Communications Sector-Specific Plan

An Annex to the NIPP 2013

2015

Homeland Security

Table of Contents

LETTER FROM THE COUNCIL CHAIRS

The Department of Homeland Security designed this Communications Sector-Specific Plan (CSSP) to guide the sector's voluntary, collaborative efforts to improve security and resilience over the next four years. The CSSP describes how the Communications Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this CSSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Communications Sector. The sector strategy closely aligns with the NIPP 2013 national strategy, the 2014 Joint National Priorities, and Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*.

This 2015 release of the CSSP serves as an update to the original plan issued in 2010. As with the previous plan, this CSSP represents a collaborative effort among the private sector; State, local, tribal, and territorial governments; nongovernmental organizations; and Federal departments and agencies to identify and work toward shared goals and priorities to reduce critical infrastructure risk.

The Communications Sector Coordinating Council (CSCC) and Communications Sector Government Coordinating Council (CGCC) jointly developed the Communications Sector goals, objectives, and activities in this CSSP, which collectively reflect the overall strategic direction for the sector as a whole.

This CSSP also reflects the maturation of the Communications Sector partnership and the progress made to address the evolving risk, operating, and policy environments. Since 2010, Communications Sector partners in the public and private sectors have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the NIPP 2013 and EO 13636, Communications Sector partners look forward to continuing their efforts to enhance the security and resilience of our Nation's critical infrastructure assets.

Kathryn Condello
Chair
Communications Sector, Sector Coordinating Council

Andy Ozment
Assistant Secretary, Office of Cybersecurity and Communications
U.S. Department of Homeland Security

Caitlin Durkovich
Assistant Secretary, Office of Infrastructure Protection
U.S. Department of Homeland Security

EXECUTIVE SUMMARY

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry, using terrestrial, satellite, and wireless transmission systems. The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting sector infrastructure and assets. Working with the Federal Government, the private sector is able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other sectors, and affect response and recovery efforts.

As such, the Communications Sector Coordinating Council (CSCC) and Communications Sector Government Coordinating Council (CGCC) worked collaboratively to develop an update to the 2010 Communications Sector-Specific Plan (CSSP) in accordance with the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013). In this 2015 CSSP, the CSCC and CGCC developed joint goals that the sector will pursue to guide the mission over the next four years: (1) Protect and enhance the overall physical and logical health of communications; (2) Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects; and (3) Improve the sector's national security and emergency preparedness (NS/EP) posture with Federal, State, local, tribal, international, and private sector entities to reduce risk. To achieve these goals, the sector developed associated priorities to focus their efforts. The graphic below shows how the sector goals align to the joint sector priorities.

Table ES-1: Communications Sector Goals and Priorities

Sector Goals	Joint Sector Priorities
1 Protect and enhance the overall physical and logical health of communications.	**Cyber and Physical Security**: Coordinate with public and private sector partners regarding cyber and physical security information and trends, strategies, initiatives, programs, and best practices. **Future State**: Enhanced cyber and physical risk identification and management capabilities through the use of existing programs.
2 Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects.	**Resilience**: Promote and coordinate efforts to improve communications resilience by public and private sector partners before, during, and after incidents affecting communications. **Future State**: Enhanced sector programs and initiatives that increase sector-wide incident response and recovery capabilities.
3 Improve the sector's national security and emergency preparedness (NS/EP) posture with Federal, State, local, tribal, international, and private sector entities to reduce risk.	**Dependencies and Interdependencies**: Coordinate identification of sector dependencies and interdependencies with public and private sector partners and implement appropriate mitigation actions to make critical infrastructure more resilient and less vulnerable to manmade or natural threats. **Future State**: Improved ability to identify cross-sector dependencies and interdependencies and develop sector-wide risk mitigations strategies to address them.
	Partnership and Engagement: Coordinate with public and private sector partners regarding critical infrastructure security and resilience information, trends, strategies, initiatives, programs, and best practices. **Future State**: Advanced outreach and awareness programs that communicate sector-developed risk management and mitigation practices and strategies with sector stakeholders.

This updated CSSP will guide security and resilience efforts, inform partner decisions, and improve risk management practices over the next four years. As a part of this 2015 CSSP, the CSCC and CGCC have identified sector-specific risks and interdependencies. Consistent with the NIPP 2013 Critical Infrastructure Risk Management Framework, the Communications Sector's approach to network defense prioritizes assets, assesses threats and vulnerabilities, and then uses the findings of these assessments as criteria to focus resources on defenses that yield optimal protection. The Communications Sector regularly undertakes risk assessments to address evolving issues by topic, segment, or threat. Across the Communications Sector, industry and government partners collaborate to conduct risk assessments as an ongoing activity, with the intent to maintain a national communications infrastructure that is resilient, diverse, redundant, and recoverable.

The vision, goals, and joint sector priorities contained in the 2015 CSSP demonstrate how the sector is contributing towards the advancement of the NIPP 2013 Goals and the Joint National Priorities established by the NIPP Call to Action (CtA) #1, which advocated for the development of joint national priorities to inform resource allocation and decision-making on the part of critical infrastructure partners.

In order to implement this CSSP, the Communications Sector partners developed a set of broad objectives aligned to the four sector priorities that will contribute to sector goals and priorities. Details on the sector's objectives are in Chapter Five, Measuring Effectiveness, which includes both voluntary partnership activities and tasks the sector may pursue on its own volition.

The Communications Sector will leverage the NIPP 2013 CtA categories to track and report, on a quarterly basis, the progress of sector activities to DHS's Office of Infrastructure Protection. The NIPP 2013's CtA guides efforts to achieve national goals and, therefore, to enhance national critical infrastructure security and resilience. The NIPP 2013 CtA will serve as a roadmap to ensure continuous improvement of security and resilience through the Communications Sector's efforts.

This update also reflects the maturation of the Communications Sector partnerships and the progress made to address the evolving risk, operating, and policy environments.

1. INTRODUCTION

This Communications Sector-Specific Plan (CSSP) is an update to the sector's 2010 Sector-Specific Plan (SSP) in accordance with the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013).[1] The NIPP 2013 establishes a set of broad critical infrastructure security and resilience national goals, which the sector-specific priorities and planned activities outlined in this CSSP support. This update tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Communications Sector.

Since 2010, the Communications Sector has evolved rapidly in multiple areas, including mobile broadband, cloud computing, the Internet of Things (IoT), and software-defined networks (SDNs). Voice and data networks have continued to converge, and mobile devices, such as smartphones and tablet computers, have been widely adopted, creating enormous demand for mobile broadband communications. These changes increase the requirement for improved sector security and resilience, which the CSSP seeks to address by setting the strategic direction for voluntary, collaborative efforts to improve sector security and resilience over the next four years. It describes how the Communications Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities, implementation of Executive Order 13636: Improving Critical Infrastructure Cybersecurity, and the NIPP 2013 Call to Action (CtA) #2.[2]

This update also answers NIPP 2013 CtA #2, which calls upon each sector to update its SSP every four years to reflect joint priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress. The Vision, Goals, and Priorities Section of this document illustrates how the Communications Sector's priorities support both the NIPP 2013 national goals and Joint National Priorities. Public and private-sector representatives have identified shared goals and priorities, and a supporting set of collaborative activities they plan to pursue during the next four years.

This CSSP includes:

- **Sector Overview**—Provides a concise profile of the sector's evolution since 2010, characteristics, risk profile, and key public and private-sector partners and venues.
- **Vision, Goals, and Priorities**—Presents the sector's mission and updates goals and priorities for communications security and resilience over the next four years.
- **Achieving Sector Goals**—Describes mechanisms to achieve sector goals, including ongoing and planned partnership programs, activities, and resources that support the sector's current risk management

[1] Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, 2010 is available at the following URL: http://www.dhs.gov/publication/nipp-ssp-communications-2010. Accessed December 2, 2015.

[2] The NIPP 2013's CtA guides the private sector and Federal, State, local, tribal, territorial, and regional government efforts in implementing the NIPP, which has 12 actions assigned to three categories.

approach; research and development (R&D) priorities; and how the sector supports national preparedness through incident response and recovery.

- **Measuring Effectiveness**—Provides the list of initiatives that the CSCC and CGCC will undertake in partnership to address sector priorities, as well as the approach the sector will use to measure the effectiveness of individual activities.

The CSSP provides targets for Communications Sector public and private partner collaboration, specifically among government agencies, private industry, and DHS's Office of Cybersecurity and Communications (CS&C), which serves as the Sector-Specific Agency (SSA) for the Communications Sector. Partners have a clear and shared interest in ensuring the security and resilience of critical sector assets, and this plan represents the voluntary, collaborative activities that have the greatest effect on reducing sector risk and building resilience.

2. SECTOR OVERVIEW

The Communications Sector provides products and services that support the efficient operation of today's global information-based society.[3] In 2014, information and communication technology (ICT) companies accounted for 3.5 million jobs, contributing about $1 trillion to the U.S. gross domestic product (GDP) through both direct and indirect contributions, which is about 7 percent of the U.S. economy.[4] Many of these products and services are foundational or necessary for the operations and services provided by other critical infrastructure sectors. The sector recognizes that other sectors consider its services to be critical, and its practices reflect this understanding. The nature of communication networks involve both physical infrastructure (buildings, switches, towers, antennas, etc.) and cyber infrastructure (routing and switching software, operational support systems, user applications, etc.), representing a holistic challenge to address the entire physical-cyber infrastructure. The result has been the establishment of a robust, resilient network infrastructure that successfully provides services globally.

Virtually every element of modern life is now dependent on cyber infrastructure. As a result, our Nation's economic and national security relies on the security of the assets and operations of critical communications infrastructure. Past terrorist attacks and catastrophic natural disasters emphasized the need to focus our national attention on protecting the Nation's critical infrastructure and making it more resilient. Moving forward, it is essential that public and private sector partners adopt a coordinated approach to achieve joint goals for our communications infrastructure.

The public sector—Federal, State, and local governments—and the private sector share the responsibility for securing the Nation's critical communications infrastructure. Sector partners benefit from complementary skill sets, expertise, and individual resources to meet their shared responsibility for addressing all-hazard threats.

The individuals and organizations that contribute to the planning of initiatives to keep the Nation's communication networks resilient enough to withstand natural and manmade disasters, as well as those responsible for responding and restoring those networks post-event, have partnered to update this CSSP from its 2010 version. These include representatives from the five segments of the Communications Sector: broadcasting, cable, satellite, wireless, and wireline.

Key Sector Characteristics

Communication networks enable people around the world to contact one another, access information instantly, and communicate from remote areas. This involves creating a link between a sender (including voice signals) and one or more recipients using technology (e.g., a telephone system or the Internet) to transmit information from one location to another. Technologies are changing at a rapid pace, increasing the number of products, services,

[3] U.S. Department of Commerce Bureau of Economic Analysis is available at the following URL: http://bea.gov/iTable/iTable.cfm?ReqID=51&step=1#reqid=51&step=2&isuri=1. Accessed December 2, 2015.

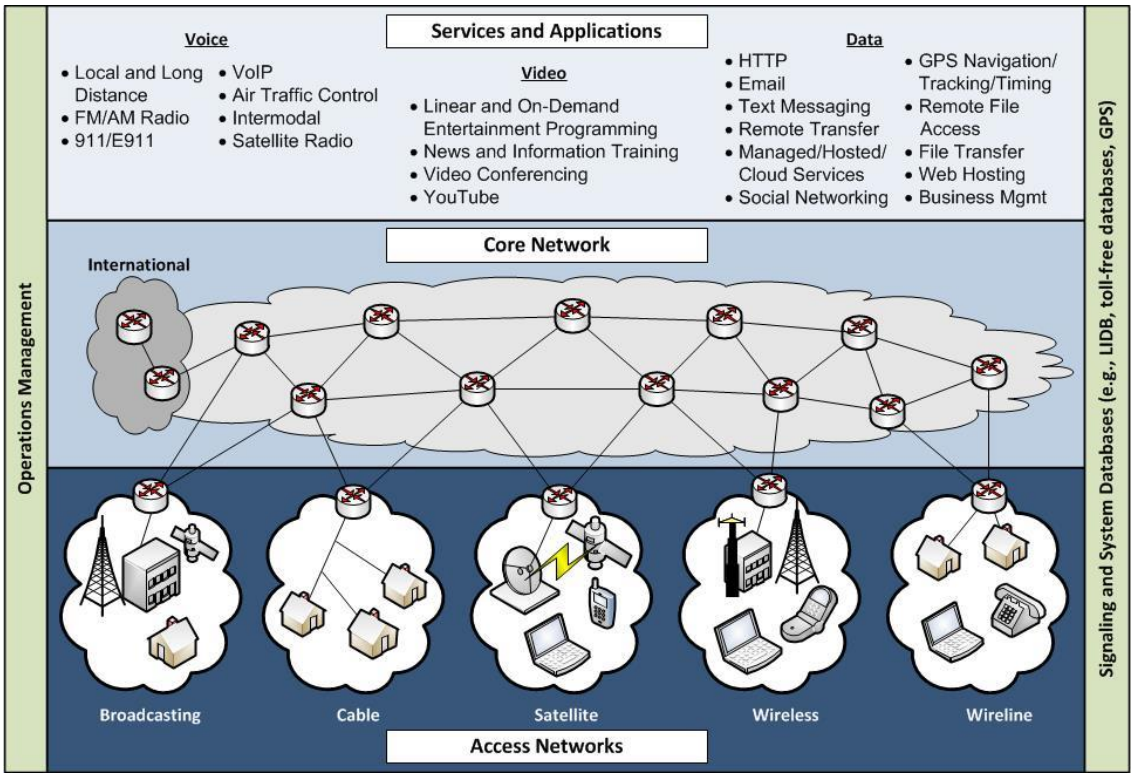
[4] Telecommunications Industry Association's *TIA2014 Playbook* is available at the following URL: http://www.tiaonline.org/PDF/9603_FinalProof_LoRes.pdf. Accessed December 2, 2015.

service providers, and communication options. The national communications architecture is a complex collection of networks that are owned and operated by individual service providers, consisting of three main functional areas: Services and Applications, Core Network, and the five segments' Access Networks.

Today, using more means than ever before, enormous volumes of information move at ever-faster speeds among an ever-increasing number of users and machines. Over the past 25 years, the public switched telephone network (PSTN) in the United States has evolved from a largely mechanical, circuit-switched network carrying voice telephone calls, which a few U.S. companies owned and operated, to a highly complex and integrated system of computer-controlled, packet-based networks carrying voice, data, and video, which thousands of domestic and international organizations own. Reliance on established circuit-based switching for communication is rapidly waning, and most of the traffic running over the public communication networks in 2014 was transmitted as data packets. The Internet is not the only part of the public network (PN) experiencing rapid growth. According to Cisco Systems, Inc., traffic from mobile data in 2013 was nearly 18 times the size of the entire Internet in 2000.[5]

[5] The Cisco® Visual Networking Index Global Mobile Data Traffic Forecast Update is available at the following URL: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html. Accessed December 2, 2015.

Figure 2-1: Communications Sector Architecture Model[6]



As more devices connect to public communication networks, service firms can provide more types of device-specific services over those networks. The Communications Sector architecture model in Figure 2-1 serves as a representation of the collective infrastructure, which illustrates at least five major ways to access the numerous voice, video, and data services on the core network: broadcasting, cable, satellite, wireless, and wireline networks.

Since 2010, the Communications Sector has continued to make rapid, technological advances in multiple areas, including network infrastructure, mobile broadband, cloud computing, IoT, Internet Protocol (IP) networks, Over-the-Top services (e.g., Voice over IP (VoIP)), and even SDNs. Network convergence has evolved alongside technology, with all forms of broadband infrastructure investments occurring across the United States as service providers have worked to meet individual and enterprise requirements for faster communication services. Smartphones, tablet computers, and their associated mobile applications emerged as rapidly adopted key user technologies in the Communications Sector, and their explosive growth has generated enormous demand for mobile broadband. Enterprises have since embraced cloud computing with Platform as a Service, Infrastructure as a Service, and Software as a Service enjoying widespread adoption.[7] Concurrently, the national policy environment has also evolved with the addition of Executive Order (EO) 13618, Assignment of National Security

[6] This architecture model depicts examples of network access methods and services provided. It is not intended to be comprehensive, exact or authoritative (Source: 2012 National Sector Risk Assessment for Communications (NSRA)).

[7] *National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Cloud Computing*, May 15, 2012

and Emergency Preparedness Communications Functions and EO 13636, *Improving Critical Infrastructure Cybersecurity*.

Key Sector Components

The Communications Sector represents a large number of facilities and sites that differ based on function, size, operating principles, and security risks. The sector includes five component areas that have similar functions and operations, thereby representing the access segments. The following section provides a brief overview of the five access segments for each component area.

Broadcast

Broadcasting systems consist of free and subscription based, over-the-air radio and television (TV) stations that offer analog and digital audio and video programming services and data services. Broadcasting has been the principal means of providing emergency alert services to the public for six decades. Broadcasting systems operate in three frequency bands: medium frequency (MF (AM radio)), very high frequency (VHF (FM radio and TV)), and ultra-high frequency (UHF (TV)). The full transition to digital TV and ongoing transition to digital radio provide broadcast stations with enhanced capabilities, including the ability to multicast multiple programs on a single channel. Radio and TV stations also stream broadcast and additional programming content over the Internet.

Cable

The cable industry is composed of more than 7,700 cable systems that offer analog and digital video programming services, digital telephone service, and high-speed broadband services. The cable systems use a mixture of fiber and coaxial cable to provide bidirectional signal paths to the customer. This hybrid fiber/coaxial (HFC) network architecture effectively segments the cable system into a number of parallel distribution networks. The HFC architecture is beneficial to business and residential customers because it improves signal performance and increases available bandwidth and overall network reliability. Although network designs vary, the HFC architecture in any particular community is typically based on a three-level topology, which includes a headend, one or more distribution hub(s), and multiple fiber nodes.

Satellite

This is a platform launched into orbit to relay voice, video, or data signals as part of a telecommunications network. Earth station antennas transmit signals to the satellite, which are amplified and sent back to Earth for reception by other earth station antennas. Satellites use a combination of terrestrial and space components to perform many types of functions, such as the bidirectional transmission of voice, video, and data services; data collection; event detection; timing; and navigation.

Wireless

Wireless refers to telecommunication in which electromagnetic waves (rather than some form of wire) carry the signal over part of or the entire communication path. Wireless technologies consist of cellular phones, wireless hot spots (WiFi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services to provide communication services.

Wireline

Consists of circuit- and packet-switched networks via copper, fiber, and coaxial transport media. It includes private enterprise data and telephony networks, the core backbone of the Internet, and the PSTN.

2.1 Sector Risks

In 2012, the Communications Sector undertook a comprehensive, all-hazards assessment of the current physical, cyber, and human risks faced by the domestic communication networks at the local, regional, and national levels.[8] All these risks remain of concern today. Physical risks involve the impact of natural, such as Category 4 or 5 hurricanes, major urban floods, major earthquakes, and solar super storms, or manmade events, such as terrorist attacks, intentional electromagnetic interference and explosives, and accidents, such as submarine cable damage, on communications infrastructure. Cyber risks involve threats from both malicious and non-malicious actors, including resource exhaustion, system alteration, or damage to the white space frequency database (e.g., unused spectrum). Human risks involve the impact of humans on network confidentiality, integrity, and availability across multiple categories: access of communications personnel to a disaster area, security of personnel and equipment during response and recovery, employee security awareness, and internal and external threats. Depending on the specific physical, cyber, or human threat, the risk posed may be minimal or elevated in its impact on local, regional, or national communications.

Communications Sector Risk Profile

Natural Disasters and Extreme Weather

Hurricanes, wildfires, and other extreme weather events have increased in frequency and severity in recent years, impacting local and regional communications infrastructure in the United States. On a national level, a geomagnetic solar super storm, such as the one in July 2012, could cause an electromagnetic pulse that collapses electric power grids and triggers a long-term outage (LTO) in national communications.[9]

[8] These risks were assessed in the 2012 NSRA.

[9] Information about the July 2012 solar super storm is available at the following URL: http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/. Accessed December 2, 2015.

Supply Chain Vulnerabilities

The Communications Sector depends on suppliers for the products and services that are necessary to deliver communication services to users. In particular, the sector is dependent on reliable hardware and software. This is an area the sector continues to scrutinize closely.

Global Political and Social Implications

The Communications Sector is global with significant numbers of partners, suppliers, customers, employees, and facilities located outside the United States. As a result, the sector monitors geopolitical unrest, economic conditions, and other factors as they may affect distribution patterns, foreign operations, employees, or partners.

Cyber Vulnerabilities

The Internet is a complex ecosystem comprising suppliers, networks, and service providers, all of whom are part of the Communications Sector. Any vulnerabilities or threats to functions and capabilities outside of the Communications Sector (e.g., hardware, software, and operating systems) have the potential to affect network provider services and, therefore, require ongoing attention.

Emerging Sector Risks

A number of long-range strategic threats, as noted in DHS's *2014 Quadrennial Homeland Security Review* (QHSR), are emerging and include pandemic diseases, climate change, and aging critical infrastructure.[10] More relevant emerging risks include risks to the Global Positioning System (GPS), risks associated with the IoT, and risks associated with the need for rapid mobilization and coordination of critical commercial sector assets in response to a large-scale incident of national security concern.[11,12,13]

Cross-Sector Dependencies and Interdependencies

The NIPP 2013 identifies lifeline functions—which include communications, energy, transportation, and water[14]—and resources essential to the operations of most critical infrastructure partners and communities. Identifying lifeline functions, specifically those that are interdependent with other sectors, can support preparedness planning and capability development. Communication dependencies include:

---

[10] *2014 Quadrennial Homeland Security Review*, June 18, 2014, pgs. 22-23

[11] U.S. Government Accountability Office Report, *GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced*, November 2013

[12] *NSTAC Report to the President on Information and Communications Technology Mobilization*, November 19, 2014

[13] *NSTAC Report to the President on the Internet of Things*, November 19, 2014

[14] NIPP 2013, *Partnering for Critical Infrastructure Security and Resilience*, page 17

Lifeline Functions: Energy, Transportation, and Water

Communication networks—including customer premise equipment (CPE), central office switching, transmission equipment, and routing and Domain Name System (DNS) infrastructure in Internet points of presence (PoPs) and datacenters—require electric power to operate. While backup generation provides power needed to operate in the short term or safely shutdown a facility, an LTO would significantly disrupt operations.

The Communications Sector generally relies on diesel fuel to power its backup generators and the Transportation Sector to deliver those fuels.

In some cases, water sources are also necessary for cooling and other processes. Service providers generally have alternate sources of water available for short-term service interruptions; an LTO could result in a significant shutdown.

Other Communications Sector Dependencies: Supply Chain, Information Technology (IT), GPS

The Communications Sector also has second-tier dependencies in the Information Technology Sector and Defense Industrial Base (DIB) Sector.

The Communications Sector relies on the IT Sector to deliver reliable products (e.g., routers, switches, software, operating systems, etc.) and services (such as domain name resolution) in order to provide end-to-end communication services for customers.

The primary use of GPS, as part of the DIB sector, in the commercial communications industry is in support of precision timing and network synchronization functions. The Communications Sector does leverage alternate precision timing capabilities for core functions, but the ubiquitous coverage of GPS permits greater flexibility for end users.

While the Communications Sector has few significant dependencies, other critical infrastructure sectors are dependent on the Communications Sector. As such, the Communications Sector is one of the few sectors that can affect all other sectors. At a minimum, each sector depends on services from the Communications Sector to support its operations and associated day-to-day communication needs for corporate and organizational networks and services (e.g., Internet connectivity, voice services, and video teleconferencing capabilities). Some sectors have even more significant dependencies on the Communications Sector beyond these routine operations. Table 2-1 provides a high-level overview of how other sectors are critically dependent on the Communications Sector.

Table 2-1: Sectors Dependent on the Communications Sector

Sector	Key Dependencies
Emergency Services	Relies on networks for emergency operations center connectivity, interconnecting land mobile radio networks, backhauling traffic, operating public alert and warning systems, and receiving emergency 911 calls.
Energy	May rely on communications infrastructure to aid in monitoring and controlling operations and electric transmission.

Sector	Key Dependencies
Financial Services	Relies on communications for transmitting transactions and financial market operations.
IT Sector	Depends on Communications Sector networks for delivering and distributing applications and services.
Transportation	May rely on communications infrastructure to aid in monitoring and controlling transportation infrastructure (e.g., signals, mass transit, air traffic control, and vehicle traffic monitoring).

The Communications Sector recognizes the importance of addressing the dependencies of other sectors on its services. In terms of the responsibility for risk, the Communications Sector typically considers other critical infrastructure sectors to be customers. As customers, these other sectors need to be aware of their responsibility to ensure the resiliency of their operations through redundancy and diversity of service. To this end, Communications Sector industry and government partners are committed to working with other critical infrastructure sectors to address cross-sector dependencies through customer relationships as well as through other SSAs and sector partnerships.

2.2 Critical Infrastructure Partners

Voluntary collaboration between private sector and government stakeholders remains the primary mechanism for advancing collective action toward Communications Sector security and resilience. Like all 16 critical infrastructure sectors, the Communications Sector operates under the NIPP Partnership Model, which encourages participation from across the sector. The success of the model depends on leveraging the full spectrum of capabilities, expertise, and experience across the critical infrastructure community and associated stakeholders. This requires efficient sharing of actionable and relevant information among partners to build situational awareness and enable effective risk-informed decision-making.

The NIPP Partnership Model employs public and private sector councils and uses the Critical Infrastructure Partnership Advisory Council (CIPAC) framework to facilitate collaboration between government and private sector partners. The succeeding paragraphs below describe the key partnerships that support the implementation of the Communications Sector critical infrastructure partnership model.

Partnership councils meet to exchange ideas and lessons learned; facilitate sector-level planning and resource allocation; establish effective coordinating structures; and develop security and resilience tools, guidelines, products, and programs. Functioning as the SSA, DHS's CS&C leads sector coordination, serves as the primary federal interface for sector-specific security and resilience efforts, promotes sector-wide information sharing, and supports implementation of the NIPP 2013 within the Communications Sector.

The CSCC is a self-organized, self-run, and self-governed private sector council consisting of owners and operators and their representatives from each of the five industry segments. The CSCC provides a forum for members of the private sector to discuss infrastructure security and resilience issues among themselves or to communicate directly with the CGCC and SSA. The CSCC enables communication system and infrastructure

owners and operators to coordinate on a wide range of sector-specific strategies, policies, activities, and issues related to the security and resilience of the sector. Communications owners and operators are vital contributors to CSCC implementation-level initiatives. A current list of the CSCC members is available on the CSCC Webpage.

The CGCC consists of representatives from across the Federal, State, and local governments. These public sector participants represent departments and agencies involved in various aspects of ICT policy, protection, and implementation. The CGCC helps to coordinate the implementation of the NIPP and corresponding CSSP across government and between government and the private sector. The CGCC works closely with the CSCC to plan, implement, and execute sector-wide resilience and security programs for the Nation's Communications Sector. A current list of CGCC members is available on the Communications Sector CIPAC Charters and Membership Webpage.

In addition to NIPP-related activities associated with the CSCC and CGCC, the Communications Sector participates in a number of public-private advisory and operational forums, ranging from chief executive officer (CEO)-level engagement on policy issues to incident response activities associated with operational activities. Figure 2-2 outlines the segmentation of these NIPP-related activities.

Figure 2-2: Communications Sector Partnership Model

Through the President's National Security Telecommunications Advisory Committee (NSTAC), industry helps to inform government decisions about NS/EP communications. NSTAC comprises up to 30 CEOs from major telecommunication companies, network service providers, IT firms, financial firms, and aerospace companies. Through a deliberative process, NSTAC provides the President with recommendations intended to ensure vital telecommunication connections are operational during any event or crisis and to help the Federal Government maintain a reliable, secure, and resilient national communications posture. Key areas of NSTAC focus include strengthening national security, enhancing cybersecurity, maintaining the global communications infrastructure, ensuring communications for disaster response, and addressing critical infrastructure interdependencies.

In January 2000, the White House designated the National Coordinating Center for Communications (NCC) as the Information Sharing and Analysis Center (ISAC) for telecommunications in accordance with Presidential

Decision Directive 63. The Communications Information Sharing and Analysis Center (Comm-ISAC), consisting of 66 member companies, has facilitated the exchange of information among industry and government participants regarding vulnerabilities, threats, intrusions, and anomalies affecting the telecommunications infrastructure. The Comm-ISAC supports and facilitates the information-sharing environment to ensure critical infrastructure security and resilience through regular meetings of critical infrastructure partners across government and with private industry. During emergencies, daily or more frequent meetings are held with industry and government personnel involved with the response effort. Under the new EO 13691, *Promoting Private Sector Cybersecurity Information Sharing*, the Communications Sector may (subject to applicable law) be able to expand cybersecurity threat information sharing within the private sector and between the private sector and government.[15]

Established in 1991, the Government and NSTAC Network Security Information Exchanges (NSIE) meet bimonthly to share information and views on threats and incidents affecting the PN's software elements, vulnerabilities, and possible remedies. In addition, NSIE members periodically assess the risk to the PN from electronic intrusion. The U.S. NSIE holds multilateral exchange meetings with its counterparts from the United Kingdom, Canada, Australia, and New Zealand.

The Communications Sector actively engages in the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Committee (CSRIC). Through this advisory committee, industry can recommend actions for the FCC to take to promote reliable, secure, and resilient communication services and networks. Industry also uses this venue to identify best practices that may be useful to support these same objectives. Individual communication enterprises can look to these and other industry best practices as guides to improving the security of their network and facilities.[16]

Communication networks are global in scope, and the Nation's communications infrastructure is linked with and dependent on infrastructure owned and operated by foreign states and organizations. As the SSA for the Communications Sector, CS&C engages bilaterally and internationally on both cybersecurity and communication issues. CS&C's Office of Emergency Communications (OEC) addresses emergency communications, interoperability, and critical infrastructure security and resilience issues. In striving to fulfill its mission, OEC has developed a strong, working relationship with Canada on NS/EP communications.

---

[15] EO 13691:*Promoting Private Sector Cybersecurity Information Sharing*, February 13, 2015, is available at the following URL: https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. Accessed December 2, 2015.

[16] Multiple industry best practices are available, including Carnegie Mellon University's Capability Maturity Model Integration CMMI®22 Measurement and Analysis Process; ISO/IEC 15939; ISO/IEC 27004; NIST SP800-55 Rev1, Draft Practical Measurement Framework for Software Assurance and Information Security; and the FCC Website, which is available at the following URL: https://www.fcc.gov/search/#q=best%20practices. Accessed December 2, 2015.

3. VISION, GOALS, AND PRIORITIES

The Communications Sector's vision acknowledges the Nation's critical reliance on assured communications. Accordingly, the Communications Sector will strive to ensure that the Nation's communication networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. An effective Communications Sector partnership between public and private components is essential for achieving this shared mission of security and resilience. To guide the mission, the CSCC and CGCC developed joint goals that the sector will pursue over the next four years: (1) Protect and enhance the overall physical and logical health of communications; (2) Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects; and (3) Improve the sector's NS/EP posture with Federal, State, local, tribal, international, and private sector entities to reduce risk.

The Communications Sector developed priorities associated with these goals and identified a future state for each priority towards which the sector will work over the next four years. These goals and priorities are shown in Table 3-1, while Table 3-2 shows their direct alignment to the Joint National Priorities and the NIPP 2013 Goals.

The **Cyber and Physical Security priority** involves the identification of communications assets, the implementation of protection measures for those assets, the detection of threats and attacks against the assets, appropriate and effective response to attacks, and the recovery of damaged communications functionality.

The **Resilience priority** involves the appropriate development, implementation, and ongoing enhancements of processes and technologies that improve the survivability performance of communications networks, applications, and services.

The **Dependencies and Interdependencies priority** involves the ongoing mapping of the Communications Sector ecosystem; identifying intertwined vulnerabilities; and developing, implementing, and enhancing the practical strategies to mitigate cascading consequences of attacks.

The **Partnership and Engagement priority** involves the challenging but rewarding work of ensuring that public and private components, driven by differing motivating primary principles, cooperate effectively to their mutual benefit and the overall benefit of the Communications Sector as a whole.

Table 3-1: Communications Sector Goals and Priorities

Sector Goals	Joint Sector Priorities
1 Protect and enhance the overall physical and logical health of communications.	**Cyber and Physical Security**: Coordinate with public and private sector partners regarding cyber and physical security information and trends, strategies, initiatives, programs, and best practices. **Future State**: Enhanced cyber and physical risk identification and management capabilities through the use of existing programs.
2 Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects.	**Resilience**: Promote and coordinate efforts to improve communications resilience by public and private sector partners before, during, and after incidents affecting communications. **Future State**: Enhanced sector programs and initiatives that increase sector-wide incident response and recovery capabilities.
3 Improve the sector's national security and emergency preparedness (NS/EP) posture with Federal, State, local, tribal, international, and private sector entities to reduce risk.	**Dependencies and Interdependencies**: Coordinate identification of sector dependencies and interdependencies with public and private sector partners and implement appropriate mitigation actions to make critical infrastructure more resilient and less vulnerable to manmade or natural threats. **Future State**: Improved ability to identify cross-sector dependencies and interdependencies and develop sector-wide risk mitigations strategies to address them.
	Partnership and Engagement: Coordinate with public and private sector partners regarding critical infrastructure security and resilience information, trends, strategies, initiatives, programs, and best practices. **Future State**: Advanced outreach and awareness programs that communicate sector-developed risk management and mitigation practices and strategies with sector stakeholders.

Table 3-2: Communications Joint Sector Priorities Aligned to Joint National Priorities and NIPP 2013 Goals

Communications Sector Priorities	Joint National Priorities					NIPP Goals
	Strengthen the Management of Cyber and Physical Risk to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision Making	Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	
Cyber and Physical Security: Enhance cyber and physical risk identification and management capabilities through the use of existing programs.	✓					Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments. Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities.
Resilience: Enhance sector programs and initiatives that increase sector-wide incident response and recovery capabilities.		✓			✓	Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services. Promote learning and adaptation during and after exercises and incidents.
Dependencies and Interdependencies: Improve the ability to identify cross-sector dependencies and interdependencies and develop sector-wide risk mitigation strategies to address them.			✓			Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
Partnership and Engagement: Advance the outreach and awareness programs that communicate sector-developed risk management and mitigation practices and strategies with sector stakeholders.				✓		

4. ACHIEVING SECTOR GOALS

Risk management is the cornerstone of the NIPP 2013 and of the national effort to strengthen security and resilience. It focuses on enabling owners and operators to make risk-informed decisions that best allocate limited resources to the most effective mitigation solutions. The NIPP outlines a Risk Management Framework that enables the critical infrastructure community to focus on those threats and hazards likely to cause harm, as well as employs prioritized approaches designed to prevent or mitigate the effects of those incidents. The NIPP also increases security and strengthens resilience by identifying and prioritizing actions to ensure (1) continuity of essential functions and services during incidents and (2) support rapid response and restoration.

The CSSP provides a strategic framework for the sector's partners to collaboratively protect the Nation's communications infrastructure. The basic goals of the CSSP risk management framework are:

- **Resilient Infrastructure:** Critical infrastructure and their communication capabilities should be able to withstand natural or manmade hazards—with the exception of extreme events, such as an LTO—with minimal interruption or failure.[17]
- **Diversity:** Facilities should have physically and logically diverse primary and backup communications capabilities that do not share common points of failure.
- **Redundancy:** Facilities should use multiple communication capability types to sustain business operations and eliminate single points of failure that could disrupt primary services.
- **Recoverability:** Plans and processes should be in place to restore operations quickly if an interruption or failure occurs.

The Communications Sector's goals and priorities are directly rooted in the NIPP 2013 Critical Infrastructure Risk Management Framework. Updated goals and priorities reflect the maturation of the partnership and the significant progress made since the 2010 CSSP. This section presents the sector's ongoing efforts and the planned approaches that support risk management and national preparedness, response, and recovery following an incident that affects Communications Sector operations.

4.1 Risk Management

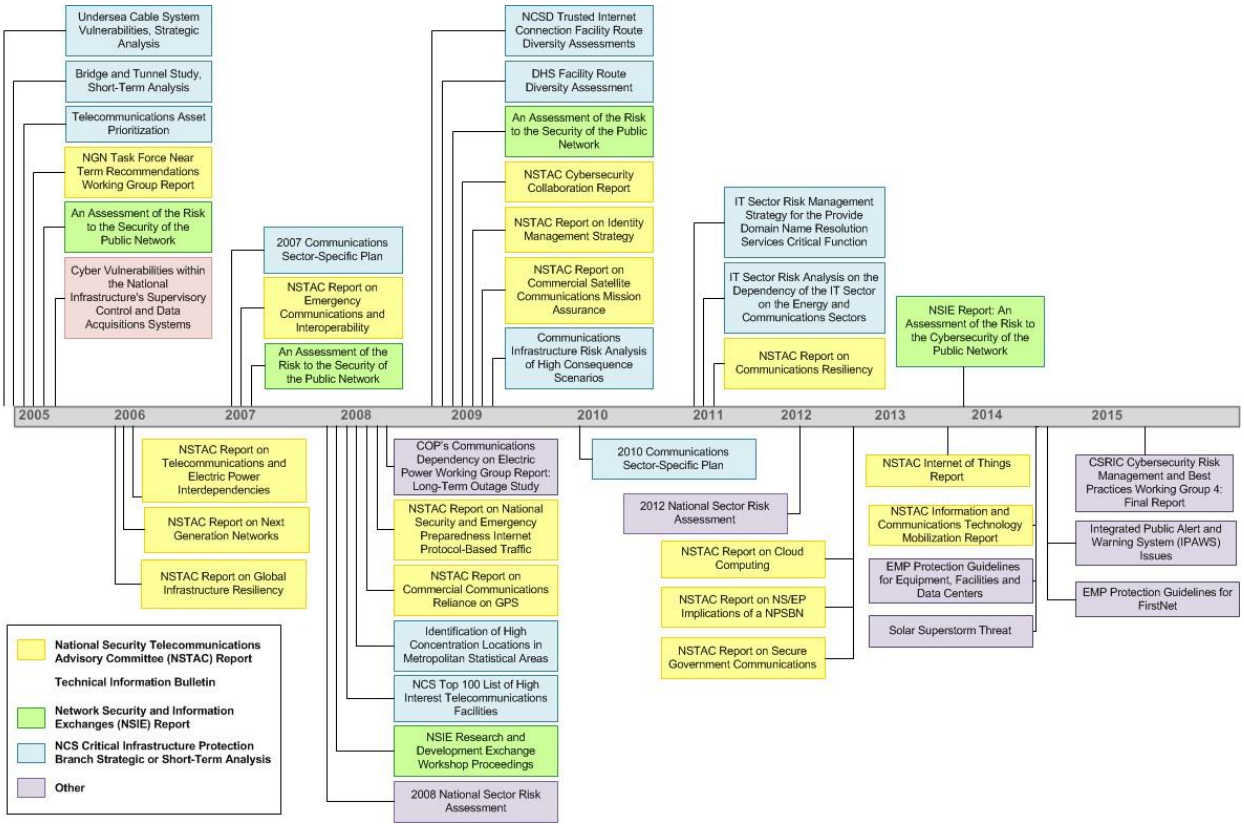
In the United States, Government officials and critical infrastructure owners and operators depend on the Communications Sector to support and receive NS/EP communications, thereby ensuring that the Nation can maintain mission essential functions during steady-state and crisis circumstances. The confidentiality, integrity, and availability of the public communication networks are a matter of national security and not merely a matter of

[17] For the 2012 NSRA, the Sector defined an LTO as an interruption of electrical power within a large enough geographical area and for a period of time beyond the capability of backup power systems currently in use to provide for the continuing operation of communications systems and networks (Source: National Communications System Committee of Principals, *Communications Dependency on Electric Power Working Group Report: Long-Term Outage Study*, 2009).

convenience. Nation states, criminal groups, and lone hackers are well aware of the significance of ICT infrastructure vulnerabilities at multiple levels (e.g., network, service, application, and user).

In the face of this dynamic environment, risk avoidance is simply not possible—no organization can prevent all threats or attacks or eliminate all of its vulnerabilities. Therefore, consistent with the NIPP 2013 Critical Infrastructure Risk Management Framework, the Communications Sector's approach to network defense prioritizes assets, assesses threats and vulnerabilities, and then uses such criteria to focus resources on those defenses that can yield optimal protection. The Communications Sector regularly undertakes risk assessments to address evolving issues by topic, segment, or threat. Across the Communications Sector, industry and government partners (including CSCC, CGCC, NSTAC, NCC, and NSIE) collaborate to execute risk assessments as an ongoing activity with the intent to maintain a national communications infrastructure that is resilient, diverse, redundant, and recoverable. Figure 4-1 highlights some of the risk assessment activities undertaken by the Communications Sector over the past decade.

Figure 4-1: Communications Sector's Risk Assessment History

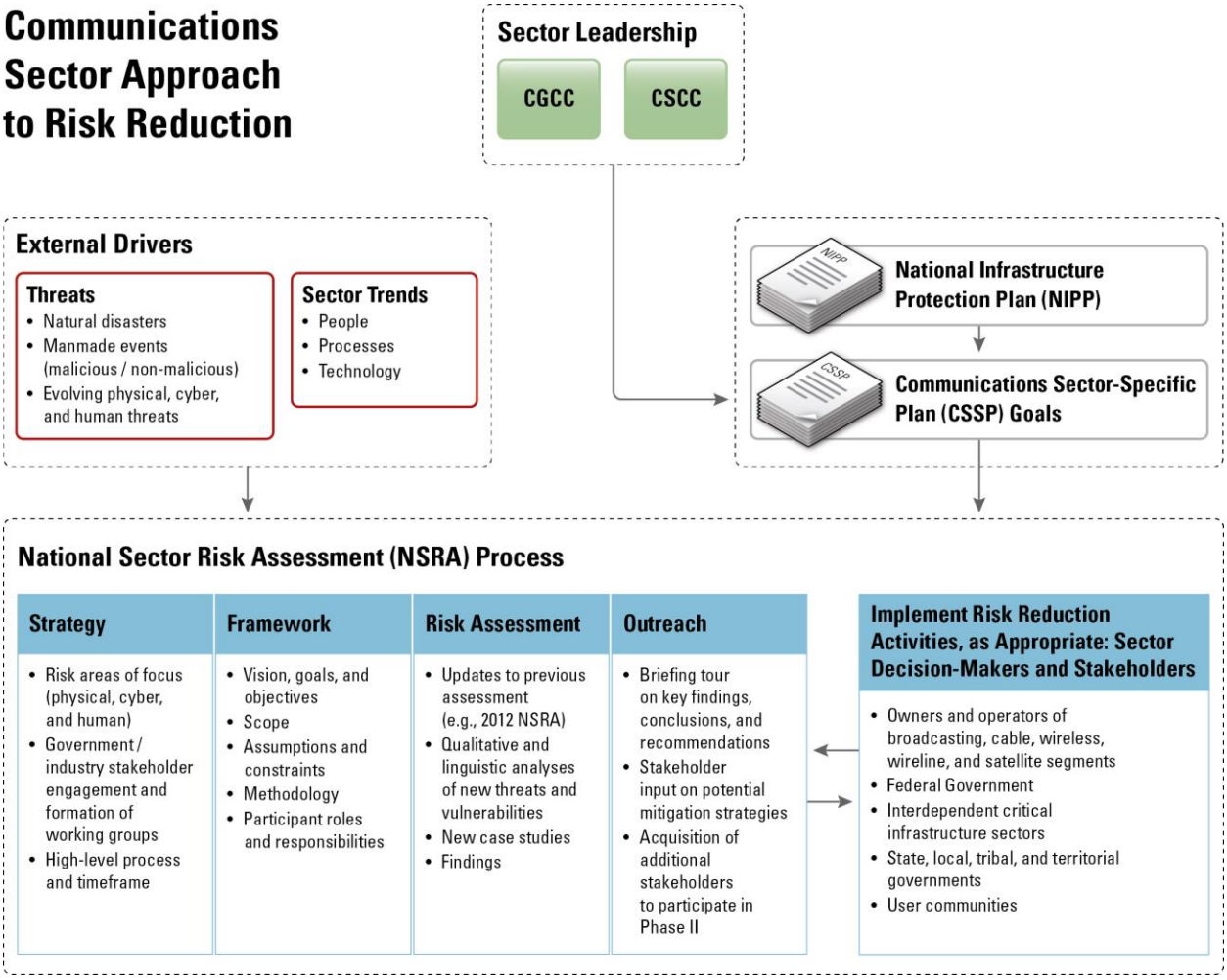


Under the NIPP 2013 Critical Infrastructure Risk Management Framework, risk is defined as the potential for an adverse outcome from an event, determined by the event's likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs. While individual owners and operators are responsible for managing risk to their individual assets, the Communications Sector has undertaken the risk assessments highlighted above to improve understanding of threats, vulnerabilities, and consequences, as well as

to provide owners and operators with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the facility and sector level.

The Communications Sector separately and collectively, regularly and routinely undertakes risk assessments to address evolving issues by topic, by segment, or by threat. Figure 4-2 outlines the Communications Sector's approach to risk reduction.

Figure 4-2: Communications Sector Approach to Risk Reduction

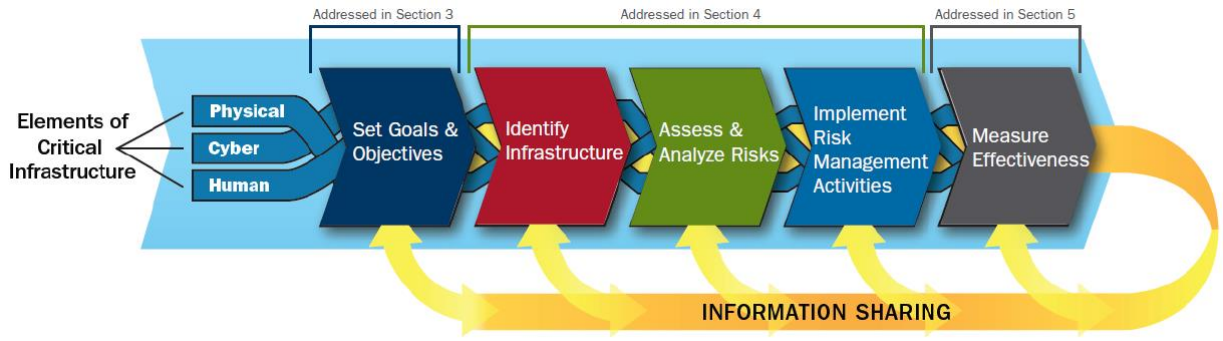


At the implementation level, the sector's critical infrastructure risk management approach aligns to the NIPP 2013 Critical Infrastructure Risk Management Framework (Figure 4-3).

- **Identify Infrastructure:** Identify assets, systems, and networks that contribute to critical functionality and collect information pertinent to risk management, including analysis of dependencies and interdependencies.
- **Assess and Analyze Risks:** Evaluate the risk, taking into consideration the potential direct and indirect consequences of an incident, known vulnerabilities to various potential threats or hazards, and general or specific threat information.

- **Implement Risk Management Activities:** Make decisions and implement risk management approaches to control, accept, transfer, or avoid risks. Approaches can include prevention, protection, mitigation, response, and recovery activities.

Figure 4-3: NIPP 2013 Critical Infrastructure Risk Management Framework



Identify Infrastructure

After the Communications Sector has jointly determined its shared vision and mission and then established its priorities and goals to achieve them, the Communications Sector works with owner and operators of other critical services to identify which assets or operations are the most crucial for national security and resilience. The Communications Sector ensures that response and restoration activities for these assets are included in State, local, and regional response plans. Communications owners and operators also work with their critical customers to develop emergency operations plans. As the SSA for the Communications Sector, DHS's CS&C helps to identify and obtain appropriate data for assets, systems, and networks that play a vital role in the Nation's security or economy.

Assess and Analyze Risks

Each individual owner and operator performs risk assessments for critical assets using diverse methodologies, ranging from failure modes and impact analyses, to hazard and operability studies. DHS works with all sector partners to identify existing risk tools and methodologies that may contribute toward developing a sector-wide risk assessment. Many communications companies are global corporations with extensive experience in handling natural and manmade threats and have very sophisticated methodologies for analyzing risks and prioritizing investments. In addition to individual security practices and risk mitigation measures implemented at individual facilities, owners and operators work with their peer companies and government partners to develop risk assessment programs.

Implement Risk Management Activities

Mitigation Options

Risk assessment results inform the selection and implementation of mitigation activities and the establishment of risk management priorities for Communications Sector owners and operators. Owners and operators prioritize and

implement risk mitigation activities based on their cost-effectiveness, feasibility, and potential for risk reduction. Risk management actions include measures designed to deter, disrupt, and prepare for threats and hazards; reduce vulnerability to an attack or other disaster; mitigate consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident.

The Communications Sector implements risk reduction activities, as appropriate, with multiple mitigation options relevant to specific identified risks. Physical risks require different mitigations than cybersecurity risks; for example, installation methods to protect GPS antennas or communication facilities in earthquake-prone areas will differ from methods to mitigate cybersecurity vulnerabilities pertaining to data integrity and confidentiality. The sector actively engages in the FCC's CSRIC to identify best practices that are applicable to the five industry segments: broadcasting, cable, satellite, wireless, and wireline.

Managing Cyber Risks

Cybersecurity risks and trends, when assessed collectively, can reach levels that fall beyond the ability of individual industry and government organizations to manage, such as when multiple organizations in an industry use the same software platform and become vulnerable to the same exploits. While organizations typically manage these types of issues on an individual basis or with a few key partners, examining risks from a sector level provides major long-term benefits. The Communications Sector takes a collaborative approach to cyber risk by working with DHS to evaluate the cybersecurity threats, vulnerabilities, and consequences to these critical functions and establish the sector's cyber-risk priorities. Through CSRIC Working Group #4, the sector has successfully mapped the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) to the five segments as a means to further enhance the cybersecurity of its networks and facilities.[18]

Once risks are validated, the Communications Sector has a function-by-function view of cyber risk that informs sector-specific risk management strategies and decision-making. This unified strategy provides the key linkage between national- and organization-level cyber risk management efforts, thereby enabling the Communications Sector to take a risk-informed approach to sector cybersecurity planning and stakeholder outreach over the coming years and make the most of limited government and industry resources.

Other Risk Specific Activities

Information sharing can also help to reduce risk and inform mitigation strategies. As the operational arm of the Communications Sector, and the communications operational arm of the National Communications and Cybersecurity Integration Center, the Comm-ISAC is first and foremost a response group. The Comm-ISAC also actively promotes and engages in information sharing regarding vulnerabilities, threats, intrusions, and anomalies from multiple sources with the intent of averting or mitigating effects on the communications infrastructure.

[18] The NIST CSF is available at the following URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. Accessed December 3, 2015.

Operating under the auspices of the CIPAC framework, the Communications Sector's Supply Chain Working Group (SCWG) was established to identify supply chain risk management (SCRM) best practices, mitigation opportunities, and long-term planning to institutionalize effective SCRM models across the sector.

As the nature of the threat environment changes, risk identification is cyclical. Communication entities must continually engage in prevention, protection, mitigation, response, and recovery to effectively manage and reduce risks. The Communications Sector continues to work with the Federal Government to identify opportunities for the CSCC, CGCC, and the State, Local, Tribal, and Territorial Government Coordinating Council to establish new and enhance existing programs that identify and mitigate communication response and recovery issues.

Mitigating Dependence on Lifeline Functions

Communications Sector owners and operators develop contingency plans, backup generation supplies, and alternate communication methods and transportation routes as part of their emergency operation and business continuity plans. In particular, owners and operators draw upon lessons learned from cross-sector partners during State and local emergency exercises to form more accurate expectations of lifeline function availability during a major disaster. Additionally, owners and operators also develop mitigations to address the effects of secondary dependencies, such as GPS loss and transportation. Examples of dependency mitigation actions are listed in Table 4-1.

Table 4-1: Communications Sector Critical Dependencies and Mitigations for Dependencies

Sector	Critical Dependencies	Mitigations for Dependencies
Energy	Provides each segment of the communications infrastructure with electric power (e.g., power and fuel to run cellular infrastructure, central offices, PoPs, and other communication facilities)	Use of backup electric power systems, including battery backup systems and generators, to keep its critical network components operational
Transportation	Supports delivery of fuel to support backup power systems	Established refueling contracts for emergency incidents
IT	Provides products, software systems, and applications that are used to operate the Communications Sector (e.g., DNS, operating systems, certificate authorities)	Industry risk management practices to manage and mitigate supply chain-related threats
Water	Provides potable water for heating and cooling of data centers and other communications facilities (e.g., high-tonnage heating, ventilation and air conditioning systems that require drinkable water to operate in order to keep their computer systems cool)	Use of backup and redundant water supplies onsite

Sector	Critical Dependencies	Mitigations for Dependencies
DIB (GPS)	Supports precise timing and synchronization for networks	Automatic backup capabilities and other mitigations to manage network performance in the event of GPS loss

4.2 Research & Development

The *Critical Infrastructure Security and Resilience National Research and Development Plan* (CISR National R&D Plan) required by Presidential Policy Directive 21 was released in February 2015. The CISR National R&D Plan presents five overarching Priority Areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community.

The CISR National R&D Plan Priority Areas are:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics;
- Develop integrated and scalable risk assessment and management approaches;
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action; and
- Build a crosscutting culture of critical infrastructure security and resilience R&D collaboration.

The Communications Sector will consider these five Priority Areas as inputs in its planning and coordination efforts to align its R&D activities and support implementation of the CISR National R&D Plan. The Communications Sector will continue to use the R&D process outlined in the 2010 CSSP for identifying, managing, and planning new and existing R&D initiatives.

Many of the new challenges facing the Communications Sector call for innovations in science and technology, making R&D initiatives essential to sector critical infrastructure security and resilience. The Communications Sector will continue to work collaboratively to identify criteria used to select new and existing R&D initiatives. The Communications Sector will use the R&D Planning Process outlined in the 2010 CSSP.[19]

4.3 Critical Infrastructure and National Preparedness

[19] The Communications R&D planning strategy is available within the Communications Sector-Specific Plan on pages 63-68, available at URL: http://www.dhs.gov/publication/nipp-ssp-communications-2010. Accessed December 3, 2015.

Despite the potential large-scale implications of a major disaster, critical infrastructure preparedness, response, and recovery takes place primarily at the community and regional level among cross-sector owners and operators of regionally critical assets. Sector partners have conducted several activities to improve incident response and recovery at the regional level to contribute to national preparedness.

EO 13618 highlights the Federal Government's need to communicate at all times and under all circumstances to carry out its most critical and time sensitive functions.[20] The Communications Sector plays an essential role by working closely with DHS's OEC to establish and maintain NS/EP communication services and programs, including the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP) Program. GETS and WPS provide priority completion of wireline and wireless calls when the PSTN is congested in an emergency, while the TSP program provides for priority restoration and provisioning of telecommunication circuits following a disruption of service.

Government and industry help to guide the formulation of policy considerations for communications that support the Executive Office of the President. EO 13618 also established the NS/EP Executive Committee to address NS/EP communication matters and to make recommendations to the President on NS/EP communications, thereby enhancing the survivability, resilience, and future architecture of NS/EP communications, including what should constitute NS/EP communication requirements. The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing NS/EP communications policy.

At the operational or response level, the Comm-ISAC facilitates voluntary collaboration and information sharing among government and industry in support of EO 13618 and the national critical infrastructure protection goals of Presidential Decision Directive 63, *Critical Infrastructure Protection*. This operational partnership has been in place since 1984 and is the only public/private ISAC.[21] Over 60 private sector ICT companies and 24 Federal Government departments and agencies are participants in the Comm-ISAC. Industry members include communications equipment and software vendors; wireline communication providers; and wireless communication providers, including satellite providers, broadcast, public safety, and Internet Service Provider backbone networks.

The Comm-ISAC or NCC continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes. In cases of emergency, the NCC Watch leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework. With much of the Nation's cyber infrastructure tied into communications, the NCC works with both the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber

[20] EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012, is available at the following URL: https://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-. Accessed December 3, 2015.

[21] As a direct result of an NSTAC recommendation, President Ronald Reagan established the NCC in 1984 to facilitate the coordination of NS/EP telecommunications restoration and provisioning (https://www.hsdl.org/?view&did=16010). Accessed December 3, 2015.

Emergency Response Team (ICS-CERT) to monitor and resolve issues impacting cyber and communications during an emergency.

The Communications Sector also works closely with CS&C to support the Critical Infrastructure Cyber Community (C^3) Voluntary Program, which is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The Program aims to help industry increase its cyber resilience and awareness, improve its use of the NIST Cybersecurity Framework, and encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management.

5. MEASURING EFFECTIVENESS

5.1 Sector Objectives

Communications Sector partners developed a set of broad objectives aligned to the four sector priorities to help implement this CSSP and meaningfully contribute to sector goals and priorities. The following objectives in Table 5-1 include both voluntary partnership activities and tasks the sector may pursue on its own volition. Since the SSPs are updated every four years, the Communications Sector partnership may modify the activities undertaken to support those objectives in order to reflect evolving risk, changes in resource allocations, and activity completion. Based on available resources alone, the sector identified the top objectives it believes will make a significant contribution to national security and resilience. The goal of the sector is to pursue these activities. Activities identified to support those objectives will go through an additional prioritization process between the CGCC and CSCC to identify and pursue those that will be achievable in the next several years. Table 5-1 shows how the sector's joint priorities are mapped to the planned objectives over the next four years.

Table 5-1: Communications Sector Priorities and Objectives

Cyber and Physical: Coordinate with public and private sector partners regarding cyber and physical security information and trends, strategies, initiatives, programs, and best practices.			
Objective 1.1: Promote the sharing of cybersecurity information, including information on new cyber threats, vulnerabilities, remediation efforts, and trends.	**Objective 1.2**: Promote the use of effective risk management strategies, solutions, and best practices to reduce cyber risks to the sector, consistent with the NIST CSF.	**Objective 1.3**: Promote the use of effective supply chain risk management strategies.	
Resilience: Promote and coordinate efforts to improve communications resilience by public and private sector partners before, during, and after incidents affecting communications.			
Objective 2.1: Promote the use of effective risk management strategies, solutions, and best practices to ensure continued availability of systems and networks and to reduce risks to the sector.	**Objective 2.2**: Build and enhance the capabilities of sector stakeholders to respond to and recover from incidents affecting communications, including the restoration of systems, networks, and related critical functions.	**Objective 2.3**: Develop, maintain, and exercise incident response strategies, plans, and procedures.	
Dependencies and Interdependencies: Coordinate identification of sector dependencies and interdependencies with public and private sector partners and implement appropriate mitigation actions to make critical infrastructure more resilient and less vulnerable to manmade or natural threats.			
Objective 3.1: Identify and share information regarding the dependencies and interdependencies within the Communication Sector and between other sectors to initiate development of the means to manage and mitigate those dependencies.	**Objective 3.2**: Predicated on findings, promote the development of effective risk management strategies and best practices to mitigate or manage sector dependencies and interdependencies.	**Objective 3.3**: Coordinate and facilitate the establishment of trusted, reliable, authoritative, and non-conflicting information sources for those public and private entities whose information sharing requirements and relationships are either dependent or interdependent.	
Partnership and Engagement: Coordinate with public and private sector partners regarding critical infrastructure security and resilience information, trends, strategies, initiatives, programs, and best practices.			
Objective 4.1: Encourage sector-wide use of the NIST CSF and foster a better understanding of how the NIST CSF can improve the overall posture of the sector through outreach and awareness programs and participation in DHS C³ Voluntary programs.	**Objective 4.2**: Periodically review and validate the results of National Sector Risk Assessments for Communications and/or other risk assessment initiatives.	**Objective 4.3**: Share critical infrastructure security and resilience information and trends, as well as critical infrastructure security and resilience training and educational opportunities.	**Objective 4.4**: Identify, prioritize, and engage in innovative research and development initiatives to promote critical infrastructure security and resilience.

5.2 Measurement Approach

For the purposes of the CSSP, DHS CS&C, as the SSA, is primarily responsible for measuring sector-wide progress through partnership activities towards national goals using relevant metrics. The SSA is also responsible for reporting sector progress through the National Annual Reporting process and the quadrennial SSP update.

In support of DHS reporting requirements, the CSCC independently develops an Annual Report outlining sector activities undertaken the previous year to ensure the Nation's communication networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. Given the diversity of fora and venues in which the Communications Sector collaborates with government (at all levels) or other sectors, this Annual Report intends to highlight the breadth of work and where that work is ongoing. This Annual Report is also consistent with the CSCC's role to provide visibility across the sector in areas of ongoing risk management activities.

Sector Annual Reporting Process

The Communications Sector recognizes the national interest in securing all 16 sectors' critical infrastructure identified by the Federal Government, including communications critical infrastructure. Communications Sector member companies are incentivized to take appropriate measures and protect their infrastructure from the growing issue of cyberattacks. However, the Communications Sector also understands the government's need for some public assurances that provide the Communications Sector's SSA with insight into the effects of cyber threats on critical communications network infrastructure.

To this end, the sector's goals and objectives would be consistent with the language in Table 5-1 above. Additionally, the CSCC is planning to develop and incorporate macro-level assurances in the form of aggregated, quantitative metrics associated initially with the availability of communications critical infrastructure as part of the industry-developed Sector Annual Report (SAR). The sector-developed SAR will then be provided to DHS, as the Communications Sector SSA, as well as the CGCC, which includes the FCC and other government agencies. Doing so ensures that (1) the various agencies that participate in the CGCC have visibility into efforts, initiatives, and progress within the Communications Sector and (2) any information provided to support this initiative is afforded the protections of CIPAC and Protected Critical Infrastructure Information (PCII).

In addition to the aggregated quantitative metrics, the sector anticipates that the SAR will also incorporate qualitative or anecdotal examples, such as actions Communications Sector members have taken over the past year to mitigate or recover from specific cyberattacks and/or incidents.

Process for Measuring Effectiveness

The Communications Sector will continue to leverage CSRIC recommendations and other best practices from national-level exercises and the Comm-ISAC to inform the sector's ability to measure effectiveness moving forward. The Communications Sector will leverage the NIPP 2013 CtA categories to track and report, on a quarterly basis, the progress of sector activities to DHS's Office of Infrastructure Protection. The NIPP 2013's CtA guides efforts to achieve national goals and, therefore, enhance national critical infrastructure security and resilience.[22] The NIPP 2013 CtA will serve as a roadmap to ensure continuous improvement of security and resilience through the Communications Sector's efforts. The actions listed below provide strategic direction for national efforts in the coming years.

Build upon Partnership Efforts (1-4):

1. Set National Focus through Jointly Developed Priorities
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience

Innovate in Managing Risk (5-10):

[22] NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience*

5. Enable Risk-Informed Decision-Making through Enhanced Situational Awareness
6. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
7. Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
8. Promote Infrastructure, Community, and Regional Recovery Following Incidents
9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
10. Improve Critical Infrastructure Security and Resilience by Advancing R&D Solutions

Focus on Outcomes (11-12):

11. Evaluate Progress toward the Achievement of Goals
12. Learn and Adapt During and After Exercises and Incidents

Table 5-2 shows how the sector's priorities and objectives align to the NIPP 2013 CtA, which is how the sector plans to report out on progress and measure effectiveness.

Table 5-2: Communications Sector Priorities and Objectives aligned to the NIPP 2013 Calls to Action

Cyber and Physical: Coordinate with public and private sector partners regarding cyber and physical security information and trends, strategies, initiatives, programs, and best practices.		
NIPP Call To Action (CtA): CtAs 5-10: Innovate in Managing Risk, CtAs 11-12: Focus on Outcomes		
Sector Initiatives:		
Objective 1.1: Promote the sharing of cybersecurity information, including information on new cyber threats, vulnerabilities, remediation efforts, and trends.	**Objective 1.2**: Promote the use of effective risk management strategies, solutions, and best practices to reduce cyber risks to the sector, consistent with the NIST CSF.	**Objective 1.3**: Promote the use of effective supply chain risk management strategies.
Resilience: Promote and coordinate efforts to improve communications resilience by public and private sector partners before, during, and after incidents affecting communications.		
NIPP Call To Action (CtA): CtAs 1-4: Build on Partnership Efforts, CtAs 5-10: Innovate in Managing Risk		
Sector Initiatives:		
Objective 2.1: Promote the use of effective risk management strategies, solutions, and best practices to ensure continued availability of systems and networks and to reduce risks to the sector.	**Objective 2.2**: Build and enhance the capabilities of sector stakeholders to respond to and recover from incidents affecting communications, including the restoration of systems, networks, and related critical functions.	**Objective 2.3**: Develop, maintain, and exercise incident response strategies, plans, and procedures.
Dependencies and Interdependencies: Coordinate identification of sector dependencies and interdependencies with public and private sector partners and implement appropriate mitigation actions to make critical infrastructure more resilient and less vulnerable to manmade or natural threats.		
NIPP Call To Action (CtA): CtAs 1-4: Build on Partnership Efforts, CtAs 5-10: Innovate in Managing Risk, CtAs: 11-12: Focus on Outcomes		
Sector Initiatives:		
Objective 3.1: Identify and share information regarding the dependencies and interdependencies within the Communication Sector and between other sectors to initiate development of the means to manage and mitigate those dependencies.	**Objective 3.2**: Predicated on findings, promote the development of effective risk management strategies and best practices to mitigate or manage sector dependencies and interdependencies.	**Objective 3.3**: Coordinate and facilitate the establishment of trusted, reliable, authoritative, and non-conflicting information sources for those public and private entities whose information sharing requirements and relationships are either dependent or interdependent.
Partnership and Engagement: Coordinate with public and private sector partners regarding critical infrastructure security and resilience information, trends, strategies, initiatives, programs, and best practices.		
NIPP Call To Action (CtA): CtAs 1-4: Build on Partnership Efforts, CtAs 5-10: Innovate in Managing Risk, CtAs: 11-12: Focus on Outcomes		
Sector Initiatives:		
Objective 4.1: Encourage sector-wide use of the NIST CSF and foster a better understanding of how the NIST CSF can improve the overall posture of the sector through outreach and awareness programs and participation in DHS C³ Voluntary programs.	**Objective 4.2**: Periodically review and validate the results of National Sector Risk Assessments for Communications and/or other risk assessment initiatives.	**Objective 4.3**: Share critical infrastructure security and resilience information and trends, as well as critical infrastructure security and resilience training and educational opportunities.

APPENDIX A: LIST OF ACRONYMS AND ABBREVIATIONS

APEC	Asia-Pacific Economic Cooperation
ATM	Asynchronous Transfer Mode
BCP	Business Continuity Planning
BSC	Base Station Controller
BSS	Broadcast Satellite Service
CATV	Cable Television
CCMG	Continuity Communications Managers Group
CCPC	Civil Communications Planning Committee
CDEP Report	Communications Dependency on Electric Power Report
CDEPWG	Communications Dependency on Electric Power Working Group
CEPTAG	Civil Emergency Planning Telecommunications Advisory Group
CERT	Computer Emergency Readiness Team
CGCC	Communications Government Coordinating Council
CII	Critical Infrastructure Information
CIPAC	Critical Infrastructure Partnership Advisory Council
Comm-ISAC	Communications Information Sharing and Analysis Center
CIKR	Critical Infrastructure and Key Resources
CLEC	Competitive Local Exchange Carrier
CMRS	Commercial Mobile Radio Services
COG	Continuity of Government
CONUS	Continental United States
COOP	Continuity of Operations
COP	Committee of Principals
CPE	Customer Premise Equipment
COR	Council of Representatives
CS&C	Office of Cybersecurity and Communications
CSCC	Communications Sector Coordinating Council
CSF	Cyber Security Framework
CSCSWG	Cross-Sector Cyber Security Working Group
CSIA	Cyber Security and Information Assurance
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group

CSRIC	Communications Security, Reliability, and Interoperability Council
CSSP	Communications Sector-Specific Plan
CtA	Call to Action
DARPA	Defense Advanced Research Projects Agency
DEC	Disaster Emergency Communications
DHS	U.S. Department of Homeland Security
DIRS	Disaster Information Reporting System
DNS	Domain Name System
DOC	U.S. Department of Commerce
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DPAS	Defense Priorities and Allocations System
DSL	Digital Subscriber Line
DTV	Digital Television
E-911	Enhanced 911
EAS	Emergency Alert System
EC	Executive Committee
ECG	Enduring Constitutional Government
ECPC	Emergency Communications Preparedness Center
E.O.	Executive Order
EOP	Executive Office of the President
EOT	Emergency Operations Team
ERC	Emergency Response Council
ERT	Emergency Response Training
ESF-2	Emergency Support Function 2
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FPIC	Federal Partnership for Interoperable Communications
FY	Fiscal Year
GCC	Government Coordinating Council
GDP	Gross Domestic Product
GEO	Geostationary Earth Orbiter
GETS	Government Emergency Telecommunications Service
GIP&M	Government-Industry Planning and Management
GPS	Global Positioning System

HF	High Frequency
HFC	Hybrid Fiber Coaxial
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSA	Homeland Security Advisor
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network–Critical Sectors
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
IAC	Internet Analysis Capability
ICT	Information and Communication Technology
ICTAP	Interoperable Communications Technical Assistance Program
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IMA	Individual Mobilization Augmentee
IMS	Internet-protocol Multimedia Subsystem
IoT	Internet of Things
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IR	Industry Requirements
IRI	Industrial Research Institute
ISAC	Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IT-ISAC	Information Technology Information Sharing and Analysis Center
ITU	International Telecommunication Union
IXC	Interexchange Carrier
JCG	Joint Contact Group
JFO	Joint Field Office
LATA	Local Access and Transport Areas
LEC	Local Exchange Carrier
LEO	Low Earth Orbit
LERG	Local Exchange Routing Guide
LTO	Long-Term Outage
MEF	Mission Essential Function
MEO	Middle Earth Orbit
MG	Media Gateway

MGC	Media Gateway Controller
MSC	Mobile Switching Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSO	Multiple-System Operators
MSRC	Media Security and Reliability Council
MSS	Mobile Satellite Service
MVPD	Multichannel Video Programming Distribution
NARUC	National Association of Regulatory Utility Commissioners
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center
NCCIC	National Cybersecurity and Communications Integration Center
NCIPP	National Critical Infrastructure Prioritization Program
NCIRP	National Cyber Incident Response Plan
NCRCG	National Cyber Response Coordination Group
NCS	National Communications System
NCS COP	National Communications System Committee of Principals
NCSD	National Cyber Security Division
NDAC	Network Design and Analysis Capability
NECP	National Emergency Communications Plan
NEF	National Essential Function
NENA	National Emergency Number Association
NGN	Next-Generation Network
NGPS	Next-Generation Priority Service
NICC	National Infrastructure Coordinating Center
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NLE	National Level Exercise
NOC	National Operations Center
NPTS	National Plan for Telecommunications Support in Non-Wartime Emergencies
NRF	National Response Framework
NRSC	Network Reliability Steering Committee
NS/EP	National Security and Emergency Preparedness
NSF	National Science Foundation
NSIE	Network Security Information Exchange

NSRA	National Sector Risk Assessment
NSSE	National Special Security Event
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
OAS	Organization of American States
OEC	Office of Emergency Communications
OIC	Office for Interoperability and Compatibility
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PBX	Private Branch Exchange
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PMEF	Primary Mission Essential Function
PITAC	President's Information Technology Advisory Committee
P.L.	Public Law
PN	Public Network
POC	Point of Contact
POD	Partnership and Outreach Division
POP	Point of Presence
PSA	Protective Security Advisor
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTS	Priority Telecommunications Service
PUC	Public Utility Commission
QHSR	Quadrennial Homeland Security Review
R&D	Research and Development
RCC	Regional Communication Coordinator
RDM	Route Diversity Methodology
RDT&E	Research, Development, Testing, and Evaluation
RDTF	Research and Development Task Force
RDX	R&D Exchange
RMA	Risk Mitigation Activity
RRAP	Regional Resilience Assessment Program
SAR	Sector Annual Report

SCC	Sector Coordinating Council
SCIP	Statewide Communication Interoperability Plan
SCRM	Supply Chain Risk Management
SCWG	Supply Chain Working Group
SDN	Software-Defined Network
SG	Signaling Gateway
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SME	Subject Matter Expert
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SPP	Security and Prosperity Partnership of North America
SRAS	Special Routing Arrangement Service
SS7	Signaling System 7
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
S&T	Science and Technology Directorate
STL	Studio-to-Transmitter Link
SWIC	Statewide Interoperability Coordinator
TSP	Telecommunications Service Priority
TT&C	Telemetry, Tracking, and Command
TTX	Tabletop Exercise
UHF	Ultra-High Frequency
U.K.	United Kingdom
UN	United Nations
U.S.	United States
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture
VHF	Very-High Frequency
VoIP	Voice Over Internet Protocol
VSAT	Very Small Aperture Terminal
WPS	Wireless Priority Service