2008 Sector CIKR Protection Annual Report for the Communications Sector

July 1, 2008

Homeland
Security

Contents

Foreword

The National Communications System (NCS) as Sector-Specific Agency (SSA) for the Communications Sector worked closely with its security partners in the Communications Government Coordinating Council (CGCC) and Communications Sector Coordinating Council (CSCC) to develop the following comprehensive Sector Annual Report (SAR).

The goals, objectives, priorities and requirements stated throughout the report were jointly developed and agreed upon by both GCC and SCC representatives. While not every member of the GCC or SCC was able to participate in this process, those individuals who actively engaged in the drafting and reviewing of the SAR represented every segment of the Communications Sector. The knowledge and experience SCC members (consisting of the owners and operators of the communications infrastructure) brought to the document were essential in ensuring that the SAR was complete and conveyed an accurate representation of the current Communications Critical Infrastructure/Key Resource (CIKR) Sector landscape.

As the Communications SSA, the NCS included budgetary figures that only encompass its own programs. While this accounts for the majority of the security programs across the Communications Sector, other programs with secondary focus on Communications Sector security may be unaccounted for in the SAR.

The Modeling Simulation & Analysis (MS&A) and Research &Development (R&D) progress and effectiveness description in this SAR only include the efforts of the NCS; other Communications Sector wide MS&A and R&D activities are not incorporated into this report. The Sector, however, has and will continue to work closely with the Department of Homeland Security's Science and Technology Directorate as well as individual companies, academic institutions, and trade associations to ensure Sector-wide MS&A and R&D efforts are coordinated at the highest degree possible.

Executive Summary

Over the past year, the Communications Sector has made significant progress in assessing risk to its critical infrastructure/key resources (CIKR). The Communications Sector, a partnership between the Communications Government Coordinating Council (CGCC) and the Communications Sector Coordinating Council (CSCC), continued with the implementation of the Communications Sector-Specific Plan (CSSP), which provides a comprehensive risk-management framework that defines critical infrastructure protection roles and responsibilities for all levels of Government and private industry.

During this reporting period, the Communications Sector heavily focused on the completion of the Communications National Sector Risk Assessment (NSRA) to meet the goals of the National Infrastructure Protection Plan (NIPP) and the CSSP. The NSRA identifies national level communications architecture elements that are at elevated risk and serves as a baseline to prioritize the communications infrastructure. In May 2008, the CSSP Implementation Working Group (hereafter referred to as the Working Group), which consists of Federal government representatives from the CGCC, industry representatives from the CSCC and liaison representatives of the Information Technology Sector Coordinating Council successfully completed the NSRA.

The NSRA provides a high level, qualitative assessment by analyzing all segments of the Sector including broadcast, cable, satellite, wireless and wireline. The NSRA includes two overarching assessments, one on physical threats and a second on cyber threats to the communications infrastructure. Each assessment reflects the results of qualitative risk analyses that consider threats, vulnerabilities, and consequences as defined in the CSSP. The NSRA concludes that single event threats pose no substantial risk to national communications but single incidents could affect a local or regional geographic area, which may have an impact on the national level. The Working Group recommended continued discussion in identifying a path forward on the following issues:

- Assessing risks associated with global communications infrastructure;
- Assessing coordinated multiple attacks;
- Assessing risks from communications dependencies;
- Assessing risks to other Critical Infrastructure Sectors, based on dependency upon communications;
- Identifying communications architecture elements at elevated risk; and
- Obtaining additional cyber security funding.

In addition to the NSRA, industry partners continue to self-assess risk to their infrastructures and Communications Sector security partners have already began scoping the need for additional detailed risk assessments based on the results of the NSRA, protective programs and R&D activities.

The National Communications System (NCS), as the Communications Sector-Specific Agency (SSA), manages numerous protective programs that industry developed and operates to further help reduce risk to the Communications Sector by ensuring the security of the communications infrastructure and delivery of National Security and Emergency Preparedness (NS/EP) communications services, with a strong focus on response and recovery. These programs include the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and the Telecommunications Service Priority (TSP) Program. The NCS has also begun to work with industry to develop a Next Generation Priority Service (NGPS). The overarching goal of the above programs is to improve access and expedite restoration or provisioning for national security and emergency preparedness users should there be congestion in the network.

In the Communications Sector, partnerships are the foundation for all protective programs. The NCS manages various communications partnerships that aim to improve situational awareness and the exchange of information such as the National Coordinating Center (NCC) and the Network Security Information Exchanges, participates in the Cross-Sector Cyber Security Working Group and closely collaborates with the National Security Telecommunications Advisory Committee (NSTAC) and the Committee of Principals. Furthermore, the Communications Sector industry and Government partners have an excellent and longstanding partnership responsible for the effective implementation of the CSSP, the timely completion of the NSRA, and the overall improvement of the Communications Sector's defense posture.

In addition to utilizing the above protective programs, the Communications Sector continues to perform security-related research and development (R&D), which are vital to both the protection and the advancement of NS/EP communications as the Communications Sector continues its transition into next generation networks. The NCS, in collaboration with industry completed a study on the impact of pandemic influenza on communications networks and continued to enhance its Internet data and next-generation networks (NGN) modeling and analysis capabilities. Due to funding constraints, however, the NCS has been unable to effectively continue the migration of its GETS services to an IP platform, which significantly jeopardizes NS/EP communications during times of severe network congestion and/or disruption.

Furthermore, Communications Sector Government programs need additional funding to perform detailed risk assessments and cross-dependency analyses and carry out work related to its Modeling Simulation &Analysis (MS&A) and R&D objectives. The NCS' budget has been severely cut, which will impede its efforts to maintain existing and implement new programs necessary for the execution the CSSP and the improvement of the overall security of the Communications Sector.

The Communications Sector's security practices focus on built-in resiliency, response, and recovery. To ensure the security of the Communications Sector, owner/operators regularly perform risk assessments on their facilities; maintain a suite of physical, cyber, and human security measures; and collaborate with other companies and trade associations on best practices. The Communications Sector continues to address issues related to threat information sharing and the improvement of access to disaster areas for restoration crews.

During the past year, the Communications Sector has made significant progress in completing specific actions and milestones in pursuit of advancing the seven goals detailed in its CSSP. Going forward, the CGCC and the CSCC will be working in collaboration to determine the next steps in the implementation of the CSSP. The two groups will continue to develop next-generation priority services, develop a Communications Sector outreach program, focus on cyber security related programs and activities and explore follow-on activities to the NSRA.

Section 1: Sector Security Goals and Priorities

1.1 Sector Security Goals, Mission, and Vision Statement

The Communications Sector set seven goals in the Communications Sector-Specific Plan (CSSP), published in May, 2007 (Table 1-1). These goals represent specific outcomes, conditions, end points, and performance targets for the Communications Sector and provide a framework for the implementation of the CSSP. They also guide the Communications Sector's resources and focus on protective measures and give the Communications Sector means by which to evaluate its progress and performance. These goals are being used as the guide for setting priorities in the implementation of the CSSP and prioritizing risks. The Communications Sector security goals for 2008 remain the same as established in the CSSP.

Table 1-1 Communications Sector Security Goals

Goal 1	Protect the overall health of the national communications core network.
Goal 2	Rapidly reconstitute critical communications services after national and regional emergencies.
Goal 3	Plan for emergencies and crises by participating in exercises and updating response and continuity-of-operations plans.
Goal 4	Develop protocols to manage the exponential surge in use during an emergency situation and ensure the integrity of Communications Sector networks during and after an emergency.
Goal 5	Educate security partners on communications infrastructure resiliency and risk-management practices in the Communications Sector.
Goal 6	Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decision makers in the Communications Sector.
Goal 7	Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness and cross-sector incident management.

The Communications Sector's mission directly corresponds to infrastructure protection activities outlined in the CSSP. According to the mission statement, industry and government partners commit to both individually and cooperatively mitigate risks to those national communications infrastructure assets and services whose exploitation would result in a national impact. The Communications Sector's mission has remained unchanged since its initial establishment in the CSSP.

The Communications Sector's vision in the CSSP states: "The Communications Sector acknowledges the Nation's critical reliance on assured communications. The Communications Sector will strive to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster." The Communications Sector vision's statement has also remained unchanged since it's initially establishment in the CSSP.

1.2 Sector CIKR Risk Profile

Part of the CSSP framework includes conducting the Communications National Sector Risk Assessment (NSRA) to identify risks to the national communications infrastructure. In May 2008, the CSSP Implementation Working Group (hereafter referred to as the Working Group), completed the NSRA to meet the goals of the National Infrastructure Protection Plan (NIPP), and as a result, provided numerous recommendations for future implementation. The Working Group consists of Federal government representatives from the Communications Government Coordinating Council (CGCC), industry representatives from Communications Sector Coordinating Council (CSCC), and liaison representatives of the Information Technology Sector Coordinating Council.[1]

The NSRA comprehensively evaluated the Communications Sector's exposure to risk by analyzing the three factors the National Infrastructure Protection Plan (NIPP) uses to define risk: threats, vulnerabilities, and consequences. The Working Group focused on those threats with which the Department of Homeland Security (DHS) is most concerned, specifically threats described by the Federal Emergency Management Agency (FEMA) in the *National Planning Scenarios* and by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) in the 2007 Strategic Homeland Infrastructure Risk Assessment (SHIRA). The Working Group concluded that these two sources provided a well-rounded set of threats that addressed the "all-hazards" approach outlined in the NIPP.

The NSRA provides a high level, qualitative assessment by analyzing all segments of the Communications Sector including broadcast, cable, satellite, wireless and wireline. The NSRA includes two overarching assessments, one on physical threats and a second on cyber threats to the communications infrastructure. Each assessment reflects the results of qualitative risk analyses that consider threats, vulnerabilities, and consequences as defined in the CSSP. The NSRA concludes that single event threats pose no substantial risk to national communications but single incidents could affect a local or regional geographic area, which may have an impact on the national level.

The analysis produced the following specific key findings:

- ***The Communications Sector is diverse* –** The national communications infrastructure consists of many architecture elements owned by different companies providing diverse technologies, services, routes, connectivity, and utilizing various vendors. The Communications sector has invested billions of dollars in designing, building, and maintaining the infrastructure to achieve intra-segment resiliency (e.g., within wireline) and cross segment resiliency (e.g., between wireless and wireline) to provide an overall robust communications network. This diversity and resiliency minimizes the risk to the national infrastructure.

[1] The CGCC was established in late Spring 2005 to coordinate communications security strategies, activities, policies and communication across the Federal, State and Local Governments and between the Government and the communications sector in support of the Nation's homeland security mission. The CGCC acts as the Government counterpart and partner to the private industry-led CSCC for planning, implementing and executing sufficient and necessary sector-wide security programs for the Nation's communications critical infrastructure.

- ***Single physical incidents present no risk of nationally disruptive effects on the communications infrastructure –*** Single physical incidents present no risk to national communications because of the resiliency and redundancy of the core network, signaling and databases, and operations management. At most, single physical incidents could affect communications in a local or regional geographical area.
- ***The risk of disruptive effects on the communications infrastructure from a single cyber incident is greater than the risk from a single physical incident –*** Cyber threats are different than physical threats because they have no geographic boundaries and limitations. However, it is unlikely that a single cyber threat would have nationally disruptive effects on the communications infrastructure. A cyber incident could affect multiple service providers if it disrupted signaling and databases or the core network, but there are significant protective measures and mitigations in place to prevent such incidents from occurring or creating visible disruptive effects. Local and regional communications are at higher risk of being disrupted because the access segment is more vulnerable to an incident.
- ***Availability of the communications infrastructure, compared to confidentiality and integrity, is at elevated risk from both cyber and physical incidents –*** Cyber and physical incidents pose a greater risk to the availability of the communications infrastructure than to its confidentiality and integrity. Physical incidents will only affect availability. Although some cyber incidents may affect integrity or confidentiality of the communications within the network, such incidents pose a greater risk to availability.
- ***Access networks and signaling databases are functional areas of elevated risk, the core network and operations management are at lower risk –*** Compared to other functional areas of the architecture model, access is the most vulnerable to single physical incidents and cyber incidents. Thus, local and regional communications are at higher risk of being disrupted due to less redundancy at the edge of the network. Based on the results from the cyber risk assessment, signaling and databases are at elevated risk to cyber incidents compared to the core network and operations management architecture elements.
- ***Local and regional disruptive effects on communications may lead to national impacts*** National impacts are effects on human life, economy, and government capability. The impacts of local and regional events in the communications networks would not likely affect human life, but may harm the economy, public morale, or government capability. The severity of these impacts depends on the particular area disrupted and the network implementation and mission of the affected government and commercial end users.
- ***Risk is dependent on location –*** Although this NSRA has a national scope, the risk of disruptions to communications services varies depending on the location of architecture elements. For example, elements in higher-profile urban areas are likely to be at a higher risk than elements in less-populated areas. This does not incorporate modeling of networks which evaluates the impact on other sectors.
- ***Communications Sector has dependencies on other sectors –*** The reliance of the Communications Sector on other critical sectors is extensive. Coordination with the other critical sectors is crucial to ensuring the communications infrastructure can be supported in the event of a long-term impact.

- ***Access/credentials, fuel, and security are critical*** – Access/credentials, fuel, and security are critical in responding to attacks, accidents and any service impairment for all segments. If access/credentials, fuel, or security are not available, then the ability to repair, recover, or reconstitute the networks will be impacted and the duration and scope of a disruption may increase.
- ***Skilled workers and research and development are critical in continuing to reduce and mitigate cyber risk*** – Protective measures have been implemented by the Communications Sector (both government and industry) to mitigate cyber risk. These measures include actions to safeguard against and mitigate cyber incidents, such as a layered security approach and extensive testing prior to implementing updates and upgrades. Critical to these efforts are research and development, hiring skilled workers, and education and training for the future work force. Each of these actions is critical in safeguarding against non-malicious cyber incidents and underscores the importance of the availability of skilled staff and adequate research and development resources.

1.3 CIKR Protection Gaps

The National Communications System (NCS), as the Sector Specific Agency (SSA) for the Communications sector, manages numerous protective programs that mitigate risk for national security and emergency preparedness (NS/EP) user groups, as well as information-sharing programs that reduce risk by actively sharing information about threats, vulnerabilities, and anomalies. In addition, individual companies have protection mechanisms in place to protect their assets, systems, and networks.

The NSRA has, however, identified gaps that need to be addressed in the future. Based on the risk analysis of the physical threats, the Working Group concluded that single incidents present no substantial risk to the national communications infrastructure because of the resiliency and redundancy of the core network, signaling and databases, and operations management. However, by comparison, access networks and local and regional communications are more vulnerable to these incidents. Local and regional disruptive effects on communications may have substantial impacts (or national consequences) if such communications support critical users or functions. Additional areas the NSRA has identified include:

- The risk of disruptive effects on communications infrastructure from a single cyber incident is higher than the risk from a single physical incident.
- Availability of communications infrastructure, compared to confidentiality and integrity, is at elevated risk with a cyber or physical incident.

The Communications Sector recognizes that local or regional disruptions may result in national impacts. For this reason, the Communications sector has established mutual aid agreements and works with the Government through the NCS National Coordinating Center (NCC) to facilitate communications among carriers and the government, including mitigating and responding to disasters. The Communications Sector also works to address post-disaster access issues to minimize the duration of any communications disruptions.

Even with these efforts, government, commercial, and individual end users must take the initiative to procure the level of availability, security, and diversity from their local access networks commensurate with their respective mission requirements for communications availability and business continuity planning. If communications are critically important, end users should investigate whether multiple separate and distinct access methods are available. End users should also determine their resiliency requirements and work with their service providers to implement them. Simply having more redundancy or diversity at a given facility is not sufficient if the end user is not properly prepared or has not conducted business continuity planning to respond to disruptions in service.

The Working Group used the same methodology to conduct its analysis of the risk resulting from single physical incidents and single cyber events. However, because of the significant differences between physical and cyber risks, the Working Group analyzed these risks separately. The Working Group's cyber assessment established that risks to the communications cyber infrastructure are real and must continue to be managed. Service providers use multiple mechanisms to mitigate cyber risk by reducing the vulnerabilities that can be exploited by a given threat and improving threat identification and response capabilities. Additionally, diversity in carrier infrastructure, network topologies, and deployed equipment reduce the risk of a single incident's impact on the national network's capability to function as related to national impacts.

It is important that the awareness of cyber risk continue to grow, including in the academic communities and be supported by government and industry research and development programs. Both enhanced capabilities and stronger, more secure protocols are needed to defend against rapidly changing threats. Using lessons learned to continually refine infrastructure designs and operational processes increases the Nation's defense posture.

The NSRA concluded that risks from a specific set of single events pose no substantial threat to national communications. However, there are additional issues that the Communications Sector recognizes and recommends for further scoping. Many of these issues were also recommended by the Network Security Information Exchanges (NSIE) during its "Birds of a Feather" meetings on September 17, 2007 for possible investigation by the NSIE. These issues recommended for further scoping are listed below:

- ***Global infrastructure* –** The international nature of the communications infrastructure should continue to be studied (both in terms of physical location and interconnectivity). International collaboration and mutual aid agreements are critical to responding to a disaster or attack. The President's National Security Telecommunications Advisory Committee (NSTAC) Report on International Communications defined a number of protection gaps in effective incident management and response. In reaction to the report the NCS Committee of Principles has formed an International Working Group to explore the above issues.
- ***Coordinated multiple attacks*** – Although this assessment focused on single event incidents, supporting analysis found that strategic coordinated attacks to the communications infrastructure may pose a greater threat to the Communications Sector.

Such attacks could consist of simultaneous physical or cyber attacks on multiple targets (for example, simultaneous attacks against multiple bridges and tunnels), or a blended cyber-physical attack. Therefore, the threats posed by multiple or coordinated attacks should be identified as one of the critical subjects for future studies.

- ***Communications interdependencies*** **–** The Working Group also recommends scoping the interdependencies between the Communications Sector and other sectors critical to communications through government-sponsored cross-sector dependency analyses or other analysis methods. The national sector risk assessment only addressed direct impacts on the Communications Sector; however, indirect impacts may cause severe national consequences and need to be further assessed. The Communications Sector's dependence on electric power is a good example to demonstrate indirect impacts. Regional power failures, which tend to occur during or as a result of attacks or natural disasters, could exacerbate the impact of an event that disrupts the communications infrastructure. Alternatively, if the electric power infrastructure is damaged by a targeted attack, the communications infrastructure would be adversely affected, even if all the elements were fully functioning.
- ***Communications architecture elements at elevated risk*** **–** The Working Group recommends continued discussion within the public / private partnership to determine the strategy going forward on conducting detailed risk assessments on some of the specific types of architecture elements identified as having elevated risk by the NSRA.
- ***Additional cyber security funding*** **–** The Working Group proposes to investigate the need for additional funding to support cyber security, including cyber research and development, education and training, and the development of a skilled cyber workforce.

Using the results of the NSRA as a basis, the Working Group recommends that government and industry partners work together to enhance existing protective programs and identify new programs able to reduce risk to the Communications Sector. The Communications Sector, the events and associated risks continuously change. Consequently, the NSRA is iterative in nature and should be updated or repeated periodically.

The Communications Sector is also addressing major areas of concern through the implementation of the CSSP as well as various partnerships. For example, the COP is currently examining the Communications Sector's dependency on electric power based upon a recommendation from the NSTAC. In addition, the NCS supports the Office of Emergency Communications' efforts to improve nation-wide communications interoperability and the National Cyber Security Division's mandate regarding cyber security.

1.4 Sector Priorities

The NCS has made significant progress towards the implementation of its 2007 Communications Sector priorities, as identified in its 2007 Critical Infrastructure and Key Resources (CIKR) Sector Annual Report. In addition to the detailed description of the Communications Sector's progress in Section 6, the following table lists each of the 2007 Sector priorities with the progress noted for each item.

2007 Communications Sector Priorities

Progress Status	Associated Goal(s) No.	Priority Description
Completed	1	Conduct a NSRA to identify risks to the national communications infrastructure.
Ongoing	2	Continue to work with industry to develop next-generation priority services to meet the evolving requirements of critical communications customers in a converged communications environment.
Ongoing	2, 3	Revise Emergency Support Function (ESF) #2 (Communications) Annex to the National Response Plan to reflect current processes and lessons learned from previous crises.
Completed	5	Partner with the IT Sector on the NSRA for the Internet.
Ongoing	7	Develop concept of operations between the NCC and United States Computer Emergency Response Team (US-CERT) to improve cross-sector information sharing and operations.
In progress	6	Initiate discussions with HITRAC to improve information-sharing processes with the law enforcement and intelligence communities.
In progress	4	Continue outreach on priority service programs.
Ongoing	3	Conduct ESF#2 spring and winter conferences to improve knowledge of industry and Government representatives in the regions of ESF#2 processes and NCS programs.
Not started	5	Develop an outreach program to educate Communications Sector customers and other infrastructures on communications infrastructure resiliency and risk-management practices.
Pandemic Flu study completed	3	Participate in National Pandemic Flu Planning by studying the potential impact of substantial surges in telework in the event of a pandemic and evaluate potential corporate actions necessary to maintain network operations.
In progress	7	Develop a capability to work with other sectors to assess their dependency on communications, especially for other sector's critical assets, networks, systems, and functions.
Ongoing	7	Collaborate with the National Infrastructure Simulation and Analysis Center (NISAC) on the interdependency analyses.

The Communications Sector's highest priority objectives within the past reporting cycle focused on the completion of the Communications NSRA to meet the goals outlined in the CSSP. The focus of the NSRA effort was to identify those architectural elements that are nationally critical because their loss could severely impact national or regional communications. As a result of the assessment, industry and Government will need to jointly determine the strategy for the next steps toward the completion of the CSSP, which should include programs to reduce areas of defined risk as well as training and credentialing programs to aid in recovery efforts. As stated in the NSRA, additional detailed risk assessments and cross-dependency analyses will be necessary to better understand the vulnerabilities of and consequences to the Communications Sector. In addition to the above, the CGCC and CSCC have agreed that the highest priorities for the Communications Sector consist of:

1. Partnering with the IT sector on cyber security; enhancing the work and expanding the membership of the recently established Cyber Committee of the CSCC.

2. Developing a sector outreach program to educate Communications Sector customers and other infrastructures on communications infrastructure resiliency and risk-management practices.

3. Establishing measurements pursuant to the SSP to effectively evaluate the success of the sector in its effort to improve its security and resiliency.

4. Consult with government representatives and organizations and private sector entities to ensure appropriate exchanges of information to enhance key initiatives, such as:
   - Access and Credentialing
   - Regionalization of Communications Support
   - National Emergency Communications Plan (NECP)

The Communications Sector will also continue to focus on other areas that align closely with national protection priorities:

- Participation in National Pandemic Flu Planning; and
- Improving information sharing between industry and government, including with the law enforcement and intelligence communities.

Section 2: Sector Programs, Activities, and Tools

This section describes the major CIKR protection programs, initiatives, and collaboration with industry and government partners by the NCS.

2.1 CIKR Protection Programs and Initiatives

As detailed in the CSSP, the Communications Sector has protective and preparedness programs that help to ensure the security of the communications infrastructure and delivery of NS/EP communications services, with a strong focus on response and recovery. There are also a number of programs concentrating on Internet security, managed by the National Cyber Security Division (NCSD) that help mitigate cyber attacks across all sectors. These cyber security programs are not listed here, because they are cross-sector initiatives.

The NCS develops and manages a number of priority programs to reduce the impact of network congestion and improve access and expedite restoration or provisioning for NS/EP users:

- *Government Emergency Telecommunications Service (GETS)* provides emergency access and priority processing in the local and long-distance segments of the public switched telecommunications network (PSTN). This service increases the likelihood that NS/EP personnel can complete critical calls during periods of PSTN disruption and congestion resulting from natural or man-made disasters. GETS uses three major types of networks: major long-distance networks, local networks, and Government-leased networks.

- *Wireless Priority Service (WPS)* provides priority Commercial Mobile Radio Service during and after emergencies for NS/EP personnel by ensuring WPS calls receive the next available radio channel during times of wireless congestion. WPS helps to ensure that key NS/EP personnel can complete critical calls by providing priority access during times of wireless network congestion to key leaders and supporting first responders.

- *The Telecommunications Service Priority (TSP) Program* provides the regulatory, administrative, and operational framework for priority restoration and provisioning of NS/EP communication circuits in an emergency. Eligibility in the TSP Program extends to Federal, State, and local Governments; private industry; or foreign Governments that have communications services supporting an NS/EP mission. The NCS is currently pursuing implementation of an NSTAC recommendation[2] to enhance the TSP Program to accommodate requests from NS/EP users of wireless telecommunications services at critical sites.

- *Next Generation Priority Service (NGPS)* is being developed by the NCS and its industry partners. This technology will provide priority service capabilities over the Internet, standardize the technology across industry through the commercial standards process, and migrate current priority service features to the Internet.

In addition to priority programs, the NCS manages a national training and exercise program, and is working to engage and facilitate feedback and continuous improvement in the process of industry involvement and participation. Recent successes include Government/industry coordination in addition to increased priority communications program subscriptions during Cyber Storm II. Additionally, initial feedback from the recently-completed National Level Exercise 2-08 included increased industry participation with the Northern Command (NORTHCOM) and hazardous materials (HAZMAT) teams. It is important that industry be involved during the planning of future exercises to build upon these successes.

2.2 Coordination Groups and Security Partners

In the Communications Sector, partnerships are the foundation for all protective programs. The following are six of the most significant partnerships for infrastructure protection, because they are forums for improving situational awareness, sharing information, developing best practices and providing policy analysis and recommendations.

- *The NCC* serves as a joint industry-Government operations center with an operational mission to coordinate response and restoration priorities during an incident. In addition, through its Information Sharing and Analysis Center function, NCC partners actively share information about threats, vulnerabilities, intrusions, and anomalies.

[2] "National Security Telecommunications Advisory Committee Report to the President on Emergency Communications and Interoperability." National Security Telecommunications Advisory Committee, January 16, 2007.

- *United States Computer Emergency Readiness Team (US-CERT)* is a partnership between the Department of Homeland Security and the public and private sectors that coordinates defense against and responses to cyber attacks. The US-CERT serves as a vital security partner for the Communications Sector. The US-CERT and the NCC embarked on a collocation strategy during the Winter of 2008 to help increase information exchange between the IT and Communications Sectors.

- *Network Security Information Exchanges (NSIE)*, which meet jointly every 2 months, share information and views on threats and incidents affecting the public network's software elements, vulnerabilities, and their remedies. In addition, the NSIEs periodically conduct an assessment of the risk to the PSTN from electronic intrusion. The U.S. NSIEs hold bilateral and trilateral exchange meetings with their counterparts from the United Kingdom and Canada.

- *The Cross-Sector Cyber Security Working Group (CSCSWG)*, which was established in May 2007, serves as a voluntary forum to share knowledge and addresses common cyber security challenges and opportunities across the 17 CIKR sectors. The Working Group provides two-way collaboration with standing and liaison groups; encourages sectors to share cyber related preparedness efforts; and promotes Government and Industry participation in cyber related events and programs. The Communications Sector actively participates in the CSCSWG by attending meetings and contributing to various products.

- *The National Security Telecommunications Advisory Committee (NSTAC)*, which recently celebrated its 25th anniversary, provides industry-based analysis and recommendations to the President and the executive branch regarding communications policy and enhancements to national security and emergency preparedness (NS/EP). Many NSTAC activities are the genesis for technical reports, recommendations to the President, and NS/EP operational programs. For example, the NCC, the TSP program, and the NSIEs were all created as a result of NSTAC activities. The NSTAC holds annual meetings and quarterly conference calls. The NSTAC Industry Executive Subcommittee meets regularly to consider issues, analysis, or recommendations for consideration to the NSTAC.

- *The NCS Committee of Principals (COP)* is an interagency group designated by the President that provides advice and recommendations on national security and emergency preparedness communications to the Executive Office of the President (EOP). High-level Government officials representing Federal operational, policy, regulatory, and enforcement organizations compose the COP. Its diverse representation across 24 Federal departments and agencies embraces the full spectrum of Federal telecommunications assets and responsibilities. As an interagency group, it serves as a forum for members to review, evaluate, and present views and recommendations on current or prospective NCS programs to the Manager of the NCS, and the EOP. The COP enables Communications Sector security partners across the Federal government to provide input and guidance to the Sector regarding the current status of and future of the Sector as a whole.

The Communications Sector industry and Government partners have an excellent and longstanding partnership responsible for both the effective implementation of the CSSP and the timely completion of the NSRA, which was one of key tenets of the CSSP. In the first half of 2007, the CSCC and the CGCC established a steering committee and the Working Group to direct the implementation of the CSSP and carry out the Communications National Sector Risk Assessment (NSRA). The NSRA was completed and a final draft was submitted to NCS leadership in May 2008. During the drafting of the NSRA, the Working Group met to develop a methodology and architecture that encompassed all segments of the Communications Sector, performed the analysis and based on its conclusions, provided numerous recommendations. The NSRA demonstrates the partnership needed to meet the objectives of the CSSP and completes a major milestone in the implementation of the CSSP. The leadership of the CGCC and CSCC also conducted two additional meetings during the year that enabled robust discussions surrounding the current landscape of the Communications Sector, possible mitigation efforts to strengthen the Sector, as well as in depth strategic discussions, which resulted in a shared vision of the future of the Sector.

Independent of the CSSP efforts, the CSCC also collaborated with the Banking and Finance sector on a network congestion study that determined the impact of increased number of teleworkers on the communications network in the event of a pandemic flu. Some of the outcomes of the study include the identification of possible mitigation tools and the awareness of sector preparedness and capabilities.

As a whole, the CSCC represents over 35 companies and trade associations from the wireline, wireless, cable, broadcasting, and satellite sub-sectors. The CGCC membership includes representation from the Departments of Homeland Security, Justice, and Commerce; Federal Communications Commission (FCC); and General Services Administration. In addition, the CGCC coordinates with the States through a representative from the National Association of Regulatory Utility Commissioners (NARUC). The NCS is currently in the process of reassessing and revitalizing CGCC membership to achieve optimal stakeholder participation.

Section 3: CIKR R&D Progress and Updated Capability Gaps

Security-related research and development (R&D) in Communications Sector CIKR is vital to both the protection and the advancement of NS/EP communications as the Sector continues its transition into next generation networks. The R&D requirements within this section define particular topic areas within the Communications Sector. Identifying R&D requirements allows the NCS to analyze the gaps that exist between those requirements and the R&D programs, policies, and initiatives currently in place, and to more effectively plan future initiatives to address those gaps.

The Communications Sector requirements are primarily cyber focused, because physical security requirements are mainly addressed by industry, non-technological (e.g., process improvements), or are generic to all infrastructures. Several physical security initiatives that are process-focused, such as access to disaster sites, credentialing, security for private sector emergency responders, and emergency wireless protocols, are being addressed collaboratively by DHS/NCS and industry partners.

The seven Communications Sector security goals outlined in both Section 1 of this document and the CSSP form the framework for the R&D requirements. The requirements are developed with the realization of those goals in mind. Fulfillment of short- and long-term R&D requirements can influence how well the Communications Sector performs in achieving those goals, as the tools and technologies developed through R&D can greatly improve the capability to protect the Nation’s communications backbone.

The CSSP outlined a four-step cyclical process called the CIKR Protection R&D Process, by which the NCS identified requirements and measured progress toward their fulfillment. Those four steps are as follows:

- *R&D Collaboration*. The NCS collaborates with industry and Government partners to characterize the communications network.

- *Identification of R&D Requirements*. The NCS and its partners solicit and exchange information regarding the Communications Sector’s R&D requirements and create a list of requirements.

- *Analysis of R&D Gaps*. The Communications Sector performs a gap analysis to identify levels of goal maturity.

- *Establishment of R&D Priorities*. R&D priorities are identified to inform the effective allocation of limited resources to Communications Sector security partners.

3.1 Modeling and Simulation

The NCS has long been at the forefront of the government’s efforts to model, simulate, and analyze the Communications Sector’s infrastructure using its Network Design and Analysis Capability (NDAC) tool. The use of the NDAC provides Federal departments and agencies with analyses of their telecommunications infrastructure, enabling modeling and analysis of the public switched network (PSN), including the PSTN; Internet Protocol (IP) networks; Internet telephony; next-generation packet switched networks; control systems; and cable, wireless, and satellite networks. The utilization of the NDAC also enables studies of natural and man-made disruptions to the PSN and provides the ability to conduct vendor independent analyses, create models and methodologies to identify vulnerabilities and congestion, and identify network effectiveness solutions.

3.2 Progress

Major Projects Completed

Pandemic Influenza Study - The Homeland Security Council's May 2006 document entitled *National Strategy for Pandemic Influenza Implementation Plan* identified telecommuting as a key component of the national response to a pandemic influenza. This document raised concerns as to whether telecommunications infrastructures and enterprise networks are prepared to handle the anticipated change in communications traffic in response to a pandemic influenza. In 2007, the NCS, in collaboration with the industry, undertook a study of the impact of pandemic influenza on communications networks in order to address this concern. The study focused on the technical feasibility of national policy and business continuity planning related to telecommuting in response to a pandemic influenza threat. The study:

- Evaluated the potential impact on the telecommunications infrastructures and enterprise networks in the event of a pandemic influenza in the United States.

- Provided analysis and recommendations to critical infrastructures on enterprise-level communications issues that may arise during a potential pandemic influenza.

- Provided analysis and recommendations on national telecommuting policy and business continuity planning for a pandemic influenza threat.

After the conclusion of the pandemic study, the Communications Sector has performed outreach to CIKR stakeholders and the financial sector to educate them on the final result of the analysis. Most recently, the Communications Sector has participated in a joint IT/Communications Pandemic Flu Planning webinar to share planning efforts at the Federal level with owners and operators at the operational level.

Internet data modeling and analysis The Nation is becoming ever more dependent on the Internet and data networks, which represents one of the biggest areas of growth and concern in the Communications Sector. In response, the NCS continues to examine how Federal agencies and departments rely on data networks, how they connect to the Internet, the vulnerabilities that exist in Federal data network connectivity, and the consequence of disruptions in service, such as congestion or loss, that arise due to NS/EP incidents.

In an effort to facilitate DHS support of the Federal government cyber security needs, the NCS continues to develop NDAC capabilities for conducting network analysis. The NCS's primary area of focus in the past year has been the development of analytical tools and methods that baseline the logical and physical infrastructure assets of the cyber networks. This information, when used in concert with other critical Sector data, provides the NCS the means to assess cross-sector dependencies on the Internet. The NCS has developed a suite of tools and capabilities to analyze this information, including the Internet Analysis Tool (IAT) and its collected datasets. Over the past year, the IAT has been leveraged to conduct network topology assessments and holistic analyses of federal networks and their connectivity to the Internet. Moving forward, the NCS seeks to refine the above capability in order to better support the Trusted Internet Connection (TIC) initiative and assist government in moving towards its cyber security goals.

Next-generation networks (NGN) modeling and analysis -The industry offers priority service restoration to Federal departments and agencies through the GETS, WPS, and TSP programs.

NGPS is being developed by the NCS and its industry partners. However, as technological advancements are made, the complexity of communications infrastructure and networks increases. Complex networks involving a multitude of new and existing technologies and protocols are referred to as NGN. As communications and IT architectures converge, priority mechanisms that have been implemented on the PSTN, such as GETS, will be provided by IP networks through a next generation NS/EP priority service. It is vital to the role of the NCS as the SSA for the Communications Sector to be able to sustain NS/EP communications during times of severe network congestion and/or disruption. Unfortunately, the NCS has been facing severe funding constraints and therefore, its effort to continue to work with industry on the migration of GETS services to an IP platform has been significantly hampered. It is critical that the NCS continues with its pursuit of upgrading the GETS capability within the next couple of years in order to maintain the GETS service.

Development of priority services is being supported by an iterative and exploratory process that includes four main areas: architecture development, modeling and analysis, prototyping, and industry requirements. The NCS applies modeling and analysis as an ongoing process to support NS/EP strategic and tactical needs, such as severe congestion and infrastructure damage. The modeling and analysis group within the NCS utilizes output from the architecture development and industry requirement groups to help determine whether a solution satisfies a particular cost metric or quality of service threshold. The results of these simulations can be verified through prototyping and used by standards bodies to either modify or create new standards.

This effort’s overall objectives center around the following requirements:

- Provide timely quantitative analyses of, and recommendations on, specific NGN GETS industry requirements issues that can be addressed by modeling.

- Provide quantitative analyses of, and recommendations on, industry developments and corresponding NS/EP implications by developing and exercising models that track longer term industry capabilities.

- Test the effectiveness (performance, security, availability) of candidate NS/EP protocol and technology enhancements through prototype developments and experiments.

- Integrate prototyping capability and modeling team activities to support GETS program requirements.

This past year’s primary NCS contributions to the priority services program included continued development of the Universal Mobile Telecommunications System (UMTS) access model, establishment of the IP Multimedia Subsystem (IMS) core model, and the design of appropriate call flows to accurately model the Session Initiation Protocol (SIP) in a proxy server and IMS architecture environment. The creation of a tailored user interface, the Timing Information System (TIS), allowed for enhanced understanding of model results. Various scenarios and case studies were demonstrated across the models including: NGN call establishment delay, call setup performance, mobile access congestion identification, and network throttling considerations. Many of the studies performed were in response to ad hoc questions that arose during the continued development of the NGN GETS service. Ongoing studies also include call admission control comparisons, policy control attribute establishment, additional wireless access modeling, wireless survivability determinations, and application server architecture demonstrations.

The benefits of the NGN event simulation models were immediately recognized through feedback to NCS and industry partners. The accurate demonstration of NS/EP call flow messaging, precise timing information and high fidelity environment of the models allowed expression of complex interactions to aid decisions for the development of the NGN GETS priority service.

Major Initiatives

Recognizing that the research area needs of the Communications Sector often overlap with the IT Sector and cross-sector cyber requirements, the NCS worked with NCSD and the Directorate for Science and Technology (S&T) in developing a Broad Agency Announcement (BAA) calling for R&D efforts in nine technical topic areas (TTA). This BAA continues to serve as the basis for future R&D endeavors among the NCS, NCSD, and S&T.

Of the 9 topics advertised by S&T via the BAA process, 14 awards were made covering 8 of the 9 topics. The NCS has worked closely with S&T throughout the BAA process and actively participated in the drafting of requirements scoping, proposal review process and corresponding S&T-led follow-up meetings (e.g., Principal Investigator (PI) meeting). NCS is also working directly with the institution awarded proposal funding under TTA #5 - Internet Tomography/Topography - to ensure NCS R&D requirements are fulfilled and current NCS Internet data modeling capabilities are enhanced. These capabilities are also leveraged to answer a number of Internet-related analysis questions (e.g., Identification of the Top 100 Communications Assets).

The Office of Cybersecurity and Communications within the National Protection and Programs Directorate (NPPD) is working with S&T on the submission of additional R&D requirements to meet multiple objectives associated DHS cyber security requirements within the areas of data collection, fusion, analysis, visualization, and sharing capabilities.

R&D Efforts That Address Interdependencies

The NSRA (described in Section 1.2) recommends scoping future work for interdependencies between the Communications Sector and other sectors critical to communications through government-sponsored cross-sector dependency analyses and other analysis methods. The NSRA only addressed direct impacts on the Communications Sector; however, indirect impacts on the communications infrastructure may cause severe national impacts that need to be assessed. Potential R&D activities may arise in the future based on the inherent interdependencies between the Communications Sector and other sectors.

R&D Information Sharing Communities

The process of identifying and refining R&D requirements has been shaped by multiple industry and Government collaborative efforts, and influenced by several key R&D-related documents.

The NCS has collaborated with partners from Federal, State, local, and tribal governments and industry to collect and develop R&D priorities for the Communications Sector.

The NSTAC is the NCS's direct link with communications industry partners in this area. The group is currently planning its 2008 R&D Exchange Workshop, which will take place in September 2008. The 2008 R&D Exchange Workshop will focus on emerging issues in the areas of:

- Identity Management for NS/EP Communications
- Defending Cyberspace
- Emerging Technologies that impact NS/EP Communications
- Convergent Technologies and;
- Emergency Communications Response Networks

All recommendations resulting from the workshop will be shared with the NCS and carefully considered for further actions by NSTAC.

In addition to coordinating with industry, the NCS collaborates with several other Government agencies to define R&D needs and priorities. The most prominent of these collaborations is an interagency effort involving the S&T, NCSD, and the NCS. The results of this activity are provided as Government capability gaps in Section 3.3. The NCS also works with the intelligence community on various R&D related efforts, as well as the Department of Defense's (DoD) Real Time Services Working Group and the Homeland Infrastructure Foundation-Level Data (HIFLD) Working Group. HIFLD members are involved in a wide range of different functions including: Critical Infrastructure Protection (CIP), Crisis and Consequence Management, Intelligence and Threat Analysis, and Man-Made and Natural Hazard Modeling. The NCS also continues to reach out to the National Infrastructure Simulation and Analysis Center (NISAC) for potential future collaboration on critical interdependencies with other sectors.

3.3 Capability Gaps

Table 3-1:	Communications Sector Capability Gap Statement
Questions	**Response**
Capability Gap Statement Tracking and Priority Number	2008 – 001 – Communications
Is this submission an MS&A or R&D requirement?	Yes, both
Proposed Title of Requirement	DHS Cyber Security
Goal/Objective to which Requirement Responds	The Federal government has made cyber security a top priority

Theme	This requirement cuts across all nine CIKR protection themes
Threat Identification	According to a GAO-performed study: "Federal agencies are facing a set of emerging cyber security threats that are the result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms. Examples of these threats include *spam* (unsolicited commercial e-mail), *phishing* (fraudulent messages to obtain personal or sensitive data), and *spyware* (software that monitors user activity without user knowledge or consent)."
Gaps of Existing Capabilities	Current Federal cyber security systems are not in line with the goals and objectives of government cyber security needs.
Description of Required Operational Capability	The Communications and IT Sectors need to drive improvement in the current collection, fusion, analysis, visualization, and sharing of data in order to meet the Government's cyber security needs as well as support Sector missions.
Identification of Existing Related Capabilities or Technology	Current Communications and IT Sector activities surrounding cyber security include but are not limited to: • Botnet detection and mitigation • Cyber security metrics • Network data visualization for information assurance • Internet tomography/topography • Routing security management tool • Process control system security • Insider threat detection and mitigation
Identification of Possible Approaches/Solutions	Request is for funding and support for the aforementioned activities, which will help to address current cyber security R&D and MS&A capability gaps within both the Communications and IT Sectors.

Section 4: Funding Priorities

4.1 Planned SSA Investments

Table 4-1: Communications SSA Investments

Sector:	Communications				
Agency:	Department of Homeland Security, National Communications System				
Program/ Investment Title	Priorities Addressed	Program/ Investment Description:	OMB Account	Included in the HSDB?	Budget

		How Program/ Investment Supports CIKR Protection			FY08 Request	FY08 Enacted	FY09 Request (est.)	FY09 Enacted (est.)
Priority Telecommunications (PT)		PT is a diverse set of mature and evolving activities designed to ensure priority use of communications services by NS/EP users during times of national crisis, including GETS, a nationwide landline telephone service that provides priority NS/EP telecommunications for the President; Federal, State, and local Governments; and industry organizations; WPS, a nationwide wireless telephone service that interoperates with GETS and provides priority NS/EP telecommunications via selected commercial wireless carriers; and Special Routing Arrangement Service, a GETS service for special users. NGNs will transition existing priority telecommunications features to NGN as well as acquire priority broadband capabilities. Each of these programs forms the core of the Sector's protective measure strategy, focusing primarily on response and recovery.	024-65-0565	Yes	**$124.766,000**	**$93,802,000**	$109,778,000	

Sector:	Communications
Agency:	Department of Homeland Security, National Communications System

Program/ Investment Title	Priorities Addressed	Program/ Investment Description: How Program/ Investment Supports CIKR Protection	OMB Account	Included in the HSDB?	Budget			
					FY08 Request	FY08 Enacted	FY09 Request (est.)	FY09 Enacted (est.)
Programs to Study and Enhance Telecommunications (PSET)		PSET directly support the NS/EP mission, focusing on telecommunications network resiliency, security, performance, and analysis of risks and vulnerabilities. These programs analyze and assess risks to current and next-generation communications systems; recommend appropriate protective standards and measures; inform the Sector of new and effective NS/EP-related technologies; develop a thorough understanding of the physical Internet architecture; and develop and evaluate products and technologies related to critical network infrastructure.	024-65-0566	Yes	$16,733,000	$16,000,000	$15,100,000	
Critical Infrastructure Protection (CIP)		CIP provides the core capability to monitor the status of the Sector, respond to threats, and respond and recover communications after an event. To do so, the NCC implements or conducts CIP operations, plans, and policy; analytical assessments of the telecommunications infrastructure;	024-65-0567	Yes	$10,905,000	$16,100,000	$11,260,000	

Sector:	Communications							
Agency:	Department of Homeland Security, National Communications System							
					Budget			
Program/ Investment Title	Priorities Addressed	Program/ Investment Description: How Program/ Investment Supports CIKR Protection	OMB Account	Included in the HSDB?	FY08 Request	FY08 Enacted	FY09 Request (est.)	FY09 Enacted (est.)
		continuity of operations; training and exercises; NSIEs to share threat information and develop coordinated countermeasures with industry; and priority telecommunications services.						
Industry Government Interagency Processes (IGIP)		IGIP manages the executive and technical support of the NCS System Committee of Principals and the NSTAC to formulate recommendations on national policies pertaining to NS/EP communications; seeks and establishes partnerships and alliances with key industry and Government entities associated with homeland defense and CIP to maximize NCS support to homeland security; develops a strategic outreach and communications program to raise awareness about the NCS and its programs and activities; conducts analyses of the ever-changing technological and corporate environments of the industry and the governmental legislative, regulatory, and political climates.	024-65-0568	Yes	$6,037,000	$6,037,000	$4,704,000	
Agency Total:					$158,441,000	$131,939,000	$140,842,000	

4.2 Non-SSA Investments

Industry owners and operators and Federal government departments and agencies with a stake in NS/EP communications continue to make significant investment in Communications Sector response and recovery programs, which contribute to the overall protection of the sector.

4.3 SSA Gaps

The NCS's mission to ensure NS/EP communications for the Federal Government uniquely positions it as the Communications Sector SSA. NCS's programs address both its NS/EP communications and CIP responsibilities. Because of the NCS's unique standing as the SSA, having its programs serve in dual-roles to address primary mission and SSA responsibilities, funding shortfalls for the NCS's programs will also be reflected in Communications Sector protective programs. The NCS experienced a cut in its FY08 budget that has impacted all of the NCS including its critical infrastructure protection program, and protective programs in priority services, modeling and simulation. This shortfall's impact has, and may continue to hamper the NCS's ability to maintain pre-FY08 funding levels for its protective programs, which in turn may create new capability and protection gaps that must be addressed to ensure the NCS can fulfill its mission and SSA responsibilities.

The NCS's highest profile protective program effort, transitioning its priority communications' GETS and WPS from a circuit-switched environment into the IP world, has been greatly impacted by the FY08 budget shortfall. This program has been labeled as the NCS's NGN priorities services effort, although it's been well established that the technological environment the effort is trying to move to already exists today in the marketplace. Therefore, the NGN program must move quickly to establish priority communications in the already ubiquitous IP environment to ensure the NCS can continue to provide its NS/EP services. As increasing number of telecommunications carriers are migrating to an IP platform, the risk of the NCS suffering a mission-critical capability gap greatly increases without adequate funding.

Additionally, the NCS's budget shortfall also affects its ability to implement the CSSP. Due to the FY08 shortfall, the NCS has no funding available to address it's responsibility as the SSA to conduct a detailed risk assessment and cross-sector dependency study as follow up activities to the recently-completed NSRA. More specifically, the lack of sufficient funding impacts the program-management as well as the modeling, simulation and analysis capabilities of the NCS. The risk of a capability gap in the NCS's ability to identify and prioritize Communications Sector architecture increases substantially due to inadequate funding to address the above areas of concern.

Section 5: CIKR Protection: Security Practices and Obstacles

5.1 CIKR Protection Security Practices

The Communications Sector's security practices focus on built-in resiliency, response, and recovery. These security principles are by nature customer driven; owner/operators must offer reliable service and quickly respond to and restore service when an outage occurs. To ensure the security of the Communications Sector, owner/operators regularly perform risk assessments on their facilities; have in place a suite of physical, cyber, and human security measures; and collaborate with other companies and trade associations on best practices.

5.1.1 Industry Self-Risk Assessments

Given the diverse nature of the communications industry – broadcasting, cable, satellite, wireless, and wireline – the creation of a common methodology for self-assessments is impractical. As with engineering and operational activities, specific risk-management methodologies used by companies are closely guarded. In general, changes to systems, processes, buildings, and the environment can have an impact on the level of security. Corporate self-assessments are conducted regularly as a part of companies' business continuity practices to verify compliance with policies, standards, contracts, and regulations.

Most companies use a standard process methodology for developing assessments. For example, prior to conducting a risk assessment of a facility, personnel must first understand the function of the facility. If an on-site inspection is required, employee interviews are used to determine the effectiveness of security solutions and processes. Results are analyzed and recommendations are developed and presented to the appropriate management team to begin addressing the recommendations. Progress on implementation of the recommendations is monitored by the company to ensure risks are addressed in a timely fashion. Furthermore, business relationships with vendors and business partners may require companies to perform regular assessments on another company's facility to ensure that their assets are not at increased risk and contract requirements are being met. Any issues that are discovered are discussed with the vendor or business partner, and a remediation plan is determined.

5.1.2 Security Measures

Security measures in the Communications Sector address physical, cyber/logical, and human security vulnerabilities and threats. The scope of the security measures also addresses the scope of CIKR protection, including protection and preparedness measures, as demonstrated in Table 6-2. Similar to industry self-assessments, specific security procedures exercised by individual companies are closely guarded, proprietary information.

- *Physical Security*. These measures vary depending on the characteristics of the asset's location, function in the architecture, and customer requirements. Types of assets typically include data centers, switch sites, point-of-presence sites, warehouses, call centers, retail stores, and general office buildings. For example, transmission lines that are omnipresent cannot receive the same level of security as an end office.

- *Cyber/Logical Security*. These measures are a critical security element for the infrastructure provider. Communication companies have created extensive cyber security programs designed to protect their networks from malicious attacks and unauthorized activity. Similar to the other security elements, they vary; however, some common practices exist throughout the Communications Sector. For example, access control lists and reverse path forwarding are two common practices that carriers take to secure the signaling and control planes.

- *Human Security*. These elements also vary depending on a company's human resources policies. For example, companies may screen employees to confirm their backgrounds and provide assurance of necessary trustworthiness; rotate assignments to reduce the chance of fraud and misuse of resources; enforce separation of duties and least-privilege policies; conduct periodic security awareness training; implement password and account management policies and practices; log, monitor, and audit employee online activity; monitor and respond to suspicious or disruptive behavior; and deactivate access following termination. The purpose of these procedures is to mitigate the threat posed by insiders and a company's reliance on individual employees. The Communications Sector also uses robust business continuity plans for assessing threats, vulnerabilities, and countermeasures with sound business practices to develop and maintain an appropriate state of resiliency and preparedness within the company.

Table 6-2 Examples of Protective Measures

Protective Category		Protective Measure Examples
Protection	Deter	Facility surveillance Facility and network access controls
	Devalue	Backup network operations centers Synchronous optical network ring networks
	Detect	Facility alarm systems Network monitoring
	Defend	Buffer zones for critical facilities Firewalls on control system networks
Preparedness	Mitigate	Self-healing networks Redundant signaling systems GETS, WPS, NCC
	Respond	Emergency response plans, procedures, and exercises
	Recover	Business continuity plans Mutual-aid agreements NCC, TSP

5.1.3 Business Best Practices

The development of industry best practices is prevalent in the Communications Sector. Best practices are derived from insights from historic technical support experience of individual companies that address communications infrastructure vulnerabilities. Best practices are presented to the industry only after sufficient rigor and deliberation over conceptual issues and particular wording of the practices have been established. The goals developed throughout the CSSP consider the many dimensions of the protective spectrum. In many cases, security partners leverage existing programs and best practices to set the Communications Sector goals for securing physical, cyber/logical, and human elements. Industry partners support best practices processes, although due to the Communications Sector's diversity, true Sector-wide, risk-management and Sector-specific best practices are difficult to define.

5.2 Obstacles

Impediments to the success of the Communications Sector's initiatives outlined in the CSSP and highlighted in this report can be categorized into three areas: funding, information sharing, and access.

- *Funding*. Funding of new protective programs may be an impediment for the private sector and Government. Industry will be challenged by its customers and shareholders to justify additional security measures for some assets and networks, if they extend beyond customer requirements or evolving marketplace demands. While security is a priority for Government, budget realities may prohibit the development and implementation of protective programs for all of the identified high-risk assets, networks, and functions that warrant national attention. Funding for basic research in this Communications Sector also needs to be increased.

- *Information Sharing*. Information sharing can be a challenge to the success at all levels of the program. Most importantly, industry is concerned with the protection of proprietary data from unauthorized use and public disclosure. Industry may also be reluctant to share infrastructure and vulnerability data with Government because compiling the data may create additional vulnerability. For the information-sharing relationship to be mutually beneficial, Government and it's security partners need to work together to ensure continuous improvement in the exchange of threat and vulnerability information on a timely basis as well as provisioning for the necessary level of access to sensitive information.

- *Access*. Emergency service providers require rapid access to a disaster site to restore communications. As an example, during the Hurricane Katrina response, telecommunication restoration crews were initially denied access to the disaster area. Once crews were allowed entry, they were reluctant to enter the area due to the lack of security. Priority access to fuel, staging areas, and lodging for restoration crews also delayed restitution of communications critical to the response. While efforts have been made to correct these shortfalls, these processes have not been verified with any formal study. In addition, there is still ambiguity in interpretation of statute that is needed to assist in gaining access to restricted areas and help in obtaining fuel, water, power, billeting, and workforce and asset security.

Section 6: Program Effectiveness and Continuous Improvement

6.1 CIKR Protection Mission Progress

The Communications Sector has made significant progress in completing specific actions and milestones in pursuit of advancing the seven goals detailed in its CSSP. The Communications Sector accomplished this by aligning existing CIKR protective programs and risk management decisions with the seven goals, in addition to enhancing the foundation for these protective programs through collaboration with Sector security partners. The three most significant partnerships for improving situational awareness, sharing information, and developing best practices include the NCC, NSIE, and the CSCSWG. These three partnerships promote communication between and among the Communications Sector and security partners outside the Sector through unique operating mechanisms such as Information Sharing and Analysis Centers and sector liaisons.

The NCS and its Communications Sector partners' highest priority objectives focused on the completion of the Communications NSRA to meet the goals outlined in the CSSP. The NSRA identified risks to the national communications infrastructure. Results from the NSRA will be used to guide future risk management decisions and investments following review and further analysis by the CGCC and the CSCC.

The Communications Sector continues to make considerable progress in implementing the NIPP Risk Management Framework. The NCS also manages several CIKR protective programs, in collaboration with the private sector security partners designed to mitigate the impact of network congestion, improve access, and expedite provisioning for national security/emergency preparedness users. The following programs are key focus activities:

- Government Emergency Telecommunications Service (GETS) - provides emergency access and priority processing in the local and long-distance segments of the Public Switches Telecommunications Network (PSTN). This service increases the likelihood that national security/emergency preparedness personnel can complete critical calls during periods of PSTN disruption and congestion.

- Wireless Priority Service (WPS) - provides priority commercial mobile radio services during and after emergencies for national security/emergency preparedness personnel by ensuring WPS calls receive the next available radio channel during times of congestion.

- Next Generation Priority Services (NGPS) – currently under development, this technology will provide priority service capabilities over the Internet, standardize the technology across industry through the commercial standards process, and transfer current priority services features to the Internet.

- Telecommunications Service Priority Program (TSP) - provides the regulatory, administrative, and operational framework for priority restoration and provisioning of national security/emergency preparedness communications circuits in an emergency.

The Communications Sector has made significant progress regarding their efforts to narrow several key gaps identified in its 2007 SAR, including cross-sector interdependencies, concentration of communications assets, cyber vulnerabilities, and an increased understanding of consequences as described in greater detail in sections 1.3 and 3.2. The NCS and its industry partners, through the NCC, have been actively involved in addressing interdependency issues through the U.S./Canada Civil Emergency Planning Telecommunications Advisory Group (CEPTAG) and the Security and Prosperity Partnership. Members of the IT SCC, CSCC, and CGCC support the ongoing efforts of the NSTAC including the report on International Communications, yielding the August 2007 NSTAC Report to the President on International Communications.

The Communications Sector continues to make substantial progress in accomplishing the goals and objectives in the NIPP and its CSSP. The Communications Sector's activities implemented in 2008 demonstrate its robust CIKR protection approach. Completion of the NSRA and strengthened partnerships with the CGCC and CSCC enable the Communications Sector to build on its success and focus on engaging State, local, tribal and territorial governments in the CIKR protection process.

Sector Specific Metrics (Industry Metrics)

The national communications infrastructure consists of numerous architecture elements owned by various communications service providers that use diverse technologies and modes of connectivity to provide voice, data and video services. The industry invests billions of dollars in designing, building, operating and maintaining robust communications networks, which are designed with a high degree of intra-segment diversity (e.g., within wireline) and cross-segment resiliency (e.g., between wireless and wireline), to provide reliable, cutting edge services to customers. This diversity and resiliency reduces substantially the overall risk of loss of communications to the national communications infrastructure and its users.

Industry also routinely conducts self-assessments as an important part of its business operations, which further strengthens the Communications Sector's CIKR protection posture. Corporations conduct these self-assessments to verify compliance with policies, standards, contracts, and regulations and to prevent economic loss resulting from service degradation or disruption.

The CSCC, which represents over 35 communications companies and trade associations, is currently forming a working group, which will investigate methodologies to effectively measure the industry portion of the Communications Sector's progress in its CIKR protection posture. These sector-specific metrics will be aligned with the goals the Communications Sector identified in the CSSP and focus on the following areas:

- Communications Sector diversity
- Cyber security
- Impact of other sectors on the Communications Sector
- Access/Credentialing/Fuel/Security metrics

6.2 Path Forward

The CGCC and the CSCC will be working in collaboration to determine the next steps in the implementation of the CSSP. The ability of the of the NCS as the SSA to meet the goals set forth in the CSSP will greatly depend on the amount of resources available for future programs studies and activities. The two groups will use already established Working Groups or create new ones to commence future projects. As mentioned in Section 1.4 and other parts of the document, the communications security partners will:

- Continue to develop next-generation priority services to meet the evolving requirements of critical communications customers in a converged communications environment.

- Develop a Communications Sector outreach program to educate Communications Sector customers and other infrastructures on communications infrastructure resiliency and risk-management practices

- Focus on cyber security related programs and activities.

- Explore follow-on activities to the NSRA.

Appendix 1: 2008 Sector Summary Protection Information Requirements Report

The Communications Sector relies on timely and accurate information regarding threats and vulnerabilities in order to proactively address risk and effectively accomplish its national security and emergency preparedness (NS/EP) mission. To accomplish this, the Sector depends on the National Coordinating Center, Communications Information Sharing and Analysis Center, Network Security and Information Exchanges, the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and other information sharing avenues in the Sector. The Sector continues to emphasize the need for timely and actionable threat information that can be distributed broadly throughout the Sector. In addition, the Communications Sector needs more Government and industry representatives with proper level of security clearances.

Though industry regularly conducts internal risk assessments as normal business practice, the Government must develop the means by which to augment these assessments with real-time real world threat information. The Sector hopes that it can help to develop a more efficient information sharing backbone to facilitate the dissemination of sensitive infrastructure information. The Sector had described difficulties in the dissemination of sensitive information from programs like HITRAC in its 2007 CIKR Annual Report. Over the past year, the NCS and HITRAC have been working together to make improvements in the information-sharing process.

The Sector also believes that the information reported out of HITRAC should attempt to provide greater detail as it pertains to the geographic locations of threats, the entities involved in the threats, the method by which the threat may be enacted, and what the general threat landscape is at any given point in time. A consideration that underlies all of these examples is that some threats may not be aimed at the Communications Sector or its assets, but still may be a threat based on its impact, its location, or due to a known or unknown cross sector interdependency. Not only are direct communications threats vital, but so are some of the indirect threats that may occur.

Regular briefings provided by HITRAC representatives to Communications Sector representatives would help to develop a better understanding of the capabilities of the programs and the expectations/desires of the Communications Sector of the program. In addition to regular briefings, HITRAC needs to consult with industry representatives when preparing analyses to ensure they accurately reflect how communications carriers and the network operate. The NCS, on behalf of the Sector, will continue to work with HITRAC to improve the information sharing process as well as to gain a better understanding of the HITRAC program's capabilities.

		NIPP Framework Chevrons					
		Set security goals	Identify assets, systems, networks, and functions	Assess risks (consequences, vulnerabilities and threats)	Prioritize risks	Implement protective programs	Measure effectiveness
Sector CIKR Protection Information Requirements	Threat/warning information and briefings (classified and unclassified)		X	X	X		
	Critical infrastructure risk assessments						
	Information-sharing tools/conduits/systems/technologies						
	Strategic (national level) Communications Sector risk analysis		X	X	X		
	Interdependency analysis		X	X	X		
	Decision support tools						
	Security practices/protective measures						
	Security clearances		X	X	X		

CIKR Protection Information Requirements Submission Worksheet

Tracking number: COM-1

CIKR Sector: Communications

NIPP Risk Management Phase: Identify assets, systems, networks and functions, assess risk, prioritize risk

Information Requirement Title: Threat/warning information and briefings

Information Requirement Description: The Communications Sector needs timely and pertinent threat information. The Communications Sector needs more detail as it pertains to geographic locations of threats, who are the actors involved in the threats, the types of actors who may carry out the threat (e.g., individual, cell, group), and the general landscape of the threat. In addition, the method by which the threat may be enacted is important. A consideration that underlies all of these examples is that some threats may not be aimed at the Communications Sector or its infrastructure, but still may be a threat based on its impact or location. Not only are direct communications threats vital, but so are some of the indirect threats that may occur. The frequency of the briefing would be when a significant change to the threat occurs or on a scheduled quarterly basis.

In addition to regular briefings, HITRAC needs to consult with industry representatives when preparing analyses to ensure they accurately reflect how communications carriers and the network operate.

Information Requirement Justification: By having more detailed and pertinent data on threats, a more accurate assessment can be made. This level of information can help industry and the NCS, working on behalf of the Communications Sector, in making critical resource, asset, financial, and people decisions. This would be of great benefit to the Communications Sector members and the customers that they provide service.

Submitting Organization/Agency: CSCC/CGCC

Point of Contact for Questions: Larry Hale

Phone: 703-235-5510
Email: larry.hale@dhs.gov

CIKR Protection Information Requirements Submission Worksheet
Tracking number: COM–3
CIKR Sector: Communications
NIPP Risk Management Phase: Identify assets, systems, networks and functions, assess risk, prioritize risk
Information Requirement Title: Interdependency Analyses
Information Requirement Description: The Communications Sector needs additional interdependency information to fully understand the different risks to the Communications Sector. This information would include both the cascading impacts that a communications outage may have on other sectors, to better understand its customer missions, as well as the cascading impacts resulting from outages in other critical infrastructures.
Information Requirement Justification: The Communications Sector is taking a top-down approach to risk assessments, which allows a thorough and effective means by which to assess risk not just for the Communications Sector, but cross-sector interdependencies as well.
Submitting Organization/Agency: CSCC/CGCC
Point of Contact for Questions: Larry Hale
Phone: 703-235-5510
Email: larry.hale@dhs.gov

CIKR Protection Information Requirements Submission Worksheet
Tracking number: COM-4
CIKR Sector: Communications
NIPP Risk Management Phase: Identify assets, systems, networks and functions, assess risk, prioritize risk
Information Requirement Title: Security Clearances
Information Requirement Description: The Communications Sector is in need of more individuals who hold Top Secret and Top Secret/Sensitive Compartmented Information (SCI) clearances. Private sector members need DHS to sponsor additional clearances to ensure that the right people are able to receive threat information.
Information Requirement Justification: Effective communication with the sector relies on the ability of Communications Sector representatives to be able to review classified threat data. Both industry and Government are in need of more credentialed individuals, especially at the SCI level to ensure data is shared and reviewed in a timely and effective manner.
Submitting Organization/Agency: CSCC/CGCC
Point of Contact for Questions: Larry Hale
Phone: 703-235-5510
Email: larry.hale@dhs.gov

Appendix 2: Completed Risk Reduction Activity Questionnaire

The following questionnaire was completed by the NCS as the SSA for the Communications Sector without input from the industry.

Activity Information	
Name of Program	Government Emergency Telecommunications Service (GETS)
Managing Entity	Department of Homeland Security/National Communications System
Required by Law	Yes
If so, which law	GOVERNING AUTHORITIES: Executive Order (EO) 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," 3 April 1984 (amended by EO 13286 of 28 February 2003) EO 13231, "Critical Infrastructure Protection in the Information Age," 16 October 2001 White House Memorandum, "National Level Telecommunications Program Implementation and Functional Requirements," 15 October 1991 NSDD 97, "National Security Telecommunications Policy," 13 June 1983 Presidential Decision Directive 67 (CLASSIFIED), "Enduring Constitutional Government and Continuity of Government Operations," 21 October 1998 EO 12656, "Assignment of Emergency Preparedness Responsibilities," 18 November 1988 (as amended)
Brief Description of Program	The Government Emergency Telecommunications Service (GETS) is a White House-directed emergency phone service provided by the National Communications System (NCS) in the Cyber Security & Communications Division, National Protection and Programs of the Department of Homeland Security. GETS supports Federal, State, Local, and Tribal Government, industry, and non-governmental organization (NGO) personnel in performing their National Security and Emergency Preparedness (NS/EP) missions. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). GETS is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased. GETS uses three major types of networks: long-distance networks, local networks, and

	Government-leased networks. National Security and Emergency Preparedness (NS/EP) Priority Telecommunications Service (PTS) is a White House directed program to provide specially designed telecommunications services to the NS/EP user community during natural or man-made disasters when conventional communications services are ineffective. These telecommunications services are used to coordinate response and recovery efforts, and in severe conditions, to assist with Continuity of Operations (COOP) and Continuity of Government (COG). Specifically, NS/EP PTS enhances the ability of NS/EP users to complete calls during crisis or emergency through a degraded Public Switched Network (PSN) using GETS, one of four NS/EP PTS components.
Activity Type	• Preparedness • Response/Recovery
Comments	GETS provides assured communications during NS/EP incidents, such as terrorist attacks, earthquakes, and hurricanes, to the broader national, state, local, and non-government NS/EP community.
Activity Scope	
Is this activity designed only to reduce risk in your own sector	No
Cross Sector Application	• Banking and Finance • Chemical • Commercial Facilities • Nuclear • Dams • Defense Industrial Base • Emergency Services • Energy • Food and Agriculture • Government Facilities • Healthcare and Public Health • Information Technology • National Monuments & Icons • Postal and Shipping • Communications • Transportation • Water • Maritime • Educational Facilities

Explanation

GETS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging the PSN, helps to ensure the preparedness of the Nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan, National Infrastructure Protection Plan.

Sector(s) or Subsector(s) Utilizing this Activity

- Banking and Finance
- Emergency Services
- Government Facilities
- Healthcare and Public Health
- Communications

Explanation

GETS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging the PSN, helps to ensure the preparedness of the Nation to prevent, respond to, and recover from, possible and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan of the National Infrastructure Protection Plan.

Attack Method Addressed Reduce Threat, Vulnerability, and/or Consequence

- Cyber - Directed Attack
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Cyber - Non-Directed Attack
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Nuclear Detonation
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological

Geographic Scope National

Comments GETS provides NS/EP users with priority telecommunications nationwide on a 24 hour, seven days a week basis.

Activity Budget Details

FY 2007 President's budget request	$19,538,000
FY 2007 enacted budget	$19,380,000
FY 2008 President's budget request	$18,946,000
FY 2008 enacted budget	$18,946,000
FY 2009 President's budget request	$19,708,000

Activity Operational Details

Activity Status	Execution
Comments	GETS has been deployed nationwide and provides priority treatment for NS/EP users to reduce the impact of a terrorist attack that disrupts or congests the landline public switched network. Additionally, GETS priority treatment enhancements exploit the robustness of the public switched network to reduce the vulnerability of a specific technology failure. GETS also addresses other overarching protection needs (e.g., communications, coordination, strategic planning, etc.) during NS/EP emergencies.

Additional Information/Comments

Activity Information

Name of Program	National Coordinating Center
Managing Entity	Department of Homeland Security/National Communications System
Required by Law	Yes
If so, which law	Components including: NCC 24x7 Watch operations, NCC programmatic support, and the NCS High Frequency (HF) Radio program (includes the Shared Resources (SHARES) HF Radio Program). The National Coordinating Center (NCC) is a joint industry-government body that provides a mechanism to respond to National Security and Emergency Preparedness (NS/EP) telecommunications incidents. The mission of the NCC is "to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all conditions, crises, or emergencies." GOVERNING AUTHORITIES:

	Executive Order (EO) 12472, “Assignment of National Security and Emergency Preparedness Telecommunications Functions,” 3 April 1984 (amended by EO 13286 of 28 February 2003) Homeland Security Presidential Directive 5, “Management of Domestic Incidents,” 28 February 2003 47 U.S.C. 606 “War Communications – Powers of the President,” 1996
Brief Description of Program	The National Coordinating Center Operations is an umbrella title encompassing operational.
Activity Type	• Physical/Personnel Security • Cyber Security • Identification/Prioritization • Assessments • Information Sharing/Coordination • Training/Exercises • Preparedness • Response/Recovery • Other
Comments	The NCC facilitates Communications Sector information coordination between government and industry.
Activity Scope	
Is this activity designed only to reduce risk in your own sector	No
Cross Sector Application	• Communications
Explanation	The NCC addresses coordination of National Security/Emergency Preparedness (NS/EP) communications across the full spectrum of communications including wireline, wireless, satellite, cable, equipment vendors, service providers, internet service providers, and broadcast through direct industry and government participation.
Sector(s) or Subsector(s) Utilizing this Activity	• Banking and Finance • Chemical • Nuclear • Dams • Defense Industrial Base • Emergency Services • Energy • Food and Agriculture • Government Facilities • Healthcare and Public Health • Information Technology • National Monuments & Icons

- Postal and Shipping
- Communications
- Transportation
- Water

Explanation

The NCC addresses coordination of National Security/Emergency Preparedness (NS/EP) communications across the full spectrum of communications including wireline, wireless, satellite, cable, equipment vendors, service providers, internet service providers, and broadcast through direct industry and government participation.

Attack Method Addressed
Reduce Threat, Vulnerability, and/or Consequence

- Aircraft as a Weapon
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Assault
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Biological - Contagious Human Disease
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Biological - Livestock and Crop Disease
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological

- Biological - Non-Contagious Human Disease
    - Threat - Intent
    - Threat - Capability
    - Vulnerability - Recognizability
    - Vulnerability - Countermeasure Effectiveness
    - Vulnerability - Robustness/Resistance
    - Consequence - Loss of Life
    - Consequence - Economic
    - Consequence - Psychological
- Chemical
    - Threat - Intent
    - Threat - Capability
    - Vulnerability - Recognizability
    - Vulnerability - Countermeasure Effectiveness
    - Vulnerability - Robustness/Resistance
    - Consequence - Loss of Life
    - Consequence - Economic
    - Consequence - Psychological
- Cyber - Directed Attack
    - Threat - Intent
    - Threat - Capability
- Cyber - Non-Directed Attack
- Food or Water Contamination
- Improvised Explosive Device
- Maritime Vessels as Weapons
- Nuclear Detonation
- Radiological Dispersal Device
- Standoff Weapons - Guided
- Standoff Weapons - Unguided
- Vehicle-Borne Improvised Explosive Device

Geographic Scope	National
Comments	The entire communications infrastructure.

Activity Budget Details

FY 2007 President's budget request	$4,592,000
FY 2007 enacted budget	$4,555,000
FY 2008 President's budget request	$4,389,000
FY 2008 enacted budget	$3,853,000
FY 2009 President's budget request	$4,536,000

Activity Operational Details

Activity Status	Execution
Comments	The NCC Watch is responsible for 24x7 coordination of communications critical infrastructure protection information among Government and industry partners to assist in the response to any incident impacting the communications infrastructure. It enhances the physical and cyber security of the Nation's critical communications infrastructures by facilitating cooperation, information sharing, and system-to-system interaction among the critical infrastructures and between the Government and the private sector. The NCC averts or mitigates impact on the communications infrastructure by collecting, analyzing, and sharing information on threats, vulnerabilities, intrusions, and anomalies from the communications industry, Government, and other sources. The NCS HF Radio Program provides technical, administrative, operational, and readiness support to four emergency DHS/NCS HF radio operational activities: SHAred RESources (SHARES) HF Radio Program, NCC HF Radio Program (NCC-HF), the NCS Regional Managers HF Radio Program (NCS RM-HF), and the NCS Auxiliary HF Radio Program (NCS AUX-HF). These programs support a nationwide radio network of approximately 1,300 HF radio stations contributed by 98 Federal, state and industry organizations to form a nationwide emergency message-handling network. SHARES has made a significant contribution to NS/EP support in over 40 emergencies since it was formally established in 1989 and serves as a backup HF communications vehicle linking key Federal entities with the major telecommunications infrastructure service providers. The NCS HF Radio Program supports the NCS mission of coordinating the restoration of communications services (Emergency Support Function- 2, Communications) under the National Response Plan (NRP) and is an essential tool supporting the NCC mission. At present, there is no functional equivalent to the NCS HF Radio Program that coordinates and interfaces with key Federal and Industry radio entities.

Additional Information/Comments

Activity Information

Name of Program	Network Security Information Exchanges (NSIE)
Managing Entity	Department of Homeland Security/National Communications System
Required by Law	No
If so, which law	
Brief Description of Program	The joint meetings of the NSIE, including members from the President's National Security Telecommunications Advisory Committee (NSTAC)

	and Government Network Security Information Exchanges (NSIEs) provide a trusted environment in which industry and Government representatives exchange information on threats to and vulnerabilities of the Public Network (PN). The NSIEs focus on technical issues affecting the security of the PN, such as unauthorized penetration or manipulation of the PN software, databases, and other infrastructures supporting national security/emergency preparedness telecommunication services. The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the PN and its supporting infrastructures. Members of the Government NSIE represent agencies that have research, standards, regulatory, law enforcement, or intelligence functions related to the PSN, or are major telecommunications users. NSTAC NSIE members include representatives from telecommunications service providers, equipment vendors, systems integrators, and major users.
Activity Type	• Cyber Security • Assessments • Information Sharing/Coordination
Comments	
Activity Scope	
Is this activity designed only to reduce risk in your own sector	No
Cross Sector Application	
Explanation	
Sector(s) or Subsector(s) Utilizing this Activity	• Banking and Finance • Defense Industrial Base • Government Facilities • Information Technology • Communications
Explanation	
Attack Method Addressed Reduce Threat, Vulnerability, and/or Consequence	• Cyber - Directed Attack o Threat - Intent o Threat - Capability o Vulnerability - Recognizability o Vulnerability - Countermeasure Effectiveness o Vulnerability - Robustness/Resistance o Consequence - Loss of Life o Consequence - Economic o Consequence - Psychological • Cyber - Non-Directed Attack

- Threat - Intent
- Threat - Capability
- Vulnerability - Recognizability
- Vulnerability - Countermeasure Effectiveness
- Vulnerability - Robustness/Resistance
- Consequence - Loss of Life
- Consequence - Economic
- Consequence - Psychological

Geographic Scope	National
Comments	

Activity Budget Details

FY 2007 President's budget request	$607,000
FY 2007 enacted budget	$602,000
FY 2008 President's budget request	$580,000
FY 2008 enacted budget	$509,000
FY 2009 President's budget request	$392,000

Activity Operational Details

Activity Status	Execution
Comments	The NSIEs meet jointly every two months and share information with the objectives of: • Learning more about intrusions into and vulnerabilities affecting the public network (PN) • Developing recommendations for reducing network security vulnerabilities • Assessing network risks affecting network assurance • Acquiring threat and threat mitigation information • Providing expertise to the NSTAC on which to base network security recommendations to the President NSIE representatives voluntarily share information related to threats, incidents, and vulnerabilities affecting operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. This information includes attempted or actual penetrations or manipulations of software, databases, and systems related to critical NS/EP telecommunications. Representatives also share information on tools and techniques used to conduct and prevent attacks. In addition, representatives share information on physical intrusions pursuant to attacking critical telecommunications assets. Although most

often NSIE representatives share their information at the bimonthly meetings, events occur that warrant a more rapid response and representatives communicate with each other on an ad hoc basis between meetings. Through personal contacts, telephone, and e-mail, NSIE representatives have developed an informal, accelerated information sharing capability. In addition, relationships with NSIE representatives provide Government with industry points of contact to confirm events in real-time. NSIE member organizations are required to sign a nondisclosure agreement, and their representatives and all guests are required to sign a personal acknowledgment before they attend their first NSIE meeting. All representatives must have a SECRET security clearance.

Additional Information/Comments

Activity Information

Name of Program	Next Generation Priority Service (NGPS)
Managing Entity	Department of Homeland Security/National Communications System
Required by Law	Yes
If so, which law	GOVERNING AUTHORITIES: Executive Order (EO) 12472, “Assignment of National Security and Emergency Preparedness Telecommunications Functions,” 3 April 1984 (amended by EO 13286 of 28 February 2003) EO 13231, “Critical Infrastructure Protection in the Information Age,” 16 October 2001 White House Memorandum, “National Level Telecommunications Program Implementation and Functional Requirements,” 15 October 1991 NSDD 97, “National Security Telecommunications Policy,” 13 June 1983 Presidential Decision Directive 67 (CLASSIFIED), “Enduring Constitutional Government and Continuity of Government Operations,” 21 October 1998 EO 12656, “Assignment of Emergency Preparedness Responsibilities,” 18 November 1988 (as amended)
Brief Description of Program	National Security and Emergency Preparedness (NS/EP) Priority Telecommunications Service (PTS) is a White House directed program to provide specially designed telecommunications services to the NS/EP user community during natural or man-made disasters when conventional communications services are ineffective. These telecommunication services are used to coordinate response and recovery efforts and, in severe conditions, to assist with Continuity of Operations (COOP) and Continuity of Government (COG). Specifically, NS/EP PTS enhances the ability of NS/EP users to complete calls during crisis or emergency

	through a degraded Public Switched Network (PSN) using NGPS, one of four NS/EP PTS components. NGPS is a technology insertion initiative to maintain and migrate legacy priority voice telecommunications features and to apply priority to data applications as the PSN evolves to NGN.
Activity Type	• Preparedness • Response/Recovery
Comments	NGPS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging the converged PSN, the NGN, helps to ensure the preparedness of the Nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan, National Infrastructure Protection Plan.
Activity Scope	
Is this activity designed only to reduce risk in your own sector	No
Cross Sector Application	
Explanation	NGPS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging the converged PSN, the NGN, helps to ensure the preparedness of the Nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan, National Infrastructure Protection Plan.
Sector(s) or Subsector(s) Utilizing this Activity	• Banking and Finance • Emergency Services • Government Facilities • Healthcare and Public Health • Communications
Explanation	NS/EP priority telecommunications. NGPS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging the converged PSN, the NGN, helps to ensure the preparedness of the Nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan, National Infrastructure Protection Plan.
Attack Method Addressed	• Cyber - Directed Attack o Vulnerability - Recognizability

Reduce Threat, Vulnerability, and/or Consequence

- Vulnerability - Countermeasure Effectiveness
- Vulnerability - Robustness/Resistance
- Consequence - Loss of Life
- Consequence - Economic
- Consequence - Psychological

- Cyber - Non-Directed Attack
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Nuclear Detonation
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological

Geographic Scope	National
Comments	NGPS will provide NS/EP users with priority telecommunications nationwide on a 24 hour, seven days a week basis via the converged PSN (the NGN).

Activity Budget Details

FY 2007 President's budget request	$14,194,000
FY 2007 enacted budget	$14,080,000
FY 2008 President's budget request	$52,064,000
FY 2008 enacted budget	$21,100,000
FY 2009 President's budget request	$56,000,000

Activity Operational Details

Activity Status	Planning
Comments	NGPS will provide NS/EP users with priority telecommunications nationwide on a 24 hour, seven days a week basis via the converged PSN (the NGN).

Additional Information/Comments

Activity Information

Name of Program	Telecommunications Service Priority (TSP) Program
Managing Entity	Department of Homeland Security/National Communications System
Required by Law	Yes GOVERNING AUTHORITIES:
If so, which law	Executive Order (EO) 12472, “Assignment of National Security and Emergency Preparedness Telecommunications Functions,” 3 April 1984 (amended by EO 13286 of 28 February 2003) FCC Report and Order 88-341, 17 November 1988
Brief Description of Program	The Federal Communications Commission (FCC) issued a Report and Order (88-341) on November 17, 1988, that established the TSP System and officially adopted the TSP System rules as part of the Code of Federal Regulations. It assigns the responsibility of administration to the Executive Office of the President, who has delegated the responsibility to the National Communications System (NCS). NCS Directive 3-1, signed by the Executive Office of the President, implements the TSP System within the Federal Government and outlines the responsibility for management and operation. The TSP Program is the regulatory, administrative, and operational system authorizing and providing for priority treatment of National Security and Emergency Preparedness (NS/EP) telecommunications services. Under the program, service providers offer NS/EP users with priority restoration and provisioning of telecommunications services that are vital to maintaining readiness or responding to an incident. The TSP Program provides service vendors with an FCC mandate for prioritizing service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service. The TSP Program has two components: restoration and provisioning. A restoration priority is applied to telecommunications services to ensure restoration before any other services. A provisioning priority is obtained to facilitate priority installation of new telecommunications services in response to an emergency.
Activity Type	• Identification/Prioritization • Preparedness • Response/Recovery
Comments	The Telecommunications Service Priority (TSP) Program provides the

regulatory, administrative, and operational framework for priority restoration and provisioning of NS/EP communication circuits in an emergency. Eligibility in the TSP Program extends to Federal, State, and local Governments; private industry; or foreign Governments that have communications services supporting an NS/EP mission. The NCS is currently pursuing implementation of an NSTAC recommendation to enhance the TSP Program to accommodate requests from NS/EP users of wireless telecommunications services at critical sites.

Activity Scope

Is this activity designed only to reduce risk in your own sector

No

Cross Sector Application

Explanation

The TSP Program is available to all sectors and organizations (Federal, State/local, and private industry) that support and have an NS/EP mission and rely on communications in order to be prepared for and respond to emergencies and disaster situations. There are currently over 135,000 circuits enrolled in the TSP program representing over 840 organizations.

Sector(s) or Subsector(s) Utilizing this Activity

- Banking and Finance
- Chemical
- Commercial Facilities
- Nuclear
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Postal and Shipping
- Communications
- Transportation
- Water

Explanation

The TSP Program is available to all sectors and organizations (Federal, State/local, and private industry) that support and have an NS/EP mission and rely on communications in order to be prepared for and respond to emergencies and disaster situations. There are currently over 135,000 circuits enrolled in the TSP program representing over 840 organizations.

Attack Method Addressed

Reduce Threat,

Vulnerability, and/or Consequence	
Geographic Scope	National
Comments	The TSP Program is available to all sectors and organizations (Federal, State/local, and private industry) that support and have an NS/EP mission and rely on communications in order to be prepared for and respond to emergencies and disaster situations. There are currently over 135,000 circuits enrolled in the TSP program representing over 840 organizations.

Activity Budget Details

FY 2007 President's budget request	$296,000
FY 2007 enacted budget	$294,000
FY 2008 President's budget request	$667,000
FY 2008 enacted budget	$586,000
FY 2009 President's budget request	$690,000

Activity Operational Details

Activity Status	
Comments	

Additional Information/Comments

Activity Information

Name of Program	Wireless Priority Service (WPS)
Managing Entity	Department of Homeland Security/National Communications System
Required by Law	Yes
If so, which law	GOVERNING AUTHORITIES: Executive Order (EO) 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," 3 April 1984 (amended by EO 13286 of 28 February 2003) EO 13231, "Critical Infrastructure Protection in the Information Age," 16 October 2001 White House Memorandum, "National Level Telecommunications Program Implementation and Functional Requirements," 15 October 1991 NSDD 97, "National Security Telecommunications Policy," 13 June 1983 Presidential Decision Directive 67 (CLASSIFIED), "Enduring

	Constitutional Government and Continuity of Government Operations," 21 October 1998 EO 12656, "Assignment of Emergency Preparedness Responsibilities," 18 November 1988 (as amended) Federal Communications Commission Second Report and Order, FCC 00-242, "Establishment of Rules and Requirements for Priority Access Service," July 2000 National Security Council Memorandum, October 9, 2001, Subj: Minutes from October 5, 2001 Meeting on Select NS/EP Telecommunications Projects
Brief Description of Program	National Security and Emergency Preparedness (NS/EP) Priority Telecommunications Service (PTS) is a White House directed program to provide specially designed telecommunications services to the NS/EP user community during natural or man-made disasters when conventional communications services are ineffective. These telecommunication services are used to coordinate response and recovery efforts and, in severe conditions, to assist with Continuity of Operations (COOP) and Continuity of Government (COG). Specifically, NS/EP PTS enhances the ability of NS/EP users to complete calls during crisis or emergency through a degraded Public Switched Network (PSN) using WPS, one of four NS/EP PTS components. WPS is a nationwide wireless telephone service that complements and interoperates with GETS and provides priority NS/EP telecommunications via selected commercial wireless carriers.
Activity Type	• Preparedness • Response/Recovery
Comments	The Wireless Priority Service (WPS) provides priority Commercial Mobile Radio Service during and after emergencies for NS/EP personnel by ensuring WPS calls receive the next available radio channel during times of wireless congestion. WPS helps to ensure that key NS/EP personnel can complete critical calls by providing priority access during times of wireless network congestion to key leaders and supporting first responders.
Activity Scope	
Is this activity designed only to reduce risk in your own sector	No
Cross Sector Application	
Explanation	WPS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging selected PSN wireless carriers, helps to ensure

the preparedness of the Nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan, National Infrastructure Protection Plan.

Sector(s) or Subsector(s) Utilizing this Activity

- Banking and Finance
- Emergency Services
- Government Facilities
- Healthcare and Public Health
- Communications

Explanation

NS/EP priority telecommunications WPS provides assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. NS/EP PTS, by leveraging selected PSN wireless carriers, helps to ensure the preparedness of the Nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies in accordance with the National Response Plan, National Infrastructure Protection Plan.

Attack Method Addressed Reduce Threat, Vulnerability, and/or Consequence

- Cyber - Directed Attack
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Cyber - Non-Directed Attack
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological
- Nuclear Detonation
  - Threat - Intent
  - Threat - Capability
  - Vulnerability - Recognizability
  - Vulnerability - Countermeasure Effectiveness
  - Vulnerability - Robustness/Resistance
  - Consequence - Loss of Life
  - Consequence - Economic
  - Consequence - Psychological

Geographic Scope National

Comments WPS provides NS/EP users with wireless priority telecommunications nationwide on a 24 hour seven days a week basis.

Activity Budget Details

FY 2007 President's budget request	$75,128,000
FY 2007 enacted budget	$74,521,000
FY 2008 President's budget request	$49,127,000
FY 2008 enacted budget	$49,127,000
FY 2009 President's budget request	$30,000,000

Activity Operational Details

Activity Status	Execution
Comments	WPS has been deployed nationwide and provides priority treatment for NS/EP users to reduce the impact of a terrorist attack that disrupts or congests the cellular public switched network. Additionally, WPS priority treatment enhancements exploit the robustness of the public switched network to reduce the vulnerability of a specific technology failure. WPS also addresses other overarching protection needs (e.g., communications, coordination, strategic planning, etc. during NS/EP emergencies).

Additional Information/Comments