National Infrastructure Protection Plan

Postal and Shipping 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 Postal and Shipping Sector is an integral component of the U.S. economy, employing more than 1.8 million people and earning direct revenues of more than $213 billion per year. The Postal and Shipping Sector moves over 720 million messages, products, and financial transactions each day. Postal and shipping activity is differentiated from general cargo operations by its focus on letter and flat mail, publications, and small- and medium-size packages and by service from millions of senders to nearly 150 million destinations. The sector is highly concentrated, with a handful of providers holding roughly 94 percent of the market share.

Sector-specific assets include: over 400 high-volume automated processing facilities; over 40 thousand local delivery units; many and varied collection, acceptance, and retail operations; over 50 thousand transport vehicles including vans, trucks, tractor trailers and aircraft; and information and communications networks.

Every sector of the economy depends on the service providers in the Postal and Shipping Sector to deliver time-sensitive letters, packages and other shipments. These time-sensitive delivery needs are critical to the Banking and Finance, Government Facilities, Commercial Facilities, and Healthcare and Public Health Sectors, who all rely heavily on the Postal and Shipping Sector for the shipment and delivery of critical documents and packages.

Major interdependencies with other sectors include those with the Information Technology, Communications, Energy, and Transportation Systems Sectors. The Postal and Shipping Sector itself relies on: (1) the Transportation Systems Sector for the movement of mail and packages by air, road, or rail; (2) the Energy Sector for power; and (3) the Information Technology and Communications Sectors for supporting logistics operations and automatic identification and sorting. All of the aforementioned sectors are also key customers and are working together to ensure that their efforts support each other.

Sector Partnerships

The Postal and Shipping Sector has an informal Sector Coordinating Council (SCC) that is comprised of the major industry providers (UPS, United States Postal Service® (USPS), FedEx®, and DHL) who are responsible for approximately 94 percent of the market. The SCC works with DHS and other Federal agencies to ensure that the efforts of the private sector are informed by Federal activities and vice versa. This council also serves as a critical mechanism for ensuring that the concerns and perspectives of the private sector are considered in Federal actions.

Several Federal agencies have formed the Postal and Shipping Government Coordinating Council (GCC), including the Transportation Security Administration (TSA); DHS Office of Infrastructure Protection; DHS Customs and Border Protection; DHS Mail Management Program; DHS Office of Grants and Training; Department of Health and Human Services Centers for Disease Control and Prevention; and the Food and Drug Administration. The objective of the GCC is to promote effective government coordination of postal and shipping security strategies; identify gaps and activities; establish policies and standards, program metrics, and performance reporting criteria; and foster effective communications and partnerships across government and between government and the private sector.

CIKR Protection Issues

The Postal and Shipping Sector delivers to virtually every national and international location. Accordingly, postal and shipping personnel have trusted access to almost all public and private facilities in their roles as collectors and distributors of the Nation's postal commerce. To ensure ease of access to and use of the system for its customers, the sector maintains an extremely large number of collection points at which parcels and letters can be inserted for delivery. These collection facilities present a vast array of relatively anonymous entry points at which terrorists could insert dangerous materials for delivery to intended targets. This combination of ubiquitous, trusted personnel access to other sectors, an extraordinary number of anonymous insertion points, and the potential for delivery to diverse recipients potentially makes the Postal and Shipping Sector an attractive vector that terrorists may use to attack persons or critical infrastructure in other sectors.

Priority Programs

Within the Postal and Shipping Sector, protective programs primarily occur on two distinct levels: (1) overarching, sector-wide protective programs led by TSA as the SSA; and (2) protective programs that are driven by industry partners and, for the most part, performed voluntarily by asset owners and operators. High-priority sector-wide programs include:

- **Exercises.** The Postal and Shipping Sector has conducted several exercises in partnership with government and private sector stakeholders. In 2008, the sector hosted three Panflu exercises to test TSA's and the sector's preparedness to respond to such an emergency.

The sector is also planning a research and development (R&D) workshop for the SCC members to discuss DHS priorities and opportunities to conduct R&D for the sector.

- **Information Sharing.** The Postal and Shipping Sector has established a portal on the Homeland Security Information Network and a Sharepoint site where sector members can collaborate and share information. This facilitates and enables information sharing between the SSA and private sector security partners, among Federal government agencies (GCC membership), and across other critical infrastructure sectors.

In addition, the sector had the services of a dedicated Intelligence Analyst (IA) for five months. This IA provided daily updates and reports to sector members on incidents and news of interest to the sector.

- **Site Visits (SVs).** In conjunction with DHS, the SSA has performed several SVs at key Postal and Shipping Sector stakeholder facilities. The SVs were carried out at the invitation of and in full cooperation and coordination with the P&S security partners.
- **Strategic Homeland Infrastructure Risk Assessment (SHIRA).** The Postal and Shipping Sector is an active participant in the SHIRA process. A complete review was conducted in the Spring of 2008.

USPS protective programs include initiatives such as Biological Detection Systems in 272 processing and distribution centers, threat mail identification programs, a facility risk-rating model, facility security surveys, commercial mailer reviews, observation of mail conditions, Airport Mail Security Review Program, Aviation Mail Security Program, Personnel Screening Review Program, Financial Security Review Program, and a Security Force Assessment Survey.

The private sector security partners are implementing protective initiatives and programs, although the specifics of these efforts are generally considered proprietary and of a commercially sensitive nature. General examples of such programs include physical vulnerability mitigation measures, such as perimeter fencing, additional security measures for the handling and storage of hazardous materials, and closed-circuit surveillance systems; cyber security measures such as encryption and sophisticated package tracking systems; and personnel security measures, such as access control, metal detectors, and identification verification requirements.

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security

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