National Infrastructure Protection Plan

Communications Sector

Homeland Security Presidential Directive 7 (HSPD-7) identified 17 critical infrastructure and key resources (CIKR) sectors and designated Federal Government Sector-Specific Agencies (SSAs) for each of the sectors. Each sector is responsible for developing and implementing a Sector-Specific Plan and providing sector-level performance feedback to the Department of Homeland Security (DHS) to enable gap assessments of national cross-sector CIKR protection programs. SSAs are responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector.

Sector Overview

The Communications Sector is an integral component of the U.S. economy as it underlies 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.

A majority of the Communications Sector is privately owned, requiring DHS to work closely with the private sector and its industry associations to identify infrastructure, assess and prioritize risks, develop protective programs, and measure program effectiveness.

The Communications Sector is closely linked to other sectors:

- **The Energy Sector** provides power to run cellular towers, central offices, and other critical communications facilities;
- **The Information Technology Sector** provides critical control systems and services, physical architecture and Internet infrastructure;
- **The Banking and Finance Sector** relies on telecommunications for the transmission of transactions and operations of financial markets;
- **The Emergency Services Sector** depends on telecommunications for directing resources, coordinating response, alerting the public, and receiving emergency 911 calls; and
- **The Postal and Shipping Sector** uses telecommunications for its control systems, tracking shipments, and regular communications requirements.

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 CIKR 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 Government Coordinating Council, a counterpart to the SCC.

CIKR 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; and
- Assessing other sectors' communications dependencies for high-risk assets, networks, systems, and functions.

The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting sector infrastructure and assets. The industry has a long established track record for securing physical facilities and networks from threats and for restoring services in the aftermath of attacks. 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.

Priority Programs

Within the Communications Sector, protective programs primarily occur 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. The Government Emergency Telecommunications Service and Wireless Priority Service provide priority access in the Public Switched Telecommunications Network and cellular networks, respectively. The Telecommunications Service Priority Program provides the regulatory, administrative, and operational framework for priority restoration and provisioning of NS/EP communications circuits in the event of an emergency. The sector is currently working to scope out the necessary requirements and path forward to achieve priority communications over Internet Protocol (IP). This work is vital to ensuring that priority communications continue when the communications infrastructure switches from circuit-switched to IP traffic routing.
- **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.
- **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 best practices through organizations such as the Network Reliability and Interoperability Council, the Media Security and Reliability Council, and other trade associations. The use of best practices remains voluntary; not every recommendation is appropriate for every company and circumstance.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.