and networking standards bodies, but also in nontraditional standards activities addressing IdM and Web services. Industry and Government are only beginning to address these issues.

Unlike the NS/EP capabilities of legacy networks, which were built on an existing framework, the NS/EP capabilities of the NGN are developing simultaneously. With convergence, and the enhanced NS/EP services that the NGN will provide, additional standards will be critically important. Global standards bodies are also currently addressing NS/EP IP-based priority services delivery. Active participation here will help ensure the United States has the opportunity to affect the global adoption and implementation of standards that will drive the long-term effects on IP-based prioritization.

References:

- Actively Participate: GIRTF-IP-2008-2
- Agreements, Standards, Policies, and Regulations (ASPR): NGN-2006-6
- Coordinate Across Standards Bodies: NGN-2005-7; NGN IAWG-2008-6
- Improve Interagency Coordination Cooperative Mechanisms of Standards Bodies: NGN IAWG-2008-9-A
- Standard Operating Procedures: NGN IAWG-2008-7-A
- Standardized Screening Processes: TATF-2005-1

5.5 Legal

Recommendation:
Pursue legal and regulatory initiatives as outlined in NSTAC response to Section 4.0, "gaps in federal authorities".

Background:
Global communications infrastructure policy and authority are distributed across numerous Government agencies. The Government has yet to determine many of the legal requirements to protect the Nation's critical infrastructure from cyber threats. Cyber threats to global infrastructures may originate from international sources beyond the jurisdiction of U.S. and allied authorities.

Regionally-diverse legal and policy frameworks may inhibit the adoption of uniform security practices internationally. Also, different legal, regulatory, and social policies implemented with the intent of protecting societal expectations regarding privacy and other rights and privileges of local citizens may affect certain aspects of security. Private industry ownership and control of the majority of critical network assets means that "policy" is in many instances derived not from Government, but from private practices and arrangements among owners and operators. Significant gaps exist between the policies that govern and the mechanisms that enable international incident response and information sharing in the converging global network.

References:

- Examine Industry Laws / Policies: ITF-2007-1-D
- Regulatory: CATF-2008-7
- Legal Agreements: CATF-2008-1, CATF Addendum

5.6 Response Framework

Recommendation:
In collaboration with industry, create a comprehensive incident-response architecture embracing critical infrastructure facilities and core infrastructure services, including at least the "millisecond sectors" of civil industry (Communications, Information Technology, Finance, and Power).

Background:
Unlike management of physical threats and incidents, the Nation's approach for the management of cyberspace domain has been more improvisational, as it is associated with limited common terminology, few standard processes, and few established guidelines on how a situation should be handled. Cyber NS/EP incident management has traditionally existed in the realm of a physical event and a process is in place to manage those events, including how they affect wireline and wireless communications. However, the convergence of telecommunications networks in the NGN environment includes numerous new technologies and new industry players who control key network elements but who may not have relationships in place with

industry and Government incident managers. Additionally, the network itself is becoming increasingly complex and global in nature, pushing incident management out beyond the realm of the territorial United States.

A mechanism for coordinating among all key sectors, in particular, the "millisecond" critical infrastructure/key resources sectors such as telecommunications, information technology, finance, and power, must be in place to address the needs of the new cyber environment. Incident response, including planning for response, requires a joint industry/Government effort to improve communications and establish an inclusive and effective response capability.

References:

- Incident Response Coordination: NGN-2006-7
- Response Architecture Needed: NGN IAWG-2008-7
- Incident Management – Coordination: NGN IAWG-2008-7
- Embrace Critical Services within Protected Critical Infrastructure: CATF-2008-1; CATF-2008-2; CATF-2008-4
- Millisecond Sectors (Communications, IT, Finance, Power): CATF-2008-3
- Information / Technical Coordination: NCCTF-2006-2

5.7 Government / Industry Collaboration

Recommendation:
Collaborate with industry on research and development (R&D) efforts in pursuit of critical cybersecurity capabilities, and in furtherance of interoperable identity management processes between government and society.

Background:
The challenges posed by emergent cybersecurity threats demand increased investment in new research into advanced network monitoring, detection, decision making, and response capabilities. Government-sponsored research would provide a catalyst 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.

Government should ensure that its IdM mechanisms can be federated with those of the commercial sector, international networks, and across the Federal Government. Coordinated Federal agency efforts and public-private partnerships could dramatically improve IdM on the NGN. Government use of commercial IdM 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.

References:

- IdM Framework: NGN IAWG-2008-1

- Cyber Response Strategy: NCCTF-2006-6
- Government Industry Collaboration: NGN IAWG-2008-7
- Leverage Sector Expertise: ITF-2007-1
- Joint Government / Industry Incentive: NGN-2006-2
- R&D Coordination: NGN-2006-3; NGN IAWG-2008-3
- Expand the NCC: NCCTF-2006-3; NCCTF-2006-4

5.8 International Coordination

Recommendation:
Pursue development of international cyber-incident warning and response capabilities, sharing relevant information.

Background:
The expanding global interconnection of networks and the fact that foreign providers own and operate many of the networks adds new complexity for all those involved in assuring that the NS/EP telecommunications needs of the U.S. Federal Government are met. Cooperation among various foreign Governments and between the U.S. Government and industry is required to avoid, prepare for, mitigate, and recover from a catastrophic event in an evolving threat environment.

Network attacks or incidents originating outside the territorial United States raise increasing concerns about the security and availability of domestic NS/EP communications and underscores the need for an effective international capability that can respond to the disruptions affecting global networks. However, international coordination on incident response remains ad hoc and many issues remain, including how to handle incident response in a converged environment. The continuing absence of a coordinated, scalable, international structure for response that includes all relevant stakeholders undercuts efforts to develop systemic solutions and responses to ensure NS/EP communications on the global communications infrastructure.

References:
- Policy Coordination: NGN-2006-6; NGN-2006-8; NGN IAWG-2008-6
- Cyber Response Collaboration: NGN IAWG-2008-9
- Sharing Information: NCCTF-2006-6; GIRWG-2006-4
- Interoperability: ITF-2007-1-A; ITF-2007-1-B; NGN IAWG-2008-8; GIRWG-2006-4; ITF-2007-1