2007–2008 NSTAC Reports

"NSTAC: Enhancing National Security and Emergency Preparedness through Communications"

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

2007–2008 NSTAC Reports

June 2008

Table of Contents

2008 NSTAC Cycle Combined Reports

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on International Communications

August 16, 2007

Table of Contents

Executive Summary

As society moves into the 21st century, globalization1 is taking place at an increasing rate. This trend is engaging a much richer spectrum of countries as interdependent producer-partners supply the products and services needed to fuel economic growth. Among the most important enabler of this global economic growth is the communications network, which the owners and operators of the Public Network (PN) supply and maintain. This internationally connected global communications infrastructure[2]—a grid of voice, video, and data services, devices, and networks—is fueling the rapid growth of international products and services.

The daily internal operations of nation-states are also dependent on reliable services across the global communication infrastructure. In this sense, each nation-state has interests similar to functions that U.S. national security and emergency preparedness (NS/EP) programs perform. As international economies grow, those nation-states that enable and enforce stable, legal frameworks become more important on a global economic level.

Global communications depend on a reliable and sustainable global infrastructure operating across national borders in the face of natural disasters and man-made threats. On a national scale, large regional disruptions such as the September 11, 2001, attacks and Hurricane Katrina, were addressed through existing government and industry partner frameworks. On an international scale, however, large, natural, and man-made threats pose new and more insidious potential for business and government disruptions exacerbated by the absence of broadly endorsed collaboration and response international frameworks.

During the period of this President's National Security Telecommunications Advisory Committee (NSTAC) study, two significant regionalized communications outages have occurred, affecting the global communications infrastructure. On December 26, 2006, a 7.1-magnitude earthquake struck off Taiwan's southern coast, damaging undersea fiber-optic telephone cables and severely disrupting telecommunications in a wide area. Taiwan's largest telephone company, Chunghwa Telecom Company, reported that the damage disrupted 98 percent of Taiwan's communications with Malaysia, Singapore, Thailand, and Hong Kong.[3] The extensive infrastructure damage that this earthquake caused resulted in communications disruptions for several weeks while the undersea cables were being repaired.

More recently, the Baltic nation of Estonia battled what has been characterized by the press as a full-scale cyber attack that started on April 27, 2007. As denial-of-service attack protocols flooded Estonian government and private computer systems with up to a million times more data than normal, Estonian officials had to cut off or limit Internet traffic originating from international locations. Estonia, which has been a full member of the North Atlantic Treaty Organization (NATO) since 2002, requested assistance from NATO member countries. As NATO and U.S. cyber experts rushed to support Estonia, the international community witnessed many known forms of cyber attack.[4]

Such significant natural and man-made threats discussed herein, coupled with an increase in global interdependency, further underscore the worldwide reliance on the global communications infrastructure. Prior to the occurrence of the two events noted above, the NSTAC initiated this examination of the current international NS/EP communications environment to—

- Evaluate the present U.S. operational strategies, policies, and frameworks for international collaboration; and
- Prepare recommendations to the President to promote U.S. NS/EP interests in emerging international network security efforts.

In conducting this examination, NSTAC received documents, reports, and briefings from industry and Government that covered a wide range of topics from subject matter experts (SME) in policy development, international relations, operational control (such as cyber incident response), standards and protocol development, intelligence, and internationally significant infrastructure. In addition, representatives from several U.S. Government agencies, including Department of

Homeland Security (DHS), Department of Defense, and Department of State, offered input throughout the development of this report. Of particular value was the participation of senior government representatives from relevant Canadian and U.K. government agencies.

As part of this study, the NSTAC reviewed international network infrastructure incident response policies and legal frameworks that define or influence how U.S. infrastructure operators interact with foreign governments or foreign operators. The NSTAC developed an inventory of instruments that make up this framework to better describe the current policy environment. This inventory, which has been updated throughout the course of this inquiry, is included as Appendix D.

Findings

- The *rapidly evolving* global communications infrastructure is increasingly interconnected through a system of systems that provides global services and connectivity. A global workforce, including those in non-allied nations, operates and maintains the infrastructure.

- As a result of globalization, the U.S. NS/EP communities, government operations, allies, many key businesses, and their global business partners are *increasingly dependent* on the availability of global communications and related services.

- Cross-sector dependencies and interdependencies (such as between telecommunications and electric power) create additional complexities, amplifying the difficulties of mitigation and effective repair when broad-scale disruptions occur.

- Cyber threats to global infrastructures may originate from international sources *beyond the jurisdiction* of U.S. and allied authorities.

  - Attacks originating *outside* the territorial United States raise increasing 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 PNs and private sector networks, nor do they adequately include private sector participation in these processes.

Recommendations

Recognizing NS/EP communications' evolving dependence on and interdependence with global infrastructures and to enhance the resiliency of the global communications infrastructure, the NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the following:

- Task DHS to coordinate international planning and development with the appropriate Federal Agencies for adoption of a global framework incorporating operational protocols and response strategies. The framework must accomplish the following:

  - Address physical and cyber events that would disrupt the availability of critical global infrastructure services.

  - Ensure private sector participation in developing the framework to leverage extensive expertise and existing relationships.

  - Support the use of identity management solutions that address NS/EP requirements for normal operations and all-hazards crisis response.

  - Examine, with the help of private sector partners, existing U.S. laws and policies that could prevent service providers and other stakeholders from

taking the necessary proactive measures to restore service and prevent harm to NS/EP users for government essential operations during a crisis.

- In the interim, *task Federal Agencies to 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 U.S. Computer Emergency Readiness Team and the National Coordinating Center.

1 Introduction

1.1 Background

The U.S. communications infrastructure, once controlled by industry stewards with close Government relationships, is now dispersed throughout numerous companies and organizations spanning the information and communications technology (ICT)[5] industries. This global communications infrastructure,[6] a term characterizing the global Internet Protocol (IP)-based converging networks and devices that enable voice, video, data, and other broadband and mobile multimedia services, is quickly supplanting the traditional Public Switched Telecommunications Network (PSTN). This technological convergence is being mirrored by a period of policy convergence, requiring adjustments in existing government and industry approaches to the environment in which these networks and dependent services operate. At the same time, foreign management and ownership of portions of the global communications infrastructure is increasing.[7] Policies and organizational mechanisms that address security risks and incident management in the global network community are essential components to addressing these challenges. As this technological and policy convergence continues, the U.S. communications infrastructure faces several issues and concerns that will uniquely affect national security and emergency preparedness (NS/EP)[8] communications.

Communications now transit international borders without hindrance, as the Public Network (PN) becomes increasingly interconnected with networks worldwide, moving toward the ad hoc development of a global, seamless network. This global interconnectivity brings with it inherent risks: information passes over parts of the network within and outside the United States diverse in security, architecture, and management. This is particularly an issue in some foreign network segments and infrastructures, which may be more vulnerable to intrusion, deliberate disruption, or accidental damage. With this converged global network, additional operational security concerns related to access and remediation following system disruption have emerged.

Previous reports have recommended that the President's National Security Telecommunications Advisory Committee (NSTAC) expand its attention beyond domestic issues to encompass international matters to continue the protection and promotion of NS/EP communications with industry/government collaboration.[9]

1.2 Charge

As a result of international NS/EP communications concerns voiced at the NSTAC XXIX Meeting, the NSTAC began the examination of current international incident management and operational protocols in addition to the policy frameworks related to the use of NS/EP services over the global communications infrastructure. These policy and operational issue areas are particularly critical in light of the following:

- Expanding U.S. Government-initiated collaboration with key allies and global trading partners;
- International nature of the network, provider, and threat environment surrounding cyber incidents; and
- Increasing threat to and dependency on internationally significant infrastructure operated by various foreign entities.

The objectives of this NSTAC report are as follows:

- Evaluate the present U.S. operational strategies, policies, and frameworks for international collaboration; and
- Prepare recommendations to the President to promote U.S. NS/EP interests in emerging international network security efforts.

1.3 Process

The NSTAC received briefings and material from industry and Government subject matter experts (SME) in policy development, international relations, operational control (such as cyber incident response), standards and protocol development, intelligence, and internationally significant infrastructure. Briefings covered wide-ranging topics, including the Department of Homeland Security (DHS) National Communications System's

(NCS) and National Cyber Security Division's (NCSD) international activities; the Department of State's (DOS) international communications coordination activities; the private sector role within military-to-military relationships; the present interagency, DHS, and Department of Defense (DOD) NS/EP engagements and other direct NS/EP engagements with foreign governments; and the U.S.-Canadian telecommunications and electric power bilateral relationship.[10] In addition to reviewing these specific briefings, representatives from several U.S. Government agencies, including DHS, DOD, and DOS, participated in the development of this report. Of particular value was the significant, continuing participation of senior government representatives from relevant Canadian and U.K. government security agencies.[11]

As part of this study, the NSTAC reviewed international network infrastructure incident response policies and legal frameworks that define or influence how U.S. infrastructure operators interact with foreign governments or foreign operators. The NSTAC developed an inventory of instruments that make up this framework to better describe the policy environment; this inventory has been updated throughout the course of this inquiry.[12]

2 NS/EP Communications, the NGN, and the Threat Environment

This section describes the evolving NS/EP communications threat environment over the global communications infrastructure, including the NGN and provides reference to the range of definitions and analyses of NS/EP and the NGN for this report.[13]

2.1 NS/EP Communications

Historically, the "national security" component of NS/EP communications drew on the communications industry's support of warfighting, intelligence-gathering, and other national security/intelligence community missions. Likewise, the "emergency preparedness" component of NS/EP was understood to incorporate recovery from domestic natural disasters such as hurricanes and earthquakes.[14] More recently, with the advances in technology and ever more global connectivity, man-made physical and cyber threats to the communication networks come from ever wider communities and threat vectors; those exercising terrorism of the sort evidenced during the September 11, 2001, attacks as an instrument of international policy are also likely to join in these efforts.[15] Similarly, the ICT sector's emergency disaster response is no longer limited to domestic incidents. Consequently, U.S. interests charged with supporting NS/EP communications services now must be able to deploy those services globally.

The concept of national security has evolved through numerous institutional redefinitions in recent years.[16] The NSTAC has acknowledged an expanding view of national security as it affects global communications infrastructure network security and availability in several reports, including the NSTAC *Financial Services Report and Report to the President on Next Generation Networks.* The NSTAC continues to examine relevant NS/EP terminology.[17]

2.2 The NGN

The term NGN has often been used interchangeably with "converging networks." However, the NSTAC previously described the NGN as an evolving concept, from a rhetorical and technological perspective, as follows:[18]

> The NGN will logically consist of applications that deliver services, the services provided to users, and the underlying transport networks. … The NGN itself is a capability that will enable many services and applications. Some services will be provided by the network and some will be external to it, but depend upon it. NGN user-centric services will be delivered over various networks, some of which, like private customer premises networks and mesh networks, lie outside the wide scope of the PN.
>
> ***However, there is no single, universally accepted definition of the NGN. … The term NGN is not intended to represent any single configuration or architecture. Instead, it represents the set of converged networks*** [emphasis added]… expected to arise that will transparently carry many types of data and communications and allow delivery of services

> and applications that are not coupled to the underlying network. However, it is possible to note several key NGN elements or attributes over which there is little, if any, dispute.[19]

In this report, the term "global communications infrastructure" is used rather than "NGN" to emphasize breadth of coverage of these networks and to facilitate understanding by the reader, who may have a particular definition or architecture in mind for the NGN.

2.3 The Threat Environment

The NSTAC acknowledges that network incident response is an integral part of overall incident response practices.[20] The NSTAC also recognizes the potential gravity of cyber-based impacts on other critical infrastructures and agrees that these critical infrastructure (CI) interdependencies,[21] which the NSTAC has previously addressed at the domestic level, should be addressed at the international level in an integrated manner.

The global communications infrastructure consists of "physical" components such as switches, storage devices, and transmission mediums (cable and satellite), and "logical" components including control software, protocols, and applications. Threats and disruptions to the NS/EP communications infrastructure can be man-made (whether intentional or accidental) or natural and affect physical and logical elements.[22] The approach to operational response must therefore be all hazards, capable of responding to physical, logical, and blended impairments. There is cause for concern that infrastructure attacks in the future may be perpetrated to a greater extent by nation states and organized terrorists who have developed intensive military computer attack capabilities and who target U.S. economic interests, as well as critical infrastructure, private industry assets, and national security. It is therefore no coincidence that communications assets are among the first targets hit in military engagements.[23]

Recent natural and man-made events highlight the international implications for NS/EP.

On December 26, 2006, a magnitude 7.1 earthquake struck off Taiwan's southern coast, damaging undersea fiber-optic telephone cables and severely disrupting telecommunications in a wide area. Taiwan's largest telephone company, Chunghwa Telecom Company, reported that the damage disrupted 98 percent of Taiwan's communications with Malaysia, Singapore, Thailand, and Hong Kong.[24] Although the undersea cables required several weeks of repair resulting in extensive infrastructure damage, the duration of communications disruptions were minimized as traffic was rerouted as a result of international industry cooperation.

The Baltic nation of Estonia battled what has been characterized as a full-scale cyber war that started on April 27, 2007. As denial-of-service attack protocols flooded Estonian government and private computer systems with up to a million times more data than normal, Estonian officials had to cut off or limit Internet traffic originating from international locations. Estonia has been a full member of the North Atlantic Treaty Organization (NATO) since 2002, and requested assistance from NATO[25] member countries. As NATO and U.S. cyber experts rushed to support Estonia, the international community witnessed many known forms of cyber attack.[26]

Although these incidents demonstrate the effectiveness of existing industry cooperation mechanisms, they also illustrate the increasing need for international coordination to respond to incidents because the scope and magnitude of future threats remains unknown. Network attacks or incidents originating outside the territorial United States raise increasing concerns about the security and availability of domestic NS/EP communications, and an effective response requires improvements in international collaboration. Recent publicly reported international attacks on U.S. government agencies—from Moonlight Maze through Titan Rain[27]—illustrate the changing threat environment and the need for international response. Such attacks require the development of network defense strategies that are costly and continuous. U.S. industry members responsible for operating in such environments and investing in appropriate defenses globally will benefit from consistent and reliable policy approaches

designed to address an international framework for network security. The global community will in turn benefit from an available, reliable, and defensible information infrastructure.

The international community's current approach to network security, institutional interdependencies, and risk varies widely. This variance in approach is also true with respect to incident response mechanisms. U.S. industry is inherently international—NSTAC member companies have international operations and work with foreign governments and multinational companies on key issues affecting NS/EP communications. These companies have well-developed incident response processes, as do many governments and national or regional response organizations such as computer security incident response teams (CERT). Much international coordination on incident response remains ad hoc, however. It is difficult to predict with certainty whether the collection of incident response mechanisms in place will be sufficient if a serious international incident occurs, especially as the time available to respond continues to decrease. 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.

3 Policy Issues

3.1 Legal/Policy Framework and Analytic Process

One component of the NSTAC charge for this study was a review of the elements of the existing legal framework and international policies that direct or affect the way private-sector entities interact with foreign governments or foreign critical infrastructure operators. The existing legal framework examined consisted of treaties, conventions, bilateral dialogues, Mutual Recognition Agreements, Federal Trade Agreements, memoranda of operations, national plans, and other legal instruments.[28] The NSTAC determined that significant gaps exist between the policies that govern and mechanisms that enable international incident response and information sharing and the reality of the threat environment and converging global network. The review also revealed that an increasing level of effort among governments, non-governmental organizations, standards bodies, and industry groups outside the United States is directed at the same set of concerns regarding government and industry capacity and collaboration to prevent, report, respond, and recover from insults to the global information network complex.[29]

Global communications infrastructure policy has no single locus of responsibility in the United States; instead, it is distributed across numerous government agencies. Moreover, 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.

Our review of existing worldwide policy documents indicates that the international community has already begun to address the need for increased international cooperation. As with our own policy assertions, several documents outline frameworks for improved international coordination. *The National Strategy to Secure Cyberspace* charges DOS to enhance cooperation among international parties. In this capacity, DOS collaborates with other agencies, including DHS and the Department of Justice (DOJ), to increase international cyberspace security cooperation by working with existing international organizations to establish a "culture of security." According to *The National Strategy to Secure Cyberspace*, DOS will lead Federal efforts to enhance international cyberspace security cooperation. Initiatives are as follows: (1) develop secure networks in tandem with international partners and private industry owners and operators; (2) secure North American cyberspace by working closely with Mexico and Canada; (3) further secure interdependent sectors by reviewing common networks affecting sectors such as telecommunications, energy, and finance; (4) encourage international partners and organizations to develop watch and warning systems; and (5) promote laws and procedures outlined in the Council of Europe Convention on Cybercrime.[30]

The National Response Plan (NRP), in the "International Coordination Support Annex," [31] provides further detail on DOS' role in supporting international preparedness,

protection, and mitigation efforts related to cyber critical infrastructure protection (CIP), and works particularly closely with DHS and other Federal Agencies on physical and cyber-CIP efforts. In addition, DOS works on behalf of the U.S. Government to facilitate "communication with foreign governments and multilateral organizations that can assist and/or support immediate attribution/mitigation efforts." This effort is occurring in conjunction with Emergency Support Function (ESF) #2. ESF#2 is outlined in the NRP as being responsible for (1) coordination with telecommunications industry; (2) restoration and repair of telecommunications infrastructure; and (3) protection, restoration, and sustainment of national cyber and information technology (IT) resources.

The NSTAC's Next Generation Networks Task Force Report determined that "identity management is a crucial underpinning of NS/EP communications over the global communications infrastructure, which is likely to provide open access to a broad array of communications, data, and services, and interconnect an increasing number of users, processes, and devices."[32] Further, the NGN Task Force Report recommended that "the President should direct the Office of Management and Budget, the Department of Commerce (DOC), and DHS to work with the private sector in partnership to develop a federated, interoperable, survivable, and effective identity management framework for the NGN…"[33] It also recommended that the President "direct DHS, the Department of State, and DOC (including National Institute of Standards and Technology and the National Telecommunications and Information Administration) to engage actively with and coordinate among appropriate domestic and international entities to ensure that relevant policy frameworks support NGN NS/EP capabilities."[34] Clearly, given the need for globally accepted solutions in the NGN, identity management is just as crucial for NS/EP in frameworks developed for the international environment as it is at the national level.

From the analysis of the global communications policy environment, several principles emerged:

- There is a growing consensus that adequate cyber defense can occur only through international cooperation.

- The modern world cannot effectively operate without a global communications network; therefore, a major interruption of such a network is inherently an NS/EP issue.

- U.S. national, homeland, and economic security, supported by NS/EP communications, is dependent on the inviolable continuity of service of a network that has become irrevocably international.

- Cooperative information exchange between countries and service providers is essential, and trusted relationships need to be established through diverse mechanisms.

- Government-to-government interaction is, in practice, the rare exception in global communications incident response, rather than the rule; it typically occurs in only the most serious of situations. If response escalation beyond preexisting lower level standard operating procedures becomes necessary, responders will typically follow preexisting rules of engagement and will take into account the existing international legal framework, acknowledging the following:

  - Preexisting private-sector business relationships often provide a basis for continued collaboration in spite of a hostile international political environment.

  - Operational responses typically proceed at the least complex level of private sector engagement capable of addressing the issues. At this level, governments are rarely involved in response mechanisms.

  - If the U.S. Government becomes involved, it will need to extend its contacts beyond normal, trusted relationships in certain circumstances.

An appropriate U.S. network security strategy must involve efforts to shape the international environment in the following ways to reduce the risk to critical U.S. and global information infrastructures:

- Pursuing interagency coordinated bilateral, multilateral, and international initiatives that combine to enhance the U.S. and international partners' ability to not only deter, detect, identify, and prosecute perpetrators of an attack but also prevent, respond to, and mitigate its consequences.

Developing and facilitating cooperative public-private sector operational strategies designed to ensure the survivability and reliability of globally interdependent systems critical to U.S. interests, whatever the potential source of failure or compromise.[35]

These efforts should be consistent with other extant U.S. doctrine articulated in, for example, the "Critical Priorities for Cyberspace Security," as outlined in the National Strategy to Secure Cyberspace, and should underpin ensuing global communications infrastructure policy efforts.[36]

The U.S. Government has historically been a strong advocate for NS/EP requirements. Discussions on network security and CIP policy and practice are currently moving forward within several multilateral organizations.[37] These important multilateral initiatives should address NS/EP communications issues, and any such efforts should be informed by private sector SMEs.

4 Operational Issues

The NSTAC observes that fundamental operational requirements for access, security, and power are the same whether an incident is domestic or international. In responding to any incident, a network operator must inform its stakeholder or customer, mitigate harm, initiate recovery measures, and otherwise continue to collaborate with relevant infrastructure partners. Successful response depends on not only prior development of operational plans, procedures, relationships, and information paths but also trained personnel who are the product of enabling agreements and perfecting exercises with domestic and foreign stakeholders and governments.[38]

4.1 Domestic and International Collaboration on NS/EP and Incident Response

The expanding global interconnection of networks using common communication protocols, its use of shared services, and the fact that foreign providers own and operate many of these interconnected networks adds new complexity for all those involved in assuring that the NS/EP telecommunication needs of the U.S. Federal Government are met. These factors, along with the broader use and dependency on these networks for other critical national and international functions, further underscore the need for an effective international capability that can respond to disruptions affecting global networks. As stated in Presidential Executive Order (EO) 12472, emphasis on establishing *robust* international collaborative mechanisms is essential to achieving and maintaining effective responsive capabilities that not only enhance situational awareness and NS/EP incident response but also provide additional support when needed for burden sharing, troubleshooting, and other operational issues.

Existing policy collaboration is insufficient; limited policy collaboration exists in few areas. However, international collaboration in key areas developed under a more formal protocol would advance strategic IT and communications NS/EP preparedness efforts. Such protocols would help mitigate the effects on the network and would enhance response efforts during and after an incident. Moreover, it would ease continuity of operations and promote the rapid recovery of operations.

4.2 Current Collaboration Landscape

As set out in Homeland Security Presidential Directives (HSPD) 5 and 7, DHS retains much of the responsibility for U.S. Government policy direction in network security.[39] Within DHS, the NCS and NCSD are involved in U.S. Government efforts on international NS/EP in the communications and IT sectors as follows:

National Communications System

Operationally, the NCS' National Coordinating Center (NCC) is increasingly involved in international NS/EP communications issues. Most notably, communications officials from the government of Canada participate in biweekly video teleconferences with the NCC to share information about ongoing concerns. Officials from Industry Canada also have been assigned to the NCC Watch for 2-week periods to observe operations and share best practices.

National Cyber Security Division

NCSD maintains relationships with key allies abroad by sharing information products and collaborating on issues of mutual concern, in cooperation with DOS. NCSD has also established arrangements with the allied countries of Australia, Canada, New Zealand, and the United Kingdom to address strategic issues of common concern and to establish regular communication and collaboration between computer security incident response teams to build situational awareness and coordinate incident response when needed.[40] NCSD also maintains less-formalized relationships with other foreign countries.

Coordinated Training, Exercises, and Incident Response

To contribute to IT and communications NS/EP collaborative efforts effectively, similar international relationships must be created to ensure the international community has adequate collaboration between government and industry to enable information sharing, cooperation, and effective incident response. Preparation and planning based on prior policy agreement and predetermined delegations of roles and responsibilities are essential to effective operational incident response.[41]

4.3 United States Government to Industry Collaboration

Private sector owners and operators have worked closely with the NCS since its creation in 1963. This relationship was further enhanced when the NCC was established in 1984. The NCC serves as a joint industry-Government operations center with a clear mission of advancing NS/EP information sharing and coordination.

Following the issuance of Presidential Decision Directive (PDD) 63, a series of Information Sharing and Analysis Centers (ISAC) was established to facilitate industry-government collaboration on critical infrastructure protection.[42] Among these centers is an ISAC for telecommunications, which works closely with the NCS' NCC, and an IT ISAC, which works closely with NCSD's US-CERT.[43] Per HSPD-7, the U.S. Government also urged the creation of sector coordinating councils (SCC) among the critical infrastructure sectors to increase industry-Government cooperation on policy. SCCs have been established in most of the critical infrastructures, including IT and communications.[44]

An example of this collaboration can be seen in the Estonia denial of service attack. On May 2, 2007, Estonia requested assistance through NATO. DOD contacted the US-CERT, which coordinated a response with the NCC, Forum of Incident Response and Security Teams (FIRST), and North American Network Operations Group (NANOG) community.[45]

4.4 Industry's Global Collaboration

The interconnected and interdependent nature of networks has fostered crucial information sharing and cooperative response and recovery relationships among global service providers for decades. Because one service provider network problem nearly always affects other network provider-owned and –operated networks, the community has a longstanding tradition of cooperation and trust—even in today's highly competitive business environment. ISACs facilitate information sharing within and among critical sectors such as IT and communications.

Because many companies operate globally, with a strong presence in other countries, their interaction with those governments (and, in the case of foreign companies in the United States) occurs on two levels. The first level is when a company provides services to the government of that country or to critical infrastructure members within that country. In these cases, operational response efforts occur as the result of service level agreements or customer service obligations. The second level is when a company is operating in a country but is called on to assist in an incident outside any formal business arrangements. In both cases,

companies assist and work directly with their customers; in some instances, they collaborate with government entities to respond to an incident and restore services.

In working cooperatively, industry has identified several areas in which government support and assistance are critical. While responding to domestic incidents, industry has determined that establishing government-accepted credentials for critical service providers is key. Infrastructure providers also may need for the U.S. Government to facilitate physical access and, when requested, to provide security for these service providers during or immediately following an incident. In addition, the communications and IT sectors realize that their networks rely on power to function; therefore, their work must be closely aligned with that of the power/energy companies to address this critical interdependency.[46] ISACs in the telecommunications and IT sectors, CERTs, including US-CERT and DOD's joint task force/global network operations (JTF-GNO), private bodies, and commercial interests all provide a steady stream of data regarding the condition of the network, threats being mounted against it,[47] and tools for defending against or mitigating the impact of insults.

5 Findings

Based on numerous SME briefings and extensive research into international communications policy and operational issues, the NSTAC presents several findings concerning the international NS/EP communications environment:

- The rapidly evolving global communications infrastructure is increasingly interconnected through a system of systems that provides global services and connectivity. A global workforce, including those in non-allied nations, operates and maintains the infrastructure.

- As a result of globalization, the U.S. NS/EP communities, government operations, allies, many key businesses, and their global business partners are increasingly dependent on the availability of global communications and related services.

- Cross-sector dependencies and interdependencies (such as between telecommunications and electric power) create additional complexities, amplifying the difficulties of mitigation and effective repair when broad-scale disruptions occur.

- Cyber threats to global infrastructures may originate from international sources beyond the jurisdiction of U.S. and allied authorities.

  - Attacks originating outside the territorial United States raise increasing 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 PNs and private sector networks, nor do they adequately include private sector participation in these processes.

6 Recommendations

Recognizing NS/EP communications' evolving dependence on and interdependence with global infrastructures and to enhance the resiliency of the global communications infrastructure, the NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by EO 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the following:

- Task DHS to coordinate international planning and development with the appropriate Federal Agencies for adoption of a global framework incorporating

operational protocols and response strategies. The framework must accomplish the following:

- Address physical and cyber events that would disrupt the availability of critical global infrastructure services.
- Ensure private sector participation in developing the framework to leverage extensive expertise and existing relationships.
- Support the use of identity management solutions that address NS/EP requirements for normal operations and all-hazards crisis response.
- Examine, with the help of private sector partners, existing U.S. laws and policies that could prevent service providers and other stakeholders from taking the necessary proactive measures to restore service and prevent harm to NS/EP users for government essential operations during a crisis.

▶ In the interim, *task Federal Agencies to 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 NCC.

Footnotes

1 Globalization is the integration of people, companies, and governments of different nations, driven by international trade and investment and aided by information technology.

2 The "global communications infrastructure" is a vast system of distributed, interconnected, and international networks, broader than the "Public Network," including what many call the Next Generation Network (NGN). This infrastructure includes both traditional information technology and communications components, and will logically (and broadly) consist of applications and devices that deliver services, the services provided to users (some by the network and some external to it), and the underlying transport networks. The term "global communications infrastructure" is used to emphasize the breadth of coverage of these networks.

3 "Asia Communications Hit by Quake," *BBC News*, December 27, 2006.

4 "Cyber Assaults on Estonia Typify a New Battle Tactic," Washington Post, May 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_pf.html

5 Although Homeland Security Presidential Directive-7 bifurcates the U.S. ICT industry into telecommunications and information technology, ICT is the internationally accepted terminology for the combined industries and is used in this report to describe the converged technology environment.

6 The "global communications infrastructure" is a vast system of distributed, interconnected, and international networks, broader than the "Public Network," including what many call the Next Generation Network (NGN). This infrastructure includes traditional information technology and communications components, and will logically (and broadly) consist of applications and devices that deliver services, the services provided to users (some by the network and some external to it), and the underlying transport networks. The term "global communications infrastructure" is used to emphasize the breadth of coverage of these networks.

7 As reported in the *European Telecommunications Standards Institute Report,* the October 2006 *European Union Cyber-Security Report,* and the European Union Proposal the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection: http://ec.europa.eu/justice_home/doc_centre/terrorism/protection/docs/com_2006_787_en.pdf; and http://ec.europa.eu/justice_home/doc_centre/terrorism/protection/docs/com_2006_787_en.pdf.

8 "NS/EP communications" is the domain of interest of the NSTAC and its advisory activities. We acknowledge that the concepts of NS/EP and NGN are evolving. Section 2 contains a more detailed discussion of these concepts.

9 Reports include *The NSTAC Report to the President on Next Generation Networks,* 2006; *The NSTAC Report to the President on the National Coordinating Center,* 2006; *The NSTAC Report to the President on Telecommunications and Electric Power*

Interdependencies: The Implications of Long-Term Outages, 2006; *The NSTAC Financial Services Task Force Report, 2004;* and *The NSTAC Satellite Task Force Report,* 2004.

10 Appendix E contains a complete listing of briefings.

11 Appendix A provides a complete list of participants, and Appendix B contains an acronym index.

12 Appendix D contains the latest version of the inventory.

13 Appendix C provides a Glossary of Key Terms.

14 Note, however, that as a result of the major restructuring of the telecommunications industry pursuant to the 1982 Consent Decree, the National Research Council, in its 1988 report, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness,* recommended the establishment of "Software Security Measures" (Recommendation 8) "to protect the public network from penetration by hostile users, especially with regard to harmful manipulation of any software embedded within the public networks."

15 The NSTAC also observes that in the face of Hurricanes Katrina and Rita, the tsunamis, and other natural disasters, a similar evolution has occurred in understanding the EP component of NS/EP communications. This evolution has directly affected providers of EP communications services.

16 For example, the *Phase II Report of the United States Commission on National Security/21st Century, 2000* (also known as the Hart Rudman Commission).

17 Although numerous discussions have taken place regarding the term "NS/EP telecommunications," which is defined in FCC rules and regulations and 47-CFR 216, there is no universally accepted definition of "NS/EP communications." In addition, Homeland Security Presidential Directive 7 calls for the Executive Office of the President to review NS/EP communications policy. This pending review will presumably discuss and may authoritatively define NS/EP communications.

18 The NSTAC's *Report to the President on Next Generation Networks*, March 28, 2006.

19 Ibid, p. 4.

20 See also the National Incident Management System and its component National Response Plan under revision by DHS as of this writing.

21 Interdependencies are recognized as physical, technical, and human factors related.

22 The Cyber Storm Exercise, conducted in September 2006, demonstrated the impact of a blended physical-cyber attack. For more information, refer to "Fact Sheet: Cyber Storm Exercise," DHS Website, September 13, 2006, http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm, accessed April 25, 2007.

23 Brief by OSD-NII staff, June 9, 2006.

24 "Asia Communications Hit by Quake." *BBC News,* December 27, 2006.

25 For more information on the NATO response, see: *NATO News Release:* NATO to Strengthen Protection Against Cyber Attacks," June 14, 2007: http://www.nato.int/docu/update/2007/06-june/e0614b.html

26 "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post,* May 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_pf.html

27 The threat profile is rising as threats increasingly encompass international dimensions, with a substantial portion of attacks arising from or passing through locations outside of the United States. Additional attacks such as the DNS distributed denial of service attacks in January 2006 and February 2007 further illustrate the increasing threat profile. This citation was informed by subject matter expert interviews as well as the following sources: Graham, Bradley. "Hackers Attack Via Chinese Websites: U.S. Agencies' Networks Are Among Targets." *The Washington Post:* August 25, 2005, p. A1.

"Security Bytes: Chinese Websites Attack U.S. Government Networks." *SearchSecurity.com:* August 25, 2005: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1119270,00.html.

Stewart, Joe. "Myfip Intellectual Property Theft Worm Analysis." *Secure Works:* August 16, 2005: http://www.secureworks.com/research/threats/myfip/.

Thornburg, Nathan, "The Invasion of the Chinese Cyberspies," *Time,* August 29, 2005.

28 A matrix of many existing instruments that make up the international legal and policy framework was developed to analyze this environment. Appendix D provides the latest version of this matrix.

29 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006; International Telecommunication Union's "Final Acts of the Plenipotentiary Conference," Antalya, 2006.

30 *The National Strategy to Secure Cyberspace.* "Priority V: National Security and International Cyberspace Security Cooperation," February 2003, pp. 50–52.

31 DHS' NRP, December, 2004, p. INT-6. Please note that as this report was finalized, the NRP was under revision.

32 The NSTAC's *Report to the President on Next Generation Networks,* March 28, 2006, p. 15.

33 Ibid, p. 13.

34 Ibid, p. 9.

35 DOS, *International Critiqua Infrastructure Protection,* 2006.

36 Including the *National Strategy to Secure Cyberspace, National Infrastructure Protection Plan, and Information Technology Sector Specific Plan.*

37 Including the North Atlantic Treaty Organization (NATO), the Group of Eight (G8), the Organization of American States (OAS), the Organization for Economic Co-operation and Development (OECD), the International Telecommunication Union (ITU), the Asia-Pacific Economic Cooperation (APEC), and others.

38 Appendix F presents background information about operational capabilities.

39 Other agencies have network security collaboration duties, but this section focuses primarily on DHS' efforts.

40 NCSD/US-CERT is collaborating with 14 other countries in an informal arrangement to develop an International Watch and Warning Network (IWWN). Launched in 2004, the IWWN uses a secure portal for around-the-clock communications needs and holds annual conferences and workshops to build collaboration with government policy bodies, incident response teams, and law enforcement entities in the 15 countries (including the United States). In this case, the collaboration currently occurs without a formalized long-term arrangement or information sharing agreement such as a memorandum of understanding (MOU) in the military and intelligence areas.

41 Australia, Canada, New Zealand, and the United Kingdom participated in Cyber Storm I, and Cyber Storm II will include participation from government and private sector representatives from these countries.

42 PDD-63 is available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm; see also the ISAC Council Website at http://www.isaccouncil.org/about/ for more information.

43 See the Communications ISAC Website at http://www.ncs.gov/ncc/main.html, and the IT ISAC Website at https://www.it-isac.org/ for more information.

44 See the IT-ISAC Website at https://www.it-isac.org for more information.

45 US-CERT briefing to NSTAC, June 5, 2007.

46 Recent European documents addressing the availability and robustness of electronic communications infrastructures, such as the *Availability and Robustness of Electronic Communications Infrastructures,* February 2007, have noted issues associated with "ad hoc" nature of infrastructure protection issues, namely "The concept of sharing critical infrastructure information is not new to the communications industry in Europe. In fact, the study team's judgment is that some of the best processes reside in parts of Europe. However, on the whole, the practice is largely underutilized as an instrument for infrastructure protection. This leaves European communications networks avoidably less robust. For the most part, information sharing that does take place is ad hoc and occurs informally—the linkage can be easily broken with the absence of one key person."

47 Government and NSTAC NSIE, *An Assessment of the Risk to the Security of the Public Network,* April 2005.

Participant List

Member Company Participants

VeriSign, Incorporated
Mr. Michael Aisenberg, Esq., Co-Chair

Science Applications International Corporation
Dr. Marvin Langston, Co-Chair

AT&T, Incorporated
Ms. Rosemary Leffler, Co-Chair

Bank of America Corporation
Mr. Roger Callahan

BellSouth Corporation
Mr. David Barron

Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Juniper Networks, Incorporated
Mr. Robert Dix

Microsoft Corporation
Mr. Phil Reitinger, Esq.

Nortel Networks Corporation
Dr. Jack Edwards

Qwest Communications International, Incorporated
Mr. Kushal Jain

Raytheon Company
Mr. Frank Newell

Sprint Nextel Corporation
Mr. John Stogoski

Telcordia Technologies, Incorporated
Ms. Louise Tucker, Esq.

Unisys Corporation
Mr. Shawn Anderson

Verizon Communications, Incorporated
Mr. James Bean

Other Working Group Participants

British Embassy to the United States
Dr. Phil Budden

Edison Electric Institute
Mr. Larry Brown, Esq.

George Washington University
Dr. Jack Oslund

Independent Electricity System Operator Canada
Mr. Stuart Brindley

Industry Canada
Ms. Maggie Lackey
Mr. Robert Leafloor

Microsoft Corporation
Mr. Paul Nicholas

Qwest Communications International, Incorporated
Ms. Katherine Condello

Science Applications International Corporation
Mr. Hank Kluepfel

Sprint Nextel Corporation
Ms. Allison Growney

Symantec Corporation
Mr. Wesley Higaki

Telcordia Technologies, Incorporated
Mr. Bob Lesnewich

UK Centre for the Protection of National Infrastructure
Ms. Judy Baker
Mr. Mike Corcoran

VeriSign, Incorporated
Mr. Anthony Rutkowski, Esq.

U.S. Government Personnel

Central Intelligence Agency
Mr. Tom Donahue

Department of Homeland Security
Ms. Kathy Blasco
Mr. Kelvin Coleman
Ms. Liesyl Franz
Mr. David Delaney
Mr. Charles Lancaster
Mr. Thad Odderstol
Mr. Andrew Purdy, Esq.
Ms. Jordana Siegel
Ms. Christina Watson
Mr. Will Williams

Department of Commerce
Mr. Dan Hurley

Department of Defense
Mr. Thomas Dickinson
Mr. Mark Hall
Mr. Andrew Kimble

Department of State
Mr. David Chinn
Ms. Michelle Markoff

Federal Communications Commission
Mr. Richard Hovey

Federal Reserve Board
Mr. Chuck Madine

Acronym List

Acronym List

APEC	Asia-Pacific Economic Cooperation
BIAC	Business and Industry Advisory Committee
CCIPS	Computer Crimes and Intellectual Property Section
CCPC	Civil Communications Planning Committee
CI/KR	Critical Infrastructure and Key Resource
CEPTAG	Civil Emergency Planning Telecommunications Advisory Group
CERT	Computer Emergency Readiness Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CONOPS	Concept of Operations
CPNI	(UK) Centre for Protection of National infrastructure
CSCPCC	Communications Systems and Cybersecurity Policy Coordinating
CVE	Common Vulnerabilities and Exposures
DACS	Data and Analysis Center for Software
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
EO	Executive Order
ESF	Emergency Support Function
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
FIRST	Forum of Incident Response and Security Teams
G8	Group of Eight
HSARPA	Homeland Security Advanced Research Projects Agency
HSPD	Homeland Security Presidential Directive
IATAC	Information Assurance Technology Analysis Center
ICT	Information and Communication Technology
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
IT	Information Technology
ITAA	Information Technology Association of America
ITU	International Telecommunication Union
IWWN	International Watch and Warning Network
JCG	Joint Contact Group
JTF-GNO	Joint Task Force-Global Network Operations
MLAT	Mutual Legal Assistance Treaty
MNC	Multinational Corporation
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
NANOG	North American Network Operations Group
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center
NCS	National Communications System
NCSD	National Cyber Security Division
NGN	Next Generation Networks
NGO	Non-Governmental Organization
NII	National Information Infrastructure
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NRP	National Response Plan
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	President's National Security Telecommunications Advisory Committee
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
PDD	Presidential Decision Directive
PN	Public Network
PSTN	Public Switched Telecommunications Network
SCC	Sector Coordinating Council
SME	Subject Matter Expert
SPP	Security and Prosperity Partnership
SPSG	Security and Prosperity Steering Group
TEL	Telecommunications and Information Technology
TOPOFF	Top Officials
TTCP	Technical Cooperation Program
WPISP	Working Party on Information Security and Privacy
WTPF	World Telecommunication Policy Forum
UN	United Nations

Glossary of Key Terms

Glossary of Key Terms

All-Hazards

An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies.

[Source: National Infrastructure Protection Plan, Department of Homeland Security, 2006]

Information and Communications Technologies (ICT)

Although Homeland Security Presidential Directive-7 bifurcates the U.S. ICT industry into telecommunications and information technology, ICT is the internationally accepted terminology for the combined industries and will be used in this report to describe the converged technology environment.

Next Generation Networks (NGN)

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

However, there is no single, universally accepted definition of the NGN exists…The term NGN is not intended to represent any single configuration or architecture. Instead, it represents the set of converged networks…expected to arise that will transparently carry many types of data and communications and allow delivery of services and applications that are not coupled to the underlying network. However, it is possible to note several key NGN elements or attributes over which there is little, if any, dispute.

[Source: *NSTAC Report to the President on Next Generation Networks,* March 28, 2006]

National Security and Emergency Preparedness (NS/EP) Communications

Although the expression "NS/EP telecommunications" is defined in Federal Communications Commission rules and regulations (see 47-CFR 216), there is no single, universally accepted definition of NS/EP communications.

International Policy Instruments Matrix

Instrument	Summary
Treaties/Multilateral Agreement	
Council of Europe Convention on Cybercrime *[http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm]*	▶ Multilateral treaty; binds parties to cooperation in the investigation and prosecution of computer network crimes and physical-world crimes involving electronic evidence; and can provide timely extradition for computer network based crimes covered under the treaty. ▶ The treaty: (1) requires parties to establish certain substantive offenses in computer crime, (2) requires parties to adopt domestic procedural laws to investigate computer crimes, and (3) provides a solid basis for international law enforcement cooperation in combating crime committed through computer systems. ▶ United States became a full party on September 29, 2006. • Other signatory states include the United Kingdom, Canada, Germany, Japan, France, and Italy. Other ratified states include Fr0ance and the Netherlands. Of the 43 countries that have signed the treaty, 21 have completed the ratification process. ▶ U.S. law conformed to the Treaty even before ratification, so the United States needs no new laws.
Mutual Legal Assistance in Criminal Matters Treaties [*http://travel.state.gov/law/info/judicial/judicial_690.html*]	▶ "Since the first U.S. bilateral Mutual Legal Assistance Treaty (MLAT) entered into force with Switzerland in 1977, our MLATs have become increasingly important. They seek to improve the effectiveness of judicial assistance and to regularize and facilitate its procedures. Each country designates a central authority, generally the two Justice Departments, for direct communication. The treaties include the power to summon witnesses, compel the production of documents and other real evidence, issue search warrants, and serve process." (http://www.state.gov/
Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2006 *[http://www.state.gov/s/l/treaty/treaties/2006/]*	▶ Office of the Legal Adviser, United States Department of State (DOS)
1979 Radio Regulations Geneva	
1983 Revision Mobile Services	
1985 Revision Geostationary Orbit	
1987 Revision Mobile Services	
1988 Revision Geostationary Orbit	

Instrument	Summary
Statute and Regulation	
Communications Assistance For Law Enforcement Act [*http://www.askcalea.net/*]	▶ Sec. 1005. Cooperation of equipment manufacturers and providers of telecommunications support services ▶ Sec. 1008. Payment of costs of telecommunications carriers to comply with capability requirements.
Espionage Act of 1917 [http://frwebgate3.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=9286969814+0+0+0&WAISaction=retrieve]	▶ Makes it illegal for a person to share information with the purpose of interfering or infringing on U.S. Armed Forces operations or successes and makes it illegal to promote the success of the U.S.' enemies.
Computer Fraud and Abuse (CFA) Act [*http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html*]	▶ Whoever causes "damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security" can be punished under the CFA Act. ▶ The CFAA includes numerous broad provisions.
Communications Act of 1934 [*www.fcc.gov/Reports/1934new.pdf*]	▶ Section 305 (c)—the President may, provided he determines it to be consistent with and in the interest of national security, authorize a foreign government, under such terms and conditions as he may prescribe, to construct and operate at the seat of government of the United States a low-power radio station in the fixed service at or near the site of the embassy or legation of such foreign government for transmission of its messages to points outside the United States ▶ Section 706 (c)—Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States; (d) the President can (1) suspend or amend the rules and regulations applicable to any or all facilities or stations for wire communication within the jurisdiction of the United States as prescribed by the Commission, (2) cause the closing of any facility or station for wire communication and the removal there from of its apparatus and equipment, or (3) authorize the use or control of any such facility or station and its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners.
Federal Information Security Management Act of 2002	Subchapter III: "(2) recognize the highly networked nature of the current Federal computing environment and provide effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian."

Instrument	Summary
Executive Order/Presidential Directive/National Strategy Document	
Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection; Section 22(a) [*http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html*]	▶ "DOS, in conjunction with DHS, and the Departments of Justice, Commerce, Defense, and other appropriate agencies, will work with foreign governments and international organizations to strengthen the protection of U.S. critical infrastructure and other key elements." • HSPD-7 superseded Presidential Decision/Directive (PDD) 63: "There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations." [*http://www.fas.org/irp/offdocs/pdd-63.htm*]
National Strategy for Homeland Security [*http://www.whitehouse.gov/homeland/book/*]	▶ "Partner with the international community to protect our transnational infrastructure." (p 35) Text specifically mentions: (a) U.S. energy system as part of an interconnected system with Mexico and Canada, and (b) "joint steering committees with Canada and Mexico to improve the security of critical physical and cyber infrastructure." ▶ "Expand protection of transnational critical infrastructures" (p. 60) ▶ "Improve cooperation in response to attacks." (p 61) Reference to the U.S. Government expanding exercise and training activities with Canada.
The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets [*http://www.whitehouse.gov/pcipb/physical.html*]	▶ "Foster international security cooperation" (p 13); "In a world characterized by complex interdependencies, international cooperation is a key component of our protective scheme." ▶ "Conduct critical infrastructure protection planning with our international partners." (p. 24) Reference is made to Canadian and Mexican partners.
The National Strategy to Secure Cyberspace [*http://www.whitehouse.gov/pcipb/*]	▶ "Priority V: "National Security and International Cyberspace Security Cooperation" (p. 4) Reference to cross border cyber attacks. ▶ Threat and Vulnerability, a Five Level Problem: "Level 5: Global" (p. 8) Reference to "a planetary information grid of systems" and "internationally shared standards."
National Plan	
National Response Plan (NRP) [As of May 25, 2006] [*http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm*]	▶ The NRP provides an all-hazards approach that incorporates best practices from a wide variety of first responders, including fire, rescue, emergency management, law enforcement, public works and emergency medical services for responding to natural and manmade disasters. The NRP Base Plan and 15 annexes (or Emergency Support Functions [ESF]). Provide protocols for departments and agencies at all government levels: Federal, State, local and tribal, and for private sector partners. ESF# 2 applies to the Communications sector and ESF#12 applies to the Energy sector.

Instrument	Summary
National Infrastructure Protection Plan (NIPP) [As of 2006] [*http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm*]	▶ Need to protect systems and networks operating across or near borders with Canada and Mexico (pp. 13–14) ▶ "Canada and Mexico. Critical Infrastructure and Key Resource (CI/KR) interconnectivity between the [U.S.] and its immediate neighbors makes the border virtually transparent." Electricity is mentioned, but not telecommunications, as crossing borders with Canada and Mexico "as a routine component of commerce and infrastructure operations." (p. 56) ▶ "The NIPP addresses international CI/KR protection, including inter-dependencies and the vulnerability of threats that originate outside the country …The NIPP also provides tools to assess international vulnerabilities and interdependencies that complement long-standing agreements with Canada [and] Mexico…" (p. 125)
Sector Specific Plans for Energy, Communications and Information Technology (IT)	▶ "Sector specific plans (SSP) are required to include international considerations as an integral part of each sector's planning process rather than instituting a separate layer of planning. Some international aspects of CI/KR protection require additional overarching or cross sector emphasis," including…Protection of physical assets located on, near or extending across the borders with Canada and Mexico that require cooperation with and/or planning and resource allocation among neighboring countries, States bordering on these countries, and affected local and tribal governments." (pp. 125–126 of the NIPP)
Multinational MOU/Resolution/Commitments/Strategy	
United National General Assembly Resolution 56/121 [http://daccess-ods.un.org/TMP/2925134.html] and 55/63 [*http://www.apectelwg.org/e-securityTG/UN-Res-FinalRep20020501.doc*]	▶ "Combating the criminal misuse of information technologies."
The Technical Cooperation Program (TTCP) MOU	▶ AUSCANNZUKUS nations represented by various military fora known as the Multifora • Air and Space Interoperability Council • American, British, Canadian, and Australian Armies • AUSCANNZUKUS Naval C4 • Combined Communications Electronics Board • Multinational Interoperability Council • Multilateral Interoperability Program • The Technical Cooperation Program ▶ Includes Defense Departments of Australia, Canada, UK, New Zealand and United States
Combined Joint Multilateral Master Military Information Exchange MOU	▶ High-Level and Long-Standing Defense MOU ▶ Includes Defense Departments of Australia, Canada, UK, New Zealand and United States

Instrument	Summary
AUSCANNZUKUS IA/CND MOU Executive Summaries of DOD Military-to-Military Relationships; International CND Coordination Working Group (ICCWG) Terms of Reference location: [*https://livelink.bah.com/livelink/livelink?func=ll&objId=7343822&objAction=Open*]	▶ Information Assurance Computer Network Defense (CND) MOU and Terms of Reference which establish the ICCWG. ▶ Includes Defense Departments of Australia, Canada, UK, New Zealand and United States
Asia-Pacific Economic Cooperation TEL Cyber Security Strategy [*http://www.apec.org/apec/apec_groups/working_groups/telecommunications_and_information.html*]	▶ The APEC Cyber Security Strategy encompasses a set of "measures to protect business and consumers from cybercrime, and the strengthen consumer trust in the use of e-commerce."
Single Agency MOU/ Bilateral Agreement	
Executive Summaries of DOD Military-to-Military Relationships; International Computer Network Defense Coordination Working Group Terms of Reference location: [*https://livelink.bah.com/livelink/livelink?func=ll&objId=7343822&objAction=Open*]	▶ AUSCANNZUKUS nations represented by various military fora known as the multifora • Air and Space Interoperability Council • American, British, Canadian, and Australian Armies • AUSCANNZUKUS Naval C4 • Combined Communications Electronics Board • Multinational Interoperability Council • Multilateral Interoperability Program • The Technical Cooperation Program
Federal Communications Commission (FCC)—Agreement Between the Government of the United States of America and the Government of the Argentine Republic Concerning the Provision of Satellite Facilities and the Transmission and Reception of Signals to and From Satellites for the Provision of Satellite Services to Users in the United States of America and the Republic of Argentina [*http://www.fcc.gov/ib/sand/agree/others.html*]	▶ To "facilitate the provision of services to, from and within the United States and Argentina via commercial satellites…and to establish the conditions relating to the use in both countries of satellites licensed by the United States or Argentina."
FCC—Various agreements with Canada (radio and TV broadcast, non-broadcast, satellite, and by frequency band) [*http://www.fcc.gov/ib/sand/agree/welcome.html*]	

Instrument	Summary
FCC—Various agreements with Mexico (radio and TV broadcast, non-broadcast, satellite, and by frequency band) [*http://www.fcc.gov/ib/sand/agree/welcome.html*]	
Bilateral Meetings	▶ DHS, in cooperation with State and other Federal agencies, engages in bilateral discussions with close allies and others to further international cyber security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. ▶ Major Bilaterals with Australia, Canada, Japan ▶ Other bilaterals include Hungary, Netherlands, Romania, Sweden, Taiwan, UK, Nigeria, Norway, Tunisia, Rwanda
Departmental Policy/Agency Letter	
National Cyber Security Division (NCSD) Cyber Storm After Action Report	▶ The first full-scale government-led cyber security exercise to examine response, coordination, and recovery mechanisms to a simulated cyber-event within international, Federal, State, and local governments, in conjunction with the private sector.
Internet Corporation for Assigned Names and Numbers [h*ttp://www.icann.org/*] Bylaws and Articles of Incorporation	▶ "An internationally organized, nonprofit corporation that has responsibility for Internet Protocol address space allocation, protocol identifier assignment, generic and country code Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority and other entities."
European Telecommunications Standards Institute (ETSI) Directive 2006/24/EC of European Parliament and the Council of 15 March 2006 [*http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf*]	▶ Industry and law enforcement began cooperating through ETSI to develop data retention/global stored data handover specifications
Industry Policy Statement	
IT-Information Sharing Analysis Centers (ISACs) Concept of Operations Document [www.ncs.gov/nstac/reports/2006/NSTAC_XXIX_Reports_082206.pdf]	▶ "Sets out an operational mission statement, defining the roles and relationships for the IT ISAC within the information technology sector, within the larger infrastructure community, and between the sector and relevant agencies of Government and other institutions"
Communications SSP	▶ The NIPP and its complementary Sector-Specific Plans (SSP) provide a consistent, unifying structure for integrating both existing and future CI/KR protection efforts.

Instrument	Summary
Other Industry Instruments	
IT-SSP, Draft Version Available at IT-ISAC Website: [*https://www.it-isac.org/*]	▶ The IT-SSP highlights the need for the sector to identify, assess, and manage risks to the infrastructure and its international dependencies.
United States Computer Emergency Readiness Team (US CERT) [*http://www.us-cert.gov/*]	▶ US CERT "is a partnership between DHS and the public and private sectors. Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation.
Forum for Incident Response and Security Teams (FIRST) [*http://www.first.org/*]	▶ "FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large."
President's National Security Telecommunications Advisory Committee (NSTAC) Legislative and Regulatory Task Force Report: Penalties for Internet Attacks and Cyber Crime [*http://www.ncs.gov/nstac/reports/2003/LRTF%20Cyber%20Crime%20Report.pdf]*	▶ Work with international counterparts and through multilateral bodies to encourage other nations to enact substantive and procedural laws, adopt data preservation provisions, dedicate well-trained and well-equipped personnel to combat cyber crime, encourage better cooperation among nations for locating and identifying cyber criminals and designate a 24-hour point of contact on such matters for urgent cross-border investigations.
Other Instruments	
Working Group of Key Allies (AUSCANZUKUS)	▶ Working Group of key allies is made up of Australia, Canada, New Zealand, United Kingdom, and United States
Joint Contact Group (JCG)	▶ Ongoing bilateral between the U.S. and the U.K. on homeland security issues managed at the Deputy Secretary level in DHS ▶ Established in June 2003 by DHS to provide a common platform to share knowledge and good practice on joint security issues such as protecting borders, transport security and scientific/technological advances ▶ The Cyber Security Work stream was developed in 2004 ▶ Cyber Security was on the agenda for the first time in June 2006 ▶ Collaborating on the CIIP directory and exercises including Cyber Storm ▶ Leveraging ongoing efforts of international watch and warning network (IWWN) and group of key allies

Instrument	Summary
IWWN	▶ Priority V of the National Strategy to Secure Cyberspace calls for the establishment of an "…international network capable of receiving, assessing, and disseminating this information globally. Such a network can build on the capabilities of nongovernmental institutions such as the Forum of Incident Response and Security Teams." ▶ Coordinates cross-functional engagement of government cyber security policymakers, managers of computer security incident response teams with national responsibility, and law enforcement representatives with responsibility for cyber crime ▶ Reflects an arrangement among countries to establish a community and a mechanism for collaboration on CIIP ▶ DHS/NCSD co-hosted the IWWN Conference in October 2004 and June 2006, which marked the launch of the IWWN portal ▶ Planning for IWWN Conference in May 2007 ▶ Working to enhance portal content and use for collaboration ▶ Participating states include Australia, Canada, Finland, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom, and United States
Security and Prosperity Partnership of North America (SPP)	▶ U.S. Government Presidential initiative managed at the Secretary level in DHS ▶ Launched in March of 2005 as a trilateral effort to increase security and enhance prosperity among the United States, Canada, and Mexico through greater cooperation and information sharing ▶ Cyber security falls largely within Goal 9 of the SPP, which serves to "Develop and implement a common approach to critical infrastructure protection, and response to cross-border terrorist incidents, and, as applicable, natural disasters"
Organization of Economic Cooperation and Development (OECD) Working Party on Information Security and Privacy (WPISP)	▶ U.S. Delegation, led by the Department of State's Economic Bureau, includes participation from DHS, Federal Trade Commission, Commerce, Department of Justice, and the private sector ▶ The WPISP, composed of 30 countries, develops policy options by addressing information security and privacy as complementary issues at the core of our digital activities and by maintaining an active network of experts from government, business and civil society ▶ Continuing to leverage work ongoing in other forums such as Asia-Pacific Economic Cooperation Telecommunications and Information Technology Working Group (APEC TEL), bilaterals, and the International Telecommunications Union (ITU) ▶ The private sector is represented in the OECD by the Business and Industry Advisory Committee (BIAC) to the OECD. Each BIAC member organization designates national experts to BIAC committees. The U.S. BIAC Affiliate United States Council for International Business.

Instrument	Summary
Asia Pacific Economic Cooperation Telecommunications and Information Working Group	▶ The APEC TEL is a working group of APEC that addresses various telecommunications and IT issues relevant to the Asia Pacific region ▶ APEC TEL has 21 members, including the United States; ▶ APEC members are referred to as "economies" rather than "countries" to reflect APEC's economic goals and avoid political sensitivity concerning the autonomy of governments ▶ In 2002, the APEC developed and released the APEC Cyber Security Strategy. In 2005, the APEC TEL developed a strategy to ensure a "Trusted Secure and Sustainable Online Environment," which encourages actions to further cyber security efforts of member economies ▶ Cyber security issues have been elevated recently to necessitate a cyber-specific steering group for which DHS NCSD serves as Deputy Convener for the Security and Prosperity Steering Group in APEC TEL ▶ APEC TEL meets biannually and is hosted by volunteer economies on a rotating basis (a different economy hosts each TEL meeting) ▶ APEC TEL regularly hosts workshops on specific topics for member economies, *e.g.,* CSIRT development series; Malware Workshop ▶ 21 member economies include the following: Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; Russian Federation; Singapore; Chinese Taipei; Thailand; Viet Nam; United States
ITU-Development Study Group 1	▶ International organization within the United Nations System where governments and the private sector coordinate global telecom networks and services ▶ DHS and the State Department participate in ITU-D Study Group 1, which is currently reviewing Question 22 on securing information and communication networks—best practices for developing a culture of cyber security. The U.S. Government is proposing a report on recommended "best practices" for cyber security ▶ The U.S. Government looks to the U.S. private sector to engage in the ITU by participating in public/private delegation preparation meetings and by participation on the official U.S. Delegation to the relevant Study Group meetings ▶ Many private sector companies from countries across the world are ITU members; more information is available at http://www.itu.int/home ▶ Includes representation from 190 member states worldwide. It also has more than 600 private sector members and associates that make up the world's major telecommunication operators, equipment manufacturers, funding bodies, research and development organizations, as well as international and regional telecommunication organizations ▶ The Plenipotentiary Conference is the top policymaking body of the ITU

Instrument	Summary
ITU Final Acts of the Plenipotentiary Conference (Antalya, 2006)	This ITU conference decided: (1) to convene the fourth World Telecommunication Policy Forum (WTPF) in Geneva in the first quarter of 2009, to discuss and exchange views…; (2) that the fourth WTPF shall draw up a report and, if possible, opinions for consideration by ITU Member States and Sector Members and relevant ITU meetings; and (3) that arrangements for the fourth WTPF shall be in accordance with applicable Council decisions for such fora.
Organization of American States (OAS)	▶ The OAS brings together the countries of the Western Hemisphere to strengthen cooperation and advance common interests. U.S. Government agencies, including DHS, participate in the Inter-American Committee on Counter Terrorism (CICTE), which addresses cyber security. U.S. agencies also participate in the Ministers of Justice or Attorney Generals of the Americas (REMJA) and Inter-American Telecommunication Commission (CITEL) ▶ The U.S. Government leads the CICTE and REMJA initiatives and has been a driver for cyber security ▶ Member States include Antigua and Barbuda; Argentina; the Bahamas; Belize; Bolivia; Brazil; Canada; Chile; Columbia; Costa Rica; Dominica; Dominican Republic; Ecuador; El Salvador; Grenada; Guatemala; Guyana; Haiti; Honduras; Jamaica; Mexico; Nicaragua; Panama; Paraguay; Peru; Saint Kitts and Nevis; Saint Lucia; Saint Vincent and the Grenadines; Suriname; Trinidad and Tobago; United States; Uruguay; and Venezuela
Organization of American States (OAS) AG/RES. 2004 (XXXIV-O/04)	Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity
Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations [*http://www.reliefweb.int/telecoms/tampere/icet98-e.htm*]	▶ Not yet ratified by the U.S. Senate, but in force internationally as of January 8, 2005
Joint Report by the Data and Analysis Center for Software (DACS) and the Information Assurance Technology Analysis Center (IATAC) on Software Assurance Through Secure Software Engineering	▶ The report covers methods, tools, and best practices. It points to resources such as Build Security In. DACS and IATAC are information analysis centers operating under the Defense Technical Information Center
Safety and Security Extensions for Integrated Capability Maturity Models [*www.faa.gov/ipg/news/finalReport.htm*]	▶ Joint report by the Federal Aviation Administration and the Department of Defense to identify best safety and security practices in software engineering.

Instrument	Summary
U.S./Canada Civil Emergency Planning Telecommunications Advisory Group	▶ The NCS has a strong and well established working relationship with Canada, currently embodied in the U.S./Canada Civil Emergency Planning Telecommunications Advisory Group (CEPTAG). ▶ The CEPTAG, created in 1988, provides a forum for addressing shared communications concerns and for facilitating cross-border cooperation and mutual assistance in the event of an emergency. ▶ Canadian representation is provided through Industry Canada, which is the lead department for developing, maintaining, and facilitating emergency telecommunications policies and programs. ▶ The last CEPTAG meeting occurred in Ottawa, Canada, in September 2006, with extensive discussions between representatives of the NCS and Industry Canada. Agenda topics included pandemics and modeling and analysis
NCS/Industry Canada Standard Operating Procedures (SOP)	▶ The NCS and Industry Canada are working to establish and exercise an SOP to facilitate cross-border coordination. ▶ SOP 303 can be used to coordinate cellular service disruption around shared assets, such as bridges and tunnels ▶ SOP 304 is designed to expedite the transport of personnel, material, and equipment across the U.S./Canada border as part of a disaster response operation.
TTCP Beginner's Guide	
Air Force Cyberspace Command	This new command is a significant step in protecting the service's data while detecting adversary data and then denying, disrupting, and destroying the source or transmission of that information. The cyberspace force will draw on the knowledge and talents across all Air Force commands, in addition to the capabilities already housed in the 8th Air Force, including command and control, electronic warfare, net warfare, and surveillance and reconnaissance (per Air Force Print News article)
ITU's NGN-GSI Draft Document on NGN Identity Management Security	Provides a framework for identity management based on the NGN Functional Requirements and Architecture Release 2. The IdM framework is applicable to all NGN entities (such as service providers, network providers, network elements, users, and user's equipment).
Combined Communications Electronics Board [*http://www.jcs.mil/j6/cceb/*]	▶ A five-nation (Australia, Canada, New Zealand, United Kingdom, and United States) joint military communications-electronics (C-E) organization whose mission is the coordination of any military C-E matter that a member nation refers to it.
Common Vulnerabilities and Exposures Standards (CVE) [*http://cve.mitre.org/about/*]	CVE is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. Using a common name makes it easier to share data across separate databases and tools that until now were not easily integrated. This makes CVE the key to information sharing. If a report from one of the user's security tools incorporates CVE names, the user may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate this problem.

Briefings Listing

Briefer	Topic
Computer Emergency Readiness Team (CERT)/CC	CERT International Program
Computer Sciences Corporation	Research and Design Exchange 2006 Overview
Department of Commerce/National Telecommunications and Information Administration	Cyber Security and Critical Infrastructure Protection (CIP): Framework for National Action
Department of Defense(DOD)/National Information Infrastructure (NII)	International Information Assurance Program (IIAP)
Department of Homeland Security (DHS)/National Cyber Security Division (NCSD)	NCSD International Affairs Program Overview
Department of Justice (DOJ)/Computer Crime and Intellectual Property Section	United States Activities to Improve Cybercrime Legislation and Investigate Capacities
Department of State (DOS)	DOS Overview of International Telecommunications Union (ITU)/Industry Involvement in the ITU Standards Development Process
DHS/National Communications System (NCS)	Security Implications of Next Generation Networks
DHS/NCS	U.S./Canada Telecommunications Bilateral Relationship
DHS/NCSD	NCSD International Affairs Briefing
DOD/Joint Task Force—Global Network	Information Sharing Partners
DOD/NII	Private Sector Role in Military to Military Relationships
DOD/NII Computer Network Defense	Information Sharing Partners
DOS	International Critical Infrastructure Protection
DOS	DOS Four Track Plan Overview/Discussion
Edison Electric	Overview of Final Report on the Implementation of the Task Force Recommendations: U.S.-Canada Power Systems Outage Task Force
Independent Electricity System Operator—Canada	Electricity Industry—Government Relationships: US and Canada
Information Technology Association of America (ITAA)	ITAA Activities in International Cyber Security Outreach
Microsoft	National Information Assurance Partnership Common Criteria Testing Program Overview
Microsoft	Overview of National Strategy to Secure Cyberspace: Priority V
VeriSign	Network Security and Forensics: Industry Global Cooperation
VeriSign, iDefense	iDefense/Cooperation and Collaboration Overview

Operations Background

Operations Background

National Communications System

The National Communications System (NCS) was established by Executive Order (EO) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions.* EO 12472 requires the Executive Agent of the President, who is currently the Secretary of Homeland Security, to designate a "Manager of the NCS" to ensure that the NCS conducts unified planning and operations, to coordinate the development and maintenance of an effective and responsive capability for meeting the Federal Government's domestic and international national security and emergency preparedness telecommunications needs.

Some formal capabilities exist today for industry and the U.S. Government to share information about the telecommunications infrastructure through various existing mechanisms. The same applies to industry's ability to share information among various industries and for the U.S. Government to share information with foreign governments. Currently, some groups have operational capabilities that can respond to all hazard type incidents affecting networks, including incidents involving physical damage that can create cyber consequences.

Other collaboration occurs on more of an ad hoc basis, as relationships have developed in discrete business areas, and as new global collaborative business arrangements continue to emerge.

Information Sharing

In today's global environment, information technology (IT) and communications networks connect people, companies, and governments seamlessly across international borders. From communications satellites to undersea cables to cell towers operating near borders, the communications and IT industries are inherently international. The borderless nature of this network allows incidents to spread quickly from country to country.

Given the increasing reliance on the communications and IT sectors, a need exists for governments and private industry to establish trust relationships with international partners in order to enhance situational awareness, build national security and emergency preparedness (NS/EP) capabilities, establish incident response mechanisms, and, when needed and feasible, create mechanisms for burden sharing, troubleshooting, and other operational issues that may arise.

To address these issues, industry and government have developed mechanisms to share information about the communications and IT infrastructure. These mechanisms involve government-to-government, government-to-industry, and industry-to-industry and several mechanisms can respond to all-hazard type network impacting incidents, including incidents involving physical damage with cyber consequences.

Within the Department of Homeland Security (DHS), the NCS and the National Cyber Security Division (NCSD) are involved in U.S. Government efforts on international NS/EP in the Communications and IT Sectors.

In cooperation with DHS and the Department of State (DOS), the NCS actively assesses the work of multilateral organizations such as the United Nations (UN), the European Union (EU), the Organization of American States (OAS), and the Organization for Asia-Pacific Economic Cooperation (APEC). The NCS also works closely with the International Telecommunication Union (ITU), an organization within the United Nations in which governments and the private sector collaborate to standardize and regulate international radio and telecommunications.

The NCS has a working bilateral relationship with their Canadian counterparts on NS/EP and critical infrastructure protection issues. The United States and Canadian governments created the Civil Emergency Planning Telecommunications Advisory Group (CEPTAG) in 1988 to address shared communications concerns, as well as to facilitate cross-border cooperation and mutual assistance in the event of an emergency. The NCS, NCSD, and the Homeland Security Advanced Research Projects Agency (HSARPA) also have well-developed bilateral

relationship with their United Kingdom counterparts, pursued primarily through DHS' Joint Contact Group (JCG), a DHS-wide agreement for cooperation in science/technology and research and development matters. The principal NCS task under the JCG is to develop government-to-government priority routing capability for emergency communications.

The NCS is also involved in implementing the U.S./Mexico/Canada Security and Prosperity Partnership (SPP). The SPP was launched in 2005 as a dual binational effort to increase security and enhance prosperity in North America. The NCS leads several SPP initiatives as part of the larger effort to develop and implement a common approach to critical infrastructure protection and plans for response to cross-border terrorist incidents and natural disasters. The NCS also represents the U.S. Government within the North Atlantic Treaty Organization's (NATO) Civil Communications Planning Committee (CCPC). The CCPC works to assess existing and future civil postal and telecom systems, networks, and other resources relative to civil emergency planning and critical infrastructure protection in response to natural and man-made disasters.

Officials from Industry Canada have also been detailed to the NCC Watch for 2-week periods to observe operations and share best practice information.

DHS' NCSD works directly with several international organizations to raise awareness, increase outreach opportunities, and, as part of its effort, to create a culture of cyber security. This includes contributing to the previously mentioned SSP of North America and the Joint Contact Group with the United Kingdom, as well as working through multilateral organizations including the International Telecommunication Union, the Security and Prosperity Steering Group of the Asia Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), the Organization for Economic Cooperation and Development (OECD), and the Organization of American States.

The Department of Justice's (DOJ) Computer Crimes and Intellectual Property Section (CCIPS) has been organizing cybercrime programs for the past several years. Though CCIPS predates the United States' signing of the Convention on Cybercrime in 2001, CCIPS has since been "assist[ing] states in amending their legislation to meet Convention standards (not American law) and to train new law enforcement officials, including investigators, prosecutors, and judges, in cybercrime-related issues."[1] CCIPS international work extends beyond the G-8 countries, as CCIPS has provided cybercrime training and guidance to nations worldwide. In 2003, CCIPS led a U.S. delegation that provided legislative drafting training to countries in the Middles East and North Africa. In 2003, CCIPS again focused its attention on the continent of Africa, leading two cybercrime workshops for the Law Enforcement Academy. Currently CCIPS is engaged with APEC, providing training for prosecutors and judges. Finally, CCIPS has provided confidential review of pending cybercrime statutes for several countries around the globe.

As response and recovery plans have emerged domestically, NCS and NCSD have worked to involve international partners in DHS efforts to train personnel and exercise the plans. This has included Canadian, Mexican, and the United Kingdom participation in the biannual Top Officials (TOPOFF) exercise, as well as the NCSD-sponsored Cyber Storm I and forthcoming Cyber Storm II. Through these exercises, NCS and NCSD have established contacts, shared best practices and lessons learned, and have ensured that the NCC and US-CERT understand the opportunities and challenges to working with international partners.

In addition, the NCS leveraged these government-to-government and government-to-industry relationships during the response to Hurricane Katrina. Because of the overwhelming effects of the disaster, the NCS worked with private industry to facilitate the entry of communications-related personnel, goods, and equipment from Canada into the United States to assist with the response. The NCS has also worked to assist Canada during ice storms, the Northeast blackout, and other natural disasters during the past decade.

Industry collaboration across traditional borders occurs intercompany for multinational corporations, and intra-company through customer and partner relationships, through established incident response processes, and incident by incident. An exception is the work of the Forum for Incident Response Security Teams (FIRST) organization, which is a private sector, global forum for those involved in incident response security efforts. Primarily an international networking forum for incident response teams through an annual conference, FIRST provides a resource for connections to other incident response teams, either government, industry/company, or academic.

Governments continue to work on these issues internationally. For example, Meridian is an annual international conference that provides an opportunity for governments to discuss how they can work together to protect critical infrastructures, exploring the benefits and opportunities of cooperation between government and the private sector, and among governments internationally, as well as best practices from around the world. The discussions all occur in a confidential environment to foster an open dialogue.[2]

Footnotes

1 "United States Activities to Improve Cybercrime Legislation and Investigative Capacities." March 20, 2006.

2 Meridian 2006 Website, http://www.meridian2006.org/index.php?page=1, accessed April 4, 2007.

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)

February 28, 2008

Table of Contents

Executive Summary

The President's National Security Telecommunications Advisory Committee (NSTAC) performed an evaluation in response to a White House request for commercial communications industry findings on the commercial communications infrastructure's reliance on the Global Positioning System (GPS). To gain current perspectives on the industry-wide use of GPS, the NSTAC solicited information from its members, other providers within the industry, and several external subject matter experts. Specifically, the NSTAC requested information on: (1) company and industry segment use of and reliance on GPS signals; (2) impacts to networks and operations that would result from loss or degradation of GPS signals; and (3) specific strategies implemented or planned to mitigate the impact of any GPS signal loss or degradation.

A broad cross-section of the commercial communications industry submitted feedback, including responses from individual companies in the telecommunications, computer software/services, and aerospace and defense sectors, and from industry trade associations. As a result of the evaluation, the NSTAC developed several findings and a recommendation for White House review and consideration.

This evaluation focuses narrowly on the commercial communications industry's use of and reliance on GPS, in accordance with White House direction to tailor the effort to enable a quick response. The NSTAC notes that reliance on GPS signals in military, maritime, aviation, and other civil environments varies widely depending on the specific use and application. GPS-based precision-guided munitions, maritime harbor approach and constricted waterway navigation, and aviation approach and landing are examples of critical applications with varying positioning, navigation, and timing (PNT) requirements supported by GPS. While instructive in understanding overall GPS deployment trends and vulnerabilities, non-commercial information was not evaluated or integrated into the NSTAC's findings, as that area was deemed to be outside the scope of this effort. The NSTAC looks forward to ongoing engagement with the White House staff and offers its continued support to national security telecommunications policy development and program planning.

Study Findings and Recommendation

The U.S. Government's commitment to provide and maintain civil space-based PNT services, such as GPS, free of direct user fees for civil, commercial, and scientific uses has encouraged the rapid adoption of GPS-based solutions throughout the commercial communications industry. In today's environment, GPS supports a broad range of commercial communications industry functions and applications; the primary use of GPS in each industry segment is in support of the networks' precise timing and synchronization requirements. Companies have selected and widely implemented GPS-based solutions primarily because GPS provides an inexpensive, globally-available, and highly reliable Stratum 1-quality reference source. As the commercial communications network infrastructure continues to evolve toward a high-speed all-digital environment, accurate timing and synchronization functions that support the infrastructure are becoming more critical.

Another important use of GPS is support to wireless location-based services, including support of wireless Enhanced 911 (E911) Phase II requirements. As the overall market for GPS-based devices and services continues to grow, the commercial communications industry is likely to identify and utilize additional uses of GPS to increase productivity, service delivery, and the number of available end-user applications.

Because of the fundamental role that GPS plays in supporting the commercial communications infrastructure, industry employs a range of strategies to mitigate the impact of GPS loss or disruption. To protect critical functions such as network timing and synchronization, companies proactively employ multiple layers of backup capabilities, mitigation strategies, and contingency plans to ensure protection against a wide range of potential GPS outage or disruption scenarios. At critical nodes in the infrastructure, redundant Stratum 1-level sources are deployed and protected automatically by secondary and tertiary backup capabilities and

alternate timing sources. All major carriers adhere to extremely rigorous industry-standard requirements for network timing synchronization.

Technological, economic, and regulatory considerations necessarily factor into individual company decisions on how to mitigate the potential impact of GPS loss. Companies must consider available equipment types and cost, the required level of quality and precision, the failure or disruption tolerance of the underlying service/application, the desired level of redundancy, and the likelihood of GPS disruption and potential impact. As a result, while backup solutions and processes are universally implemented within the industry, specific implementations vary widely both within a particular industry segment, and across industry segments.

Because automatic backup capabilities and other safeguarding/mitigation strategies are widely available and implemented, short-term loss or disruption of GPS will have minimal impact on the commercial communications infrastructure and its operations. One important exception is that short-term loss or disruption of GPS signals will affect the ability to determine accurate location information for wireless E911 purposes.

The specific consequences of medium- to long-term loss or disruption of GPS will vary based on a number of factors, including the specific function or application being supported by GPS, the duration of the loss/disruption, the geographic size of the affected region, and the availability and implementation of effective backup capabilities and contingency plans. Feedback from the study generally indicates that the wireline network infrastructure, including wireline components of wireless, satellite, cable, and broadcast networks, will sustain operation automatically for approximately 30 days. Network performance would be closely monitored, as it is still possible for performance to be impacted during this time period. For other components, the impact of long-term GPS loss varies. For example, in the wireless network environment, the ability to hand calls off between code division multiple access-based cell sites will begin to be affected after 24 hours. In the satellite, cable, and broadcast network environments, service-specific impacts unique to those environments could occur (*e.g.*, experiencing delay in the time to acquire satellite lock, reverting to the manual recording of radio frequency signal leakage by cable network operators, experiencing In Band On Channel/Hybrid Definition radio transmission degradation in the broadcast environment).

In the extremely unlikely event of a complete and catastrophic loss of GPS over an extended period of time (*e.g.*, more than one month) and affecting a large geographic area (*e.g.*, nationwide, continental, global), overall impact is more difficult to ascertain. Because of the diverse and highly distributed implementations of GPS-based solutions across the industry, any impact likely would be experienced in the form of a gradual degradation of network performance, with little potential for cascading network failures. Additional backup capabilities, processes, and mitigation approaches can and will be used to sustain network operation beyond this period; however, mitigation of an extended and complete loss of GPS would require costly reconfiguration of the network to redistribute alternative timing sources. Such a reconfiguration would require a cooperative effort between carriers.

The NSTAC also emphasizes that commercial communications networks do not operate in a vacuum, and service providers and network operators will take immediate corrective actions in response to any size event, particularly a large-scale catastrophic event with the potential to degrade the network. Even before all automatic means of backup are exhausted, companies will have already executed contingency plans and performed manual reconfigurations and network timing adjustments as required to maintain network operation.

Overall, industry members surveyed believe that their companies have taken measures to safeguard against those disruptions to the GPS signal that are likely to be encountered; however, to date, no industry or Government exercise has sought to replicate the impact of a long-term or permanent GPS outage simultaneously on all industries. The NSTAC recommends that the President direct the Department of Homeland Security and the Department of Defense

to include various GPS outage scenarios in future planned disaster recovery exercises in coordination with the commercial communications industry.

1 Background and Purpose

In response to a January 2003 request from the Director, National Security Space Architect, the President's National Security Telecommunications Advisory Committee (NSTAC) reviewed and assessed policies, practices, and procedures for the application of infrastructure protection measures to commercial satellite communications systems used for national security and emergency preparedness communications. Specifically, the NSTAC reviewed applicable documentation addressing vulnerabilities in the commercial satellite infrastructure and identified potential policy changes that would bring the infrastructure into conformance with a standard for mitigating those vulnerabilities. As a part of its review, the NSTAC also considered Global Positioning System (GPS) timing capabilities and developed initial findings and a recommendation for further study of GPS-related issues. The results of this effort were published in the *NSTAC Satellite Task Force Report*, March 2004.

At the 2007 NSTAC Meeting, Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism, requested that the NSTAC begin a scoping effort to further evaluate the commercial communications infrastructure's reliance on GPS. Ms. Townsend called for the NSTAC to present its findings and recommendations for White House evaluation.

In response to this request, the NSTAC formed a working group comprised of industry and Government representatives to review findings from the March 2004 study and examine the commercial communications reliance on GPS, as well as the possible impacts that loss or disruption of GPS could have on the commercial communications industry, including its reliance on GPS for synchronizing local timing clocks. This response presents the NSTAC's findings for White House review and consideration.

2 Approach and Scope

The study approach and scope for this effort are briefly discussed below.

2.1 Approach

Representatives of NSTAC member companies, subject matter experts (SME) from non-NSTAC commercial communications companies, trade associations, Government participants, and GPS technical experts contributed to this effort. To gain a broad understanding of the use of and reliance on GPS within the commercial communications industry, the NSTAC invited SMEs from the Government, private sector, and academia to present briefings. The NSTAC also reviewed previous studies, including the March 2004 *NSTAC Satellite Task Force Report* findings on GPS vulnerabilities in the commercial satellite infrastructure and the findings and recommendations of the August 2001 *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, prepared by the Volpe National Transportation Systems Center. Appendix A provides a list of working group members, Government personnel, and other participants.

To gain current perspectives on the industry-wide use of GPS, the NSTAC solicited information from its members as well as representatives of the Department of Homeland Security (DHS) National Coordinating Center-administered Telecommunications Information Sharing and Analysis Center. Specifically, the NSTAC requested information on: (1) company and industry segment use of and reliance on GPS timing and precision location signals; (2) impacts to networks and operations that would result from loss or degradation of GPS signals; and (3) specific mitigation strategies implemented or planned to minimize the impact of any GPS signal loss or degradation.[1]

A broad cross-section of the commercial communications industry submitted feedback, including responses from individual companies in the telecommunications, computer software/services, and aerospace and defense industry sectors, and from industry trade associations. The NSTAC presents its findings in this document and looks forward to continued engagement with the White House staff to support ongoing national security telecommunications policy development and program planning.

2.2 Scope

This study focuses narrowly on the commercial communications industry's use of and reliance on GPS, in accordance with White House direction to tailor the effort to enable a quick response. Deliberations with SMEs and evaluation of previous studies included information involving GPS uses and applications to military, maritime, aviation, and other civil environments. While instructive in understanding overall GPS deployment trends and vulnerabilities, non-commercial information was not evaluated or integrated into the NSTAC's findings, as that area was deemed to be outside the scope of this effort.

In soliciting information and perspectives from commercial communications industry representatives and the larger SME community, the NSTAC specifically requested that data submitted for the analysis be non-proprietary and unclassified. The findings documented in this response are generally applicable across all industry segments and represent NSTAC member company consensus. However, it is important to note that the study analysis revealed significant variance in the use of and reliance on GPS across industry segments and across companies within each industry segment. Feedback from individual companies likewise indicated that a wide variety of strategies, techniques, and implementation approaches are applied to mitigate the impacts of GPS loss or disruption, reflecting company-specific business case and risk assessment determinations.

3 Commercial Communications Reliance on GPS

This section describes the commercial communications reliance on GPS. Section 3.1 discusses the use of and reliance on GPS, including applications and dependencies specific to the wireline, wireless, satellite, cable, broadcast, and corporate/enterprise network environments. Section 3.2 generally characterizes the impact of loss or disruption of GPS for each network environment. Section 3.3 identifies associated strategies, employed or planned by industry, to mitigate GPS-related impacts.

3.1 Use of GPS

GPS is a U.S. Government-owned utility that provides users with positioning, navigation, and timing (PNT) services. The U.S. Air Force operates the space and control segments, consisting respectively of the GPS satellite constellation and the worldwide control stations that maintain the satellite orbits and adjust the satellite clocks. The user employs GPS receiver equipment to receive signals from the satellites and calculate the user's location. Using the signals to measure the distances to at least four satellites simultaneously, a GPS receiver can determine three-dimensional position (latitude, longitude, and altitude) while synchronizing its clock with the GPS precise time standard.[2] The GPS constellation, illustrated in Figure 1, consists of a minimum of 24 satellites in one of six medium-earth orbits, approximately 20,000 kilometers above the earth's surface.[3]

The U.S. Department of Defense (DOD) began development in the 1970s of what would become the GPS system. However, the first U.S. pronouncement regarding civil use of GPS came in 1983 following the downing of Korean Airlines Flight 007. The Soviet Union shot down the airplane after it strayed over Soviet territory; afterwards, President Reagan announced that GPS would be made available for international civil use once the system became operational.

The first major success of GPS came in 1990-1991, during Operation Desert Storm. DOD's needs during the crisis sparked a surge in the GPS market, which had barely existed just a few years prior to the war. Desert Storm provided a showcase for all the military uses of GPS—from helping soldiers navigate across the desert to vastly improving targeting capabilities of artillery and bomber units. Following the war, GPS device sales to non-DOD customers surged, and U.S. commercial GPS manufacturers continue to produce new and cheaper receivers that are used across numerous industries and infrastructures.[4]

On December 8, 2004, the President established a new national *U.S. Space-based Positioning, Navigation, and Timing Policy* containing guidance and implementation actions for space-based PNT programs, augmentations, and activities for U.S.

national and homeland security, civil, scientific, and commercial purposes.[5] In the policy, the U.S. Government pledged to provide on a continuous, worldwide basis, civil space-based PNT services free of direct user fees for civil, commercial, and scientific uses. The policy also established an Executive Committee that is charged in part with ensuring that efforts to deny hostile use of any space-based PNT services will not unduly disrupt civil and commercial access to civil PNT services outside an area of military operations, or for homeland security purposes.

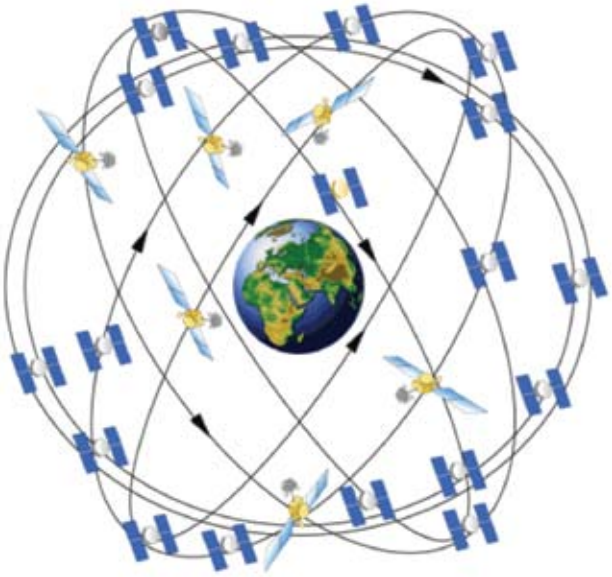

Figure 1 GPS Constellation[6]

Although DOD controls and maintains the GPS, and makes the service available to U.S. and allied armed forces, there is also a large civilian component in the user community. The Department of Transportation is responsible for overseeing all civil uses of GPS, which has become integral to navigation for aviation, ground, and maritime operations. Emergency responders depend upon GPS for location and timing capabilities in their life-saving missions. Banking, mobile phone operations, and the control of power grids are facilitated by the accurate timing provided by GPS. Farmers, surveyors, and geologists use the free and open GPS signals to pinpoint locations.[7]

Commercial communications companies have selected and widely implemented GPS-based network timing and synchronization solutions primarily because GPS provides an inexpensive, globally-available, highly reliable, and extremely accurate reference timing source. The U.S. Government's commitment to provide and maintain civil space-based PNT services, such as GPS, has also encouraged rapid adoption of GPS throughout the commercial communications industry. The use of GPS-disciplined oscillators (GPSDO), implemented extensively throughout the industry, is a cost-effective solution able to meet the various stringent network performance requirements for time and frequency. The use of and reliance on GPS in the wireline, wireless, satellite, cable, broadcast, and enterprise network environments are further described below.

Wireline Network Environment. GPS signals in the wireline network environment are fundamentally used as a primary reference timing source for a diverse range of telecommunications network equipment, including wireline switching offices, Synchronous Optical NETwork (SONET) and Synchronous Digital Hierarchy (SDH) nodes, multiplexer and demultiplexer equipment, digital cross connects, and customer premise equipment (*e.g.*, private branch exchanges [PBX]). GPS is also used as a reference timing source for other industry segment wireline-connected network elements, including mobile switching centers (MSC), satellite network control and earth station equipment, and other core cable network and broadcast network elements.

In addition to provision of a primary time reference, GPS signals also are used to support essential network time, frequency, and phase synchronization functions. Digital telecommunications networks require highly reliable precision frequency and timing information to maintain data integrity and guarantee the delivery of high quality services. Timing impairments, or "slips," can cause impacts to service quality such as increased noise or "pops" during voice calls, loss of picture content during facsimile transmission, inefficient retransmission of data packets, and video content "drop out" and "freeze frame" occurrences. More severe impacts resulting from timing and synchronization impairments include dropped calls/connections, the inability to initiate/receive calls and establish/maintain connections, the loss of circuit or transmission path integrity, and eventual network element isolation and/or placement in an "out of

service" condition. As the commercial communications network infrastructure continues to evolve toward a high-speed all-digital environment, accurate timing and synchronization functions that support the infrastructure are becoming more critical.[8]

In characterizing their use of and reliance on GPS, companies across industry segments (*e.g.*, wireless, satellite, cable, and broadcast) note the associated wireline network reliance on GPS as a potential factor in their own reliance on GPS. Network interconnections (*e.g.*, network interface points) and leased lines used to connect internal network elements are examples of underlying wireline components whose operation may have a dependence on GPS.

Wireless Network Environment. GPS is used to provide the highly accurate timing source required to synchronize mobile phones to the cellular network and to synchronize cellular network elements to one another. Radio carrier frequencies must also be synchronized precisely in order to prevent co-channel interference (*i.e.*, cross talk) and other radio frequency (RF) interference problems. For code division multiple access- (CDMA) based networks in particular, precise frequency synchronization is required to support handoff of calls between cell sites.

Another important use of GPS in the cellular network environment is in support of location-based services, including support of Enhanced 911 (E911) Phase II requirements. To comply with the Federal Communications Commission's (FCC) wireless E911 requirements, wireless carriers require accurate positioning information to provide the precise locations of wireless network callers so that police, fire, and emergency rescue personnel can be dispatched quickly.[9]

GPS also provides Time-of-Day information to support several cellular network functions including setting clock time on mobile devices and accurately time stamping billing records and data packets for network and service performance measurement. Feedback from industry also identified internal company use of wireless network services (*e.g.*, use of cellular and paging services by company employees and contractors) as a potential peripheral reliance on GPS. Internal communications may be disrupted if these wireless network services become unavailable due to loss of GPS.

Satellite Network Environment. In the satellite industry, use of GPS signals is fundamental in providing timing reference and synchronization across satellite constellations and satellite network elements. In addition to timing synchronization, satellite network operators use GPS signals broadly in support of telemetry, tracking, and control (TT&C) time tracking and ranging operations as well as frequency referencing for many applications. Most land earth stations (LES) use GPS as a primary means to set the internal station frequency standard and clocks, and central satellite control systems use GPS as a master clock timing reference. Fixed satellite-based communications terminals also use GPS for geo-location and a timing reference. GPS capabilities enable terminals to quickly locate and acquire a satellite. Terminals may also use GPS to synchronize the terrestrial communications equipment with which they interface, providing consistent data flow throughout the link. Some satellite terminals that use complex spread spectrum waveforms rely heavily on GPS for system synchronization.

Cable Network Environment. The cable television industry also relies on GPS time signals as a primary timing reference for several network infrastructure components, including Building Integrated Timing Supply (BITS) clocks, Network Time Protocol (NTP) server deployments, Data Over Cable Service Interface Specification (DOCSIS) timing interface servers, and interconnecting or supporting wireline and wireless network elements (*e.g.*, time-division multiplexing [TDM] circuits, T1 emulation circuits, microwave radio links). NTP servers are used by cable operators in support of the following: synchronization across cable system equipment such as servers, routers, switches, and terminal equipment (*e.g.*, cable modems); time stamps in simple network management protocol tables and local logging for error and event correlation; set-top boxes, which use time information for use in electronic program guides, reliable content recording, and in processing Emergency Alert messages; and service applications such as video-on-demand (VOD)

and Ad Insertion systems. Additionally, pursuant to FCC regulations, cable operators routinely monitor their systems for RF signal egress or "leakage," using signal leakage detection equipment that utilizes GPS location signals to automate the process of locating and repairing signal leaks.

Broadcast Network Environment. GPS-based systems are widely employed by broadcast radio and television (TV) stations. GPS provides precise timing and phasing references for equipment throughout the broadcast production and transmission chain. GPS is used as frequency reference for both analog and digital television transmitters. This is particularly important in the proper implementation of "Precision Off-Set," which is used to ensure that a digital TV (DTV) transmitter will not interfere with an analog transmitter operating on the same channel. In addition, single frequency TV networks recently have been approved for use by the FCC and are just beginning to be deployed in the U.S. This technology, called Distributed Transmission, relies heavily on GPS to ensure that all the transmitters in the network remain synchronized.

GPS is used to support the proper synchronization of digital radio transmitters. The U.S. In-Band-On-Channel (IBOC) digital transmission technology, also known as Hybrid Digital (HD) radio, overlays digital carriers onto an FM station's analog signal and relies on precise timing to ensure that the digital signal does not degrade those analog transmissions.

In both radio and TV production studios, GPS is used as the reference for the master clock system, which ensures that all the clocks in the studio increment their second hands simultaneously and remain locked to the same time. GPS is also used to derive master timing reference signals, which are required in a broadcast production system to keep audio and video in synchronization, to ensure that automation systems are time-aligned, and to meet the various requirements for broadcast standards compliance.

Enterprise Network and Corporate Operations Environment. Feedback from the commercial communications industry also identifies use of and reliance on GPS signals to support company-internal enterprise network operation as well as corporate operation functions. For example, one company cites use of GPS timing *via* NTP servers for synchronization of all device timing (*e.g.*, timing for switches, routers, servers, and desktops) on its global corporate network. Multiple GPS receivers feed timing data to distributed NTP servers, which synchronize their clocks to the GPS-provided time reference on a periodic basis. Network and computing resources then access the NTP servers for timing. The company also cites use of GPS timing to synchronize its internal SONET infrastructure. Regarding corporate operations, several companies cite extensive use of communications services (*e.g.*, cellular and paging services, satellite phone service, use of personal communications devices such as Blackberry® devices) by employees and/or contractors while performing their jobs. Availability of these communications services may be impacted by a GPS loss or disruption. GPS equipment vendors also utilize the GPS signal during product development, testing, and production.

In support of workforce and resource management functions, GPS signals are used across the industry by field operations staff to more effectively coordinate service and maintenance activities. For example, in support of the cable industry's field service, plant maintenance, and auditing activities, company vehicles may utilize GPS signals as a part of intelligent automated vehicle fleet management systems. Another cited example of use of GPS positioning data is a disaster recovery and employee location mapping capability used by the company in the event of a regional incident. GPS location information is also used by some companies to support industry functions such as fiber locating operations (or "call before you dig" operations) and other field test and measurement functions. As the overall market for GPS-based devices and services continues to grow, the commercial communications industry is likely to identify and utilize additional uses of GPS to increase productivity, service delivery, and the number of available end-user applications. Table 1 lists some examples of the commercial communications industry's uses of and reliance on GPS signals.

Network Environment	Application/Use
Wireline	▶ Time/frequency reference source (*e.g.*, central offices [CO], SONET, TDM circuits, digital access and cross-connect (DAC) systems, termination equipment, voice switches) ▶ Network timing/synchronization ▶ Workforce and Resource Management
Wireless	▶ Time/frequency reference source (*e.g.*, wireline elements, MSCs, cell sites, HLR/VLRs, mobile devices) ▶ Network timing/synchronization (network element-to-network element, mobile phone-to network, RF carrier frequency sync) ▶ CDMA mobile unit handoff ▶ E911 Phase II and location-based services ▶ Time-of-Day functions (clocks on mobile units, timestamp for billing and performance measurement) ▶ Workforce and Resource Management
Satellite	▶ Time/frequency reference source (*e.g.*, satellite network ground segment elements, land earth stations, TDM circuits, satellite terminals) ▶ Network/Application timing and synchronization ▶ TT&C time tracking and ranging operations ▶ Workforce and Resource Management
Cable	▶ Time/frequency reference source (*e.g.*, switches, routers, NTP server deployments, DOCSIS timing interface servers, cable modems, set-top boxes) ▶ Network timing and synchronization ▶ Set-top box use (electronic program guides, content recording, alert message processing) ▶ Service applications (VOD, Ad Insertion systems) ▶ RF signal leakage detection ▶ Workforce and Resource Management
Broadcast	▶ Time/frequency reference source (*e.g.*, broadcast production/distribution facilities, digital TV "Precision Off-Set") ▶ Network timing and synchronization (*e.g.*, DTV, IBOC/HD radio) ▶ Broadcast audio/video synchronization ▶ Time alignment for Automation systems ▶ Per occasion Applications (*e.g.*, remote broadcasting) ▶ Workforce and Resource Management
Enterprise / Corporate Operations	▶ Timing/frequency reference source ▶ Network and device timing and synchronization (SONET, servers, routers, switches, desktops) ▶ Fiber locating ▶ Workforce and resource management ▶ Development and production of GPS equipment and devices

Table 1 Examples of GPS Use and Reliance

Key findings regarding the commercial communications industry's use of and reliance on GPS are:

- The U.S. Government's commitment to provide and maintain civil space-based PNT services, such as GPS, free of direct user fees for civil, commercial, and scientific uses has encouraged rapid adoption of GPS throughout the commercial communications industry.
- GPS supports a broad range of commercial communications industry functions and applications in many commercial communications industry segments (*e.g.*, wireline, wireless, satellite, cable, and broadcast network environments).
- The primary use of GPS in the commercial communications industry and across all commercial communications industry segments is the support of precision timing and network synchronization functions.
- Another important use of GPS signals is support to location-based services, including support of wireless E911 Phase II requirements.
- As the commercial communications network infrastructure continues to evolve toward a high-speed all-digital environment, accurate timing and synchronization functions that support the infrastructure are becoming more critical.
- As the overall market for GPS-based devices and services continues to grow, the commercial communications industry is likely to identify and utilize additional uses of GPS to increase productivity, service delivery, and the number of available end-user applications.

3.2 Impact of Loss or Disruption of GPS

In its 2004 study, the NSTAC found that "impacts of a loss of GPS could be seen across all aspects of the telecommunications industry…on wireline and wireless networks…[and] fiber optic and broadband transmission systems; radio, television, and cable broadcast systems; and satellite systems–all of which use GPS to some extent for synchronizing local timing clocks." Industry submissions in this GPS study generally confirm this finding and further substantiate specific impacts of GPS loss or disruption within each industry segment.

Generally, feedback indicates that short-term loss or disruption of the GPS signals for timing will have minimal impact on the commercial communications infrastructure and its operations. One important exception is that short-term loss or disruption of GPS signals will affect the ability to determine accurate location information for wireless E911 purposes. The impact of medium- to long-term loss or disruption of GPS will vary based on a number of factors, including the specific function or application being supported by GPS, the duration of the loss/disruption, the geographic size of the affected region, and the availability and implementation of effective backup capabilities and contingency plans.

Specific impacts of GPS loss in the wireline, wireless, satellite, cable, broadcast, and enterprise network environments are described below. Additional details on strategies for mitigating the impacts of GPS loss are presented in Section 3.3.

Wireline Network Environment. In the case of a short-term complete GPS loss or a long-term localized GPS loss, carriers indicate that the impact on wireline network operation is minimal due to the availability and use of backup systems and processes, alternative timing sources, and effective business continuity planning.[10] The most commonly-cited potential impact in the wireline network environment is the eventual loss of network timing and synchronization as a result of a long-term complete loss or disruption of the GPS timing signal across an extended area. Wireline carrier feedback indicates that wireline network infrastructure (*e.g.*, circuit switches) will sustain operation automatically for approximately 30 days. Network performance would be closely monitored, as it is still possible for performance to be impacted during this 30-day window. Secondary and tertiary backup capabilities and other mitigation processes can and will be used to sustain network operation beyond this period. Carriers also note that mitigation of an extended and complete loss of GPS

beyond this period would require costly reconfiguration of the network to redistribute alternative timing sources. Such a reconfiguration would require a cooperative effort between carriers. It should be noted that such an event, resulting in complete loss of GPS for an extended time and over a large geographic area, has never occurred.[11] Additionally, no industry or Government exercises have sought to replicate the impact of a long-term or permanent GPS outage simultaneously on all industries.

CO timing signal generator (TSG) systems provide a common source for frequency and phase alignment of all network elements operating in the CO building. This synchronization is essential for interoperability of digital transmission networks. The TSG receives timing from a highly accurate GPS primary reference source (PRS), cesium PRS, or Stratum 1-traceable timing delivered *via* an interoffice facility. These timing systems provide a robust, simple-to-administer, and trouble-free network of clocks of known quality and performance characteristics. Reliable clocks ensure that network synchronization provides the necessary level of performance demanded by a growing digital network.

The hierarchy of clock requirements is grouped into four stratum levels, as defined by the American National Standards Institute (ANSI) T1.101 standard.[12] The standard defines the minimum performance requirements for telecommunications network synchronization and timing requirements for each stratum level, as shown in Table 2.

- Stratum 1 is the highest quality level in the clock hierarchy. Stratum 1 clocks are defined as autonomous sources, requiring no input from another source. In order to meet interface standards, all digital signals must be under the control of a clock or clocks traceable to a Stratum 1 source. Stratum 1-level timing sources, typically atomic oscillators (*e.g.*, cesium beam) or GPSDOs, are specified to have a maximum "drift" of 1×10^{-11}. As shown in Table 2, T1 carrier cycle slips can be expected to occur only once every 72.3 days, worst case, if Stratum 1-quality clocks are used.

- Stratum 2 and lower-level clocks require input and adjustment from a higher stratum-level clock. Stratum 2 clocks are typically used as the master TSG oscillator at critical network sites. Stratum 2 TSG systems employ rubidium oscillators for extended holdover capability.

- Stratum 3E clocks are used as the master TSG oscillator at other locations in the network that are not Stratum 2 equipped. The Stratum 3E level was defined as a result of the widespread deployment of SONET transport and the associated need for enhanced phase filtering capabilities. Stratum 3 clocks are used in digital switches, DACs, and SONET network elements.

- Stratum 4 clocks are found in distribution facilities (*e.g.*, channel banks) and end-user switching equipment (*e.g.*, PBX).

Stratum Levels	Stratum 1	Stratum 2	Stratum 3E	Stratum 3
Frequency accuracy, adjustment range	1×10^{-11}	1.6×10^{-8}	1×10^{-6}	4.6×10^{-6}
Frequency stability	NA	1×10^{-10}	1×10^{-8}	3.7×10^{-7}
Pull-in range	NA	1.6×10^{-8}	4.6×10^{-6}	4.6×10^{-6}
Time offset per day due to frequency instability	0.864 µs	8.64 µs	864 µs	32 ms
Interval between cycle slips	72.3 days	7.2 days	104 minutes	169 seconds

Table 2 Stratum Clock Hierarchy and Timing Accuracy Requirements[13]

It should be noted that every network element and every clock is effectively operating at the Stratum 1 level when the timing hierarchy is intact. The stratum level of subtending clocks only becomes a factor when the timing distribution chain is disrupted, and the holdover characteristics of the oscillators come into play.

In the event of a complete loss of GPS signals, the wireline synchronization network is designed to fall back on internal network clocks, such as cesium PRS systems and rubidium and crystal oscillators, used for extended holdover capability. As Stratum 1-level clocks, cesium PRS systems are autonomous timing sources, equal in quality to a GPS-derived timing signal. Due to cost considerations, cesium PRS systems generally are only deployed at critical network sites.

For locations that receive their timing reference from a GPS PRS, extended loss of GPS would eventually cause the oscillator in the TSG to enter holdover status. Once in holdover, the oscillator in the TSG can maintain accurate frequency timing for a period dependent on the type of oscillator. For a Stratum 2 rubidium oscillator, network performance will be maintained for about thirty days. For a Stratum 3E crystal oscillator, network performance will be maintained for seven to ten days.[14] Once the holdover capability of the TSG oscillator is exceeded, these clocks would begin to "drift" away from a common frequency, and network elements would gradually lose synchronization with one another.

Service providers also cite the use of available external timing reference sources as a means to establish an accurate time reference (*e.g.*, geographically diverse and redundant GPS-based devices, a backup precision timing reference source such as the LORAN-C signal, reconfiguration to "line time" off an interconnected network). Approaches to timing and synchronization backup (*e.g.*, the types and order of secondary and tertiary backup sources employed) vary by service provider; however, all major carriers adhere to Telcordia standards for timing synchronization.[15]

As noted in the 2004 NSTAC study, a general approach in the public switched telephone network (PSTN) is to deploy a Stratum 1 timing source to every CO through a combination of cesium PRS systems, GPS-based solutions, and interoffice distribution of Stratum 1-traceable timing references.[16] Cost remains a primary factor in selecting a solution. For example, the cost of a cesium-based solution typically exceeds that of a GPS-based solution by about $20,000. Interoffice distribution of timing references is the least capital-intensive solution, but requires extensive planning and maintenance to ensure proper execution.

In summarizing impact to the wireline network, carrier feedback indicates that the wireline network infrastructure (*e.g.*, circuit switches) will sustain operation automatically for approximately 30 days in the event of complete loss of GPS signals. Network performance would be closely monitored, as it is still possible for performance to be impacted during the 30-day window. Additional backup capabilities, processes, and mitigation approaches can and will be used to sustain network operation beyond this period. However, mitigation of an extended and complete loss of GPS would require costly reconfiguration of the network to redistribute alternative timing sources. Such a reconfiguration would require a cooperative effort between carriers.

Wireless Network Environment. Long-term GPS timing signal loss or degradation could impair wireless network timing and synchronization. GPS is utilized in wireless network synchronization and provides a precise timing and frequency reference source for cell site radio controllers, MSCs (and interconnected wireline switching offices), and other wireless network elements. All of these network elements have backup internal and/or external timing sources, but if the GPS clock source is lost or disrupted, the internal timing sources will begin to drift from component synchronization at a rate based upon the class/type of clock implemented, and the timing error will build proportionally over time during which the reference source is unavailable. The error rate will build over time, and hard failures will manifest themselves randomly once the clocks drift outside of the system synchronization thresholds.

Wireless network operators report that the cell sites in an affected area likely would be the first cellular network elements to begin to drift, as their internal clocks

typically guarantee only 24 hours of highly accurate holdover time. Beginning after 24 hours and as the timing of the cell sites drifts apart from one another (due to the lack of a common time reference), handoffs between cell sites would begin to fail, and cell sites would start to become isolated from the other cell sites in the network; however, in this scenario, cell sites would still be able to communicate with the MSC, and calls could still be originated from subscriber phones.

The wireline components of cellular networks can be expected to perform as discussed in the wireline network environment section above. For example, the lack of synchronization between MSCs would begin to result in "slips" on digital inter-office circuits/elements, eventually affecting circuit integrity between MSC locations and resulting in communication issues and data loss between network offices. It is likely that cellular telephone customers would initially experience temporary minor communication issues (*e.g.*, pops, clicks, and data loss), which would worsen until the connection to the cell site was effectively out of service.

One wireless service provider noted that even though the company's time reference is maintained with multiple high quality reference time sources, communication with network elements external to the company would also depend upon the ability of those external elements to maintain an accurate time reference. Another wireless service provider stated that, in the event of long-term loss or disruption of GPS, its wireline portion of the network would likely remain operational indefinitely due to redundant backup capabilities (*i.e.*, external Stratum 1-quality timing source as a primary backup and rubidium-based oscillators as a secondary backup).

In addition to timing and data synchronization impacts, loss or degradation of GPS-based positioning information would critically impact wireless Phase II E911 and commercial location-based services. These services would immediately suffer from the inability to gather precise ranging measurements from satellites currently in the visible horizon during a GPS outage. Having fewer operational satellites in the GPS constellation or being out of the range of the receiving site would result in fewer possible location measurement points, making the determination of a highly accurate position estimate more difficult or impossible.[17] Strategies to mitigate the impact of loss of GPS-based location data are further discussed in Section 3.3. Other impacts of GPS loss in the wireless network environment include loss of Time-of-Day data that could affect billing and measurement systems' accuracy.

In summarizing the impact on wireless networks, carrier feedback indicates that the first network elements likely to be affected are cell sites, which will sustain operation for at least 24 hours. After this time period, the ability to hand calls off between cell sites will be affected, although calls can still be originated from subscriber phones as communications with the MSC will not be affected. Wireline network elements generally will sustain operation automatically for up to 30 days, although wireless carrier estimates of this time period varied from five days to beyond 30 days.

Satellite Network Environment. The 2004 NSTAC study noted that "most satellite operators use GPS timing for TT&C time tracking, ranging operations, and timing synchronization." Current study responses concur with previous the NSTAC findings. In the event of complete loss of GPS, one satellite network operator notes that its GPS receiver equipment is able to operate independently for several days. After this time period, available backup cesium-standard clocks and stable clock generators would be used as input timing reference to the GPS receiver equipment. This approach offers a long-term solution until GPS-based satellite timing is restored. The satellite network operator notes that it also is investigating the potential for its equipment to accept an external Inter-Range Instrumentation Group (IRIG-H) signal to use for synchronization *via* the National Institute of Standards and Technology (NIST) WWVB signal.[18]

Another satellite network operator notes that the absence of GPS does not cause an immediate threat to commercial satellite fleets' health; however, the capability to monitor and control satellite fleets would degrade gradually. Backup timing synchronization can

be obtained from other sources such as NTP servers, but those servers may be dependent on GPS signals. Manual synchronization is also possible; however, it may prove unsustainable in the long term. One satellite service provider stated that failure of GPS "would be an inconvenience to the satellite control system" and would not result in loss of control.

LESs and satellite terminals are other satellite network elements whose operation may be impacted by GPS disruption. Most LESs use GPS to set the internal station frequency standard and clocks. They typically have atomic clocks for backup timing; however, one respondent noted that localized GPS anomalies may have to be resolved prior to backup initiation, resulting in a temporary outage. Some satellite user terminals require a GPS signal for location, spot beam designation and timing, while other user terminals may have access to platform navigation systems for timing. Other terminals do not require GPS or any external navigation system to function.

Another company response noted that satellite terminal designs are becoming increasingly dependent on GPS capabilities. When satellite terminals employ GPS receivers for geo-location, loss of GPS would impact the ability to quickly find, acquire, and track a satellite. Some fixed satellite-based communications terminals routinely use GPS to increase signal acquisition speed; a loss of the GPS signal would lengthen the acquisition time for an affected terminal.

The potential impact on fixed satellite-based communications terminal operation also can vary depending on terminal design and the underlying technology employed. For example, a simple frequency division multiple access terminal designed with a rubidium-based backup solution could operate almost indefinitely without GPS timing. However, satellite terminals that use more complex spread spectrum waveforms may be more dependent on accurate timing. A spread spectrum application that is not protected by an atomic frequency standard backup solution may suffer acquisition time degradation after only a few hours of GPS signal loss.

In summarizing feedback regarding the satellite network environment, network operators indicate that loss of GPS has minimal impact in the short term. Impacts of a long-term complete GPS loss will vary by company; backup capabilities and processes are available and will be used to mitigate potential impacts.

Cable Network Environment. The cable industry's wireline network infrastructure would be subject to the same wireline-associated impacts of GPS loss or disruption as previously described. The lack of GPS time signals for a prolonged time period would result in frame slips for TDM circuits, T1 emulation, and SONET systems, which would eventually impact the ability for these circuits and networks to carry traffic without some degradation. The lack of GPS time signals would also potentially result in inaccurate clocks on NTP servers used for synchronization across network equipment, set-top boxes, cable modems, and service applications. Potential impairments include inaccurate electronic program guide data, incorrect billing of digital voice calls, and prolonged debugging of network errors due to the lack of synchronized clocks. Should cellular communications become unavailable due to loss or disruption of GPS, cable operations (*e.g.*, work force coordination and management) could be significantly impacted. The use of GPS signals in support of vehicle fleet management is in a nascent stage within the cable industry and impact on productively is likely minimal at this time; however, the loss of productivity may be greater in the future when cable operators have near real-time location information integrated into automated vehicle routing and dispatch systems.

Another associated cable industry impact of GPS loss or disruption is the inability of RF signal leakage detection equipment to automate the process of precisely locating the signal leak in a cable system. Manual recording of leakage locations can be used; however, that method is likely to be less accurate than the automated methods that utilize the GPS location signals, and may lengthen the time needed to repair the signal leak.

In summarizing feedback regarding the cable network environment, the cable network infrastructure dependent upon GPS time signals will sustain operation automatically for approximately 30 days in the event of complete loss of GPS signals. Beyond this period, some circuit termination equipment could be reconfigured to utilize the receive clock from the PSTN as a reference clock; however, this option may not be viable in the event of widespread GPS outage or degradation.[19]

Broadcast Network Environment. GPS is not critical to the operation of most broadcast systems. In the studio, most equipment components, including the master clock and timing reference signal generators, have their own internal oscillators, which are very stable. If GPS fails, this equipment can be set to "manual" or will automatically revert to the internal oscillators and will be able to operate for some time without drifting off frequency. The same is fundamentally true for digital and analog television transmitters. While they rely on GPS for synchronization and frequency reference, they also have very stable internal oscillators that will take over in the event that GPS fails.

The areas for which GPS is critical are: (1) "Precision Off-Set" between analog and digital television transmitters (this area will no longer be critical after February 2009 when full service analog TV transmitters permanently stop broadcasting as required by law); (2) IBOC transmitters, which may interfere with companion analog FM signals; and (3) Distributed Transmission networks for television, in which the loss of a full-time frequency and time reference at the transmission sites will result in the transmitters creating interference with each other.

In general, through use of internal reference sources, these systems can "flywheel" through a loss of GPS synchronization for an extended period of time.[20] The severity and frequency of intermittent failures of the transmitted signals is directly proportional to the precision tolerance of the internal references. Eventually, system failure can occur due to a loss of synchronization; however, the amount of time to system failure is not easily predicted as it is dependent on the stability of the oscillators in each part of the overall transmission chain.

Enterprise Network and Corporate Operations Environment. GPS disruption may impact the commercial communications industry's enterprise network operation functions through loss of enterprise network timing synchronization. For example, one responder noted that, in the event of an extended GPS disruption or failure, the NTP servers, which provide timing for switches, routers, servers, and desktops, would eventually experience a time shift from true time. Long-term results could include network and service outages, discrepancies in security logs, invalidated public key infrastructure certificates and tokens, and SONET infrastructure failure. Corporate operations functions may also be impacted as industry employees and contractors lose the ability to communicate *via* paging, cellular, and personal communications (*e.g.*, Blackberry® devices) services impacted by GPS disruption.

GPS disruption may also impact equipment vendor corporate operations with the loss of capability to use GPS broadcast signals while developing and manufacturing company products. This would interfere with product development efforts and subsequently increase development costs, delay product manufacturing and delivery rates, and increase the risk to product operational reliability. The loss or degradation of GPS broadcast signals during development would affect the ability to completely evaluate and test operational system capabilities before production.

In summary, key findings regarding the impact of loss or disruption of GPS are:

- Generally, short-term loss or disruption of the GPS signals for timing will have minimal impact on the commercial communications infrastructure and its operations.
- Short-term loss or disruption of GPS signals will affect the ability to determine accurate location information for wireless E911 purposes.

- The impact of medium- to long-term loss or disruption of GPS will vary based on a number of factors, including the specific function or application being supported by GPS, the duration of the loss/disruption, the geographic size of the affected region, and the availability and implementation of effective backup capabilities and contingency plans. For example:

  - In the event of complete loss of GPS signals, wireline carrier feedback indicates that wireline network infrastructure (*e.g.*, circuit switches) will sustain operation automatically for approximately 30 days. Network performance would be closely monitored, as it is still possible for performance to be impacted during the 30-day window. Additional backup capabilities, processes, and mitigation approaches can and will be used to sustain network operation beyond this period; however, mitigation of such an extended GPS loss would require costly reconfiguration of the network to redistribute alternative timing sources. Such a reconfiguration would require a cooperative effort between carriers.

  - In the event of complete loss of GPS signals, wireless carrier feedback indicates that the first network elements likely to be affected are cell sites, which will sustain operation for at least 24 hours. After this time period, the ability to hand calls off between cell sites will be affected, although communications with the MSC will not be affected. Wireline network elements generally will sustain operation automatically for up to 30 days, although wireless carrier estimates of this time period varied from five days to beyond 30 days.

  - Feedback from the satellite operators indicates that impacts of a long-term complete GPS loss will vary by company, and that backup capabilities and processes are available and will be used to mitigate potential impacts.

  - In the event of complete loss of GPS signals, feedback from the cable network operators indicates that the cable network infrastructure dependent upon GPS time signals will sustain operation automatically for approximately 30 days. Beyond this period, some circuit termination equipment could be reconfigured to utilize the receive clock from the PSTN as a reference clock; however, this option may not be viable in the event of widespread GPS outage or degradation.

  - Feedback from the broadcast industry indicates that GPS is not critical to the operation of most broadcast systems. Systems that may be affected by GPS loss include "Precision Off-Set" between analog and digital TV transmitters, HD Radio, and Distributed Transmission networks for television. For these systems, loss of GPS can be tolerated for "an extended period of time," although this time period is not easily predicted and requires further study.

- In the extremely unlikely event of a complete and catastrophic loss of GPS over an extended period of time (*e.g.*, more than one month) and affecting a large geographic area (*e.g.*, nationwide, continental, global), overall impact is more difficult to ascertain. Such an event has never occurred, and, to date, no industry or Government exercises have sought to replicate the impact of a long-term or permanent GPS outage simultaneously on all industries.

3.3 Mitigation Strategies

The commercial communications industry employs a range of strategies to mitigate the impact of loss or disruption of GPS. In all communications network environments, backup solutions are deployed at the most critical nodes to protect against the loss of a GPS-provided timing reference source. Generally, service providers and network operators select backup solutions and associated implementation approaches that are specifically designed to meet the requirements of the service/application. The selection of an alternative is also an economic and business case decision that must factor in available equipment types and cost, the required level of quality and precision, the failure or disruption tolerance of the underlying service/application, the desired level of redundancy, and the likelihood of impact. As a result, implementation

of backup solutions vary widely both within a particular industry segment, and across industry segments. For example, at critical nodes (*e.g.*, wireline COs, mobile switching centers, satellite control centers), redundant Stratum 1-level sources are often deployed and further protected by secondary and/or tertiary sources. For less critical applications (*e.g.*, the time of day on a desktop computer, some NTP server applications), less accurate timing sources may be sufficient (*e.g.*, internal quartz oscillators, internal central processing unit clocks in devices).

To protect commercial communications network elements, service providers, network operators, and vendors report a wide variety of safeguarding/mitigation approaches and contingency plans. Strategies cited to mitigate the impact of loss or disruption of GPS timing signals include:

- Use of external/internal precision cesium-based devices (*e.g.*, beam clocks and oscillators);
- Use of external/internal rubidium-based devices;
- Use of quartz oscillators;
- Use of multiple geographically dispersed GPS receivers;
- Automatic fall-over to other timing sources in the event of primary failure (*e.g.*, LORAN-C timing source);
- "Line timing" off other carriers' signals and "slaving" to the wireline carrier circuit blocking;
- Manual reconfiguration to receive clock timing from the PSTN;
- Manual reconfiguration to use ad hoc timing sources during an emergency;
- Use of other timing sources such as NTP servers or an IRIG source;
- Dependence on the internal free-running oscillator of the device; and
- Use of a combination of the above strategies.

Depending on the network service or application being protected, individual companies may choose to deploy primarily one type of strategy or a combination of strategies implemented in layers to provide secondary and tertiary levels of protection.

Wireless service providers cite use of terrestrial measurements as a secondary approach to locating wireless 911 callers in the event that GPS-provided location data is unavailable.[21] One service provider noted that terrestrial network measurements would be utilized until the mobile device can no longer communicate with more than one cell site. When the device is no longer able to communicate with more than one cell site, only network identification parameters and ranging measurements to the identified cell site would be utilized. Location determination solutions of this nature result are significantly less accurate than GPS-based measurements. Another wireless provider reported that no mitigation is available for E911 caller location information.

Responses from cellular service providers are also consistent with the NSTAC's previous examination of GPS and E911 geo-location. The 2004 report found that "wireless carriers typically use GPS assist technology as one means of providing the geo-location of a 911 caller. …Different carriers use combinations of GPS and triangulation to determine the location of a wireless caller with pinpoint accuracy." The report also noted that without a properly functioning GPS system, cell site triangulation can be utilized to deliver location information, but in many areas of the country, the geographic arrangement of cell sites make the process of triangulation difficult, if not impractical. As a result, "the loss of GPS could leave 911 centers without the ability to automatically receive the location of wireless callers to 911, thereby endangering life and property. …[This impact] would be most severe in areas with low density of cell sites, particularly rural areas and highways. Unfortunately, these are areas in which emergency rescue personnel typically most need precise location information because they must cover large areas."

In other network environments, strategies to protect against loss of GPS positioning data generally entail manual measurement and recording. For example, cable operators can fall back to the manual recording of RF signal leakage locations, which will be less accurate than automated methods that utilize GPS signals, and will lengthen the repair time for the cable leakage, resulting in less technical staff productivity.

Regarding strategies to mitigate workforce management impacts of loss or disruption of GPS, company employees and contractors would fall back to use of other existing forms of communication (*e.g.*, two-way radios, other carriers' services, email) should there be a GPS-related loss to primary communications modes. In the area of fleet vehicle management, one response noted that no effective alternatives exist to compensate for loss of location data as a result of loss or degradation of GPS; however, the impact on current operations is characterized as minimal. As GPS is more fully integrated into automated vehicle routing and dispatch systems, it is anticipated that companies will put in place backup processes and systems to compensate for GPS signal loss or disruption.

Key findings regarding mitigating the impact of the loss or disruption of GPS are:

- To protect critical functions such as network timing and synchronization, companies employ multiple layers of backup capabilities, mitigation strategies, and contingency plans to provide protection against GPS outages and disruptions.
- Technological, economic, and regulatory considerations necessarily factor into individual company decisions; therefore, specific mitigation strategies and backup capabilities will vary.

4 Summary

In evaluating the commercial communications industry's use of and reliance on GPS, the NSTAC finds that:

- The U.S. Government's commitment to provide and maintain civil space-based PNT services, such as GPS, free of direct user fees for civil, commercial, and scientific uses has encouraged the rapid adoption of GPS-based solutions throughout the commercial communications industry.
- GPS supports a broad range of commercial communications industry functions and applications in many commercial communications industry segments (*e.g.*, wireline, wireless, satellite, cable, and broadcast network environments).
- The primary use of GPS in the commercial communications industry and across all commercial communications industry segments is the support of precision timing and network synchronization functions.
- Another important use of GPS signals is support to location-based services, including support of wireless E911 Phase II requirements.
- As the commercial communications network infrastructure continues to evolve toward a high-speed all-digital environment, accurate timing and synchronization functions that support the infrastructure are becoming more critical.
- As the overall market for GPS-based devices and services continues to grow, the commercial communications industry is likely to identify and utilize additional uses of GPS to increase productivity, service delivery, and the number of available end-user applications.
- To protect critical functions such as network timing and synchronization, companies employ multiple layers of backup capabilities and other mitigation strategies to provide protection against GPS outages and disruptions.
- Technological, economic, and regulatory considerations necessarily factor into individual company decisions; therefore, specific mitigation strategies and backup capabilities will vary.
- Generally, short-term loss or disruption of the GPS signals for timing will have minimal

impact on the commercial communications infrastructure and its operations.

- Short-term loss or disruption of GPS signals will affect the ability to determine accurate location information for wireless E911 purposes.

- The impact of medium- to long-term loss or disruption of GPS will vary based on a number of factors, including the specific function and application being supported by GPS, the duration of the loss/disruption, the geographic size of the region being impacted, and the availability and implementation of effective backup capabilities. For example:

  - In the event of complete loss of GPS signals, wireline carrier feedback indicates that wireline network infrastructure (*e.g.*, circuit switches) will sustain operation automatically for approximately 30 days. Network performance would be closely monitored, as it is still possible for performance to be impacted during the 30-day window. Additional backup capabilities, processes, and mitigation approaches can and will be used to sustain network operation beyond this period; however, mitigation of such an extended GPS loss would require costly reconfiguration of the network to redistribute alternative timing sources. Such a reconfiguration would require a cooperative effort between carriers.

  - In the event of complete loss of GPS signals, wireless carrier feedback indicates that the first network elements likely to be affected are cell sites which will sustain operation for at least 24 hours. After this time period, the ability to handoff calls between cell sites will be affected, although communications with the MSC will not be affected. Wireline network elements generally will sustain operation automatically for up to 30 days, although wireless carrier estimates of this time period varied from five days to beyond 30 days.

  - Feedback from the satellite operators indicates that impacts of a long-term complete GPS loss will vary by company and that backup capabilities and processes are available and will be used to mitigate potential impacts.

  - In the event of complete loss of GPS signals, feedback from the cable network operators indicates that the cable network infrastructure dependent upon GPS time signals will sustain operation automatically for approximately 30 days. Beyond this period, some circuit termination equipment could be reconfigured to utilize the receive clock from the PSTN as a reference clock; however, this option may not be viable in the event of widespread GPS outage or degradation.

  - Feedback from the broadcast industry indicates that GPS is not critical to the operation of most broadcast systems. Systems that may be affected by GPS loss include "Precision Off-Set" between analog and digital TV transmitters, HD Radio, and Distributed Transmission networks for television. For these systems, loss of GPS can be tolerated for "an extended period of time" although this time period is not easily predicted and requires further study.

In the extremely unlikely event of a complete and catastrophic loss of GPS over an extended period of time (*e.g.*, more than one month) and affecting a large geographic area (*e.g.*, nationwide, continental, global), overall impact is more difficult to ascertain. Because of the diverse and highly distributed implementations of GPS-based solutions across the industry, any impact likely would be experienced in the form of a gradual degradation of network performance, with little potential for cascading network failures. The NSTAC also emphasizes that commercial communications networks do not operate in a vacuum, and service providers and network operators will take immediate corrective actions in response to any size event, particularly a large-scale catastrophic event with the potential to degrade the network. Even before all automatic means of backup are exhausted, companies will have already executed contingency plans and performed manual reconfigurations and network timing adjustments as required to maintain network operation.

Overall, industry members surveyed believe that their companies have taken measures to safeguard against those disruptions to the GPS signal that are likely to be encountered; however, to date, no industry or Government exercise has sought to replicate the impact of a long-term or permanent GPS outage simultaneously on all industries. The NSTAC recommends that the President direct the Department of Homeland Security and the Department of Defense to include various GPS outage scenarios in future planned disaster recovery exercises in coordination with the commercial communications industry.

Footnotes

1 Within the commercial communications industry, the term "mitigation" often refers to reactive approaches or strategies applied after an event has occurred. Reflecting the industry responses collected for the study, this report uses the term more broadly to encompass both reactive approaches as well as proactive, or preventative, safeguarding strategies.

2 To synchronize its clock, a GPS receiver requires signals from only one satellite in the constellation.

3 Currently, there are 29 operational satellites and one experimental satellite in orbit.

4 Pace, Scott, *et. al.* The Global Positioning System: Assessing National Policies, 1995.

5 Available at the National Space-Based Positioning, Navigation, and Timing (PNT) Executive Committee Web site, http://pnt.gov/policy /

6 Source: National Space-Based PNT Executive Committee, http://www.pnt.gov

7 http://www.gps.gov

8 National Communications System, "Telecommunications Network Time Synchronization," NCS Technical Information Bulletin 99-4, April 1999.

9 Under Phase II, the FCC requires wireless carriers, within six months of a valid request by a Public Safety Answering Point (PSAP), to begin providing the latitude and longitude of a caller, typically within 50 to 300 meters. The FCC requires carriers using GPS-enabled handsets to locate callers within 150 meters 95 percent of the time and within 50 meters about 67 percent of the time. In September 2007, the FCC voted to require wireless operators to meet E911 requirements at a local level, specifically the jurisdictional areas of individual 911 PSAPs, expanding upon the previous statewide or multi-state level requirement. Carriers must meet location accuracy targets by September 11, 2012.

10 The term "complete GPS loss" refers to the inability to receive any GPS signals at all locations. The term "localized GPS loss" refers to the inability to receive any GPS signals within a limited geographical area (*e.g.*, campus, city, region). These terms are in contrast to the term "partial GPS loss" which refers to the inability to receive signals from some, but not all, GPS satellites. According to industry feedback, partial GPS loss has no appreciable impact on network operations and services.

11 While the examination of network impacts related to specific GPS vulnerabilities is outside the scope of this study, the NSTAC considered information on a range of threats and vulnerabilities, including unintentional disruption (*e.g.*, solar bursts and ionospheric interference, RF interference sources, human factors) and intentional disruption (*e.g.*, shutdown, jamming, spoofing, and meaconing [a system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation]). In reviewing these vulnerabilities, participants generally characterized the potential for any long-term complete GPS loss as unlikely. Participants also agreed that the further study on GPS vulnerabilities, particularly potential space weather impacts, is necessary to better characterize likelihood of impact to the commercial communications infrastructure (See Associated Press, Solar Bursts Could Threaten GPS, April 5, 2007).

12 American National Standards Institute, T1.101-1999: Synchronization Interface Standards for Digital Networks.

13 Lombardi, Michael, NIST Time and Frequency Division, Legal and Technical Measurement Requirements for Time and Frequency.

14 As noted in the 2004 NSTAC study, a Stratum 2 timing source referenced by a Stratum 1 timing source will maintain accuracy for up to one month. As shown in Table 2, a Stratum 2 source with no reference performing at the minimum ANSI T1.101 accuracy requirement (worst case) would result in an interval of

about seven days between cycle slips. Similarly, at the minimum specified frequency accuracy for Stratum 3E clocks, the worst case interval between cycle slips is 104 minutes.

15 Telcordia, Generic Requirements GR-253-CORE, Synchronous Optical Network Transport Systems, and GR-1244, Clocks for the Synchronized Network, among others.

16 NSTAC Satellite Task Force Report, March 2004.

17 Reception of satellite signals from four satellites is needed to establish accurate position.

18 National Institute of Standards and Technology, Time and Frequency Division, http://tf.nist.gov/timefreq/stations/wwvb.htm

19 Feedback from cable network operators also notes that the cable industry is deploying asynchronous links such as Gigabit Ethernet and will rely less on synchronous networks such as SONET in the future.

20 In an oscillator, the "flywheel effect" refers to the continuation of oscillations after removal of the control stimulus.

21 The Network Reliability Interoperability Council, an FCC advisory committee comprised of commercial communications companies as well as public sector stakeholders has developed generic network reliability and security best practices, including practices regarding GPS location accuracy for E911 service. http://www.nric.org.

Working Group Members

Working Group Members

Intelsat, Limited
Mr. Richard DalBello, Chair

The Boeing Company
Mr. Marc Johansen, Vice-Chair

Verizon Communications, Incorporated
Mr. James Bean, Vice-Chair

AT&T, Incorporated
Mr. Thomas Hughes
Ms. Rosemary Leffler

Bank of America Corporation
Mr. Roger Callahan

The Boeing Company
Mr. William Patrick Reiner
Mr. Robert Steele

Intelsat, Limited
Ms. Sallye Clark
Mr. Sterling Winn

Lockheed Martin Corporation
Mr. Allen Dayton

National Cable & Telecommunications Association
Mr. Andy Scott

Qwest Communications International, Incorporated
Ms. Diana Gowen
Mr. Thomas Snee

Science Applications International Corporation
Mr. Hank Kluepfel

Sprint Nextel Corporation
Mr. Lee Fitzsimmons
Ms. Allison Growney
Mr. John Stogoski

Raytheon Company
Mr. Bill Russ

Rockwell Collins, Incorporated
Mr. Ken Kato

Verizon Communications, Incorporated
Mr. Roger Higgins

Other Participants

Homeland Security Institute
Dr. Eric Sylwester

Volpe National Transportation Systems Center
Dr. James Carroll

Government Participants

Institute of Defense Analyses
Mr. Jim Doherty

Department of Homeland Security, National Communications System
Mr. Dale Barr
Mr. Kelvin Coleman

Department of Homeland Security, United States Coast Guard
Captain Curtis Dubay

National Space-Based Positioning, Navigation, and Timing Coordination Office
Mr. Robert Crane
Mr. Michael Shaw

Acronym List

Acronym List

BITS	Building Integrated Timing Supply
CDMA	Code Division Multiple Access
CO	Central Office
DAC	Digital Access and Cross-Connect
DHS	Department of Homeland Security
DOCSIS	Data Over Cable Service Interface Specification
DOD	Department of Defense
DTV	Digital Television
E911	Enhanced 911
FCC	Federal Communications Commission
GPS	Global Positioning System
HD	Hybrid Digital
HLR	Home Location Register
IBOC	In Band On Channel
IRIG	Inter-Range Instrumentation Group
LES	Land Earth Station
MSC	Mobile Switching Center
NIST	National Institute of Standards and Technology
NSTAC	National Security Telecommunications Advisory Committee
NTP	Network Time Protocol
PBX	Private Branch Exchange
PNT	Positioning, Navigation, and Timing
PRS	Primary Reference Source
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RF	Radio Frequency
SDH	Synchronous Digital Hierarchy
SME	Subject Matter Expert
SONET	Synchronous Optical NETwork
TDM	Time-Division Multiplexing
TSG	Timing Signal Generator
TT&C	Telemetry, Tracking, and Control
VLR	Visitor Location Register
VOD	Video On Demand

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Network Operations Centers

February 28, 2008

For information on this report, please contact the

National Communications System
nstac1@dhs.gov

Office of the Manager
National Communications System
Customer Service Division
Mail Stop 8510
245 Murray Lane
Washington, DC 20528-8510
(703) 235-5525
www.ncs.gov/nstac/nstac.html
nstac1@dhs.gov