



National Infrastructure Protection Plan

Communications Sector

The Communications Sector is one of 18 critical infrastructure sectors established under the authority of Homeland Security Presidential Directive 7 (HSPD-7). Each sector is managed by a Sector-Specific Agency (SSA) that provides sector-level performance feedback to the Department of Homeland Security (DHS) to enable assessment of national, cross-sector critical infrastructure protection and resilience programs. In accordance with the National Infrastructure Protection Plan (NIPP), each SSA is responsible for developing and implementing a Sector-Specific Plan (SSP), in collaboration with public and private sector partners, and for encouraging the development of appropriate information-sharing and analysis mechanisms.

Sector Overview

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Over 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 transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology to ensure interoperability.

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.

The Communications Sector is closely linked to a number of other sectors, including Energy, Information Technology, Banking and Finance, Emergency Services, and Postal and Shipping.

Sector Partnerships

As the SSA for the Communications Sector, the National Communications System (NCS) is responsible for implementing the NIPP sector partnership model and risk management framework, developing protective programs and related requirements, and providing sector-level critical infrastructure protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. The private sector works with the Federal Government on national security and emergency preparedness (NS/EP) communications issues through the National Coordinating Center (NCC) and the President's National Security Telecommunications Advisory Committee. In 2005, the communications industry formed a Sector Coordinating Council (SCC) to work with DHS and other Federal agencies to ensure coordination of infrastructure protection activities

for the sector. The SCC's members represent the majority of wireline and wireless communications industry owners and operators through major trade associations.

In addition to the NCS, the following Federal departments and agencies are involved in NIPP activities of the Communications Sector: DHS's National Cyber Security Division, the Federal Communications Commission, the General Services Administration, the National Telecommunications and Information Administration, and the Departments of Commerce, Defense, and Justice. These Federal agencies comprise the Communications Sector Government Coordinating Council, a counterpart to the SCC.

National Sector Risk Assessment

Public-private partnership is evident with the 2011 National Sector Risk Assessment (NSRA) for Communications, a joint public and private initiative aimed at reducing risk to and increasing the resilience of the Communications Sector. The goals of the 2011 NSRA for Communications include examining the evolving risks to the sector consistent with the goals presented in the 2010 Communications Sector-Specific Plan (CSSP).

Sector Annual Report

Also, through this unique partnership, the Communications Sector Critical Infrastructure Protection Annual Report provides updates on the sector's efforts to identify, prioritize, and coordinate the protection of the communications critical infrastructure. The Sector Annual Report provides the current priorities of the sector as well as the progress made during the past year in following the plans and strategies set out in the 2010 CSSP.

Critical Infrastructure Protection Issues

While it is unlikely that the loss of a single communications facility or key node would significantly impact the Nation's communications system, the loss could have cascading impacts on other critical infrastructure. Thus, the sector has focused on reducing risk by striving to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. The sector also assesses other sectors' communications dependencies for high-risk assets, networks, systems, and functions.

Information-Sharing Environment (ISE)

Information sharing is central to the success of a unified, national approach to protecting and ensuring the resilience of the Communications Sector's critical infrastructure. The newly redesigned Homeland Security Information Network-Telecommunications Sector portal provides the sector with a secure environment for public-private coordination, collaboration, and information sharing. Through the re-

establishment of the redesigned ISE, the sector continues to reduce risk by facilitating the establishment of a trusted partnership among all levels of government, industry owner/operators, State, local, tribal, territorial, and foreign partners within the Communications Sector.

Priority Programs

Within the Communications Sector, protective programs exist primarily on two distinct levels: (1) government sector-wide protective programs led by the NCS as the SSA, and (2) voluntary private sector initiatives. The following are a few examples of existing sector-wide programs.

- **NS/EP Priority Communications.** These programs ensure priority access, provisioning, and restoration of telecommunications services for NS/EP users. Programs exist for public switched and cellular networks, and emergency operations. Priority communications over Internet Protocol are under development.
- **National Coordinating Center (NCC).** The NCC's primary mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications services under all conditions, crises, or emergencies. During regular operations, industry and government representatives work together to produce and execute emergency response plans and procedures and, as part of its Information Sharing and Analysis Center function, members regularly share information about threats and vulnerabilities.
- **Network Security Information Exchange.** This program focuses on technical issues that affect the overall security of the Public Telephone Switched Network (PTSN), such as unauthorized penetration or manipulation of PTSN computers and software, databases, and other infrastructure that supports NS/EP telecommunications services.
- **Shared Resources (SHARES) High-Frequency (HF) Radio Program.** This program provides a single, interagency emergency message handling system for the transmission of NS/EP information. The SHARES program brings together the existing HF radio resources of Federal, State, and industry organizations when normal communications are destroyed or unavailable.

Private sector partners in the Communications Sector collaborate on the development of voluntary best practices through organizations such as the Network Reliability and Interoperability Council, the Media Security and Reliability Council, and other trade associations.

For questions or more information, please email Comms_Sector@HQ.DHS.GOV or visit www.dhs.gov/nipp.



Homeland
Security