U.S. Department of Homeland Security
Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Mail and Package Handling Facilities

The Postal and Shipping Sector receives, processes, transports, and distributes billions of letters and parcels annually. It consists of both private and public components, with four major service providers operating 94% of the sector's assets, systems, networks, and functions. The remainder of the sector consists of smaller firms providing regional and local courier services, other mail services, mail management for corporations, and chartered air delivery services. Numerous infrastructure sectors rely on the services provided by mail and package handling facilities.

Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to mail and package handling facilities include:

- Chemical, biological, or radiological attack (e.g. anthrax-laced letter)
- Improvised explosive device (e.g. package/letter bomb)
- Small arms attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Suspicious package and/or letter received by a carrier that might contain explosives or CBR agents. The packages or mail may have
  (1) No return address,
  (2) Excessive postage,
  (3) Been sent from outside the United States,
  (4) Indications of liquids/powder leaking from them, or
  (5) Unusual odors.
- Unusual request concerning the shipment or labeling of goods
- Packaging that is inconsistent with the shipping mode
- Evidence of unauthorized access to heating, ventilation, and air-conditioning (HVAC) areas; indications of unusual substances near air intakes
- Persons or teams of people spotted in or around the site attempting to gain unauthorized access to restricted areas

Indicators of potential surveillance by terrorists include:

- Persons possessing or observed using observation equipment (e.g., cameras, binoculars, night-vision devices) near the facility over an extended period
- Persons discovered with maps, photos, or diagrams with facilities or key facility components highlighted
- Buildings or sensitive areas left unsecured
- Persons parking, standing, or loitering in the same area over multiple days with no reasonable explanation
- Employees whose working behavior has changed or who are working more irregular hours without explanation
- Persons questioning employees off-site about practices pertaining to the mail or package handling facility and its operations, especially security screening measures or practices
- Unfamiliar service or contract personnel with passable credentials attempting to access unauthorized areas

Common Vulnerabilities

The following are key common vulnerabilities of mail and package handling facilities:

- High volume and anonymity of mail, making timely tracing and interception of individual packages difficult
- Ease of introducing biological/chemical/explosive agents into distribution and handling systems
- Potentially significant distribution system impacts resulting from function loss at one or more handling facilities

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for mail and package handling facilities include:

- **Planning and Preparedness**
  - Designate an employee as security director to develop, implement, and coordinate all security-related activities.
  - Develop a comprehensive security and emergency response plan. Coordinate the plan with appropriate agencies. Conduct regular exercises of the plan.
  - Establish liaison and regular communication with local law enforcement and emergency responders.
  - Establish procedures to implement additional protective measures as the threat level increases.
- **Personnel**
  - Conduct background checks on all employees.
  - Incorporate security awareness and response procedures into employee training programs.
  - Require contractors, vendors, and employment agencies to vouch for the background and security of their personnel who will work at the facility.
- **Access Control**
  - Provide appropriate signs to restrict access to nonpublic areas.
  - Install intrusion detection systems in sensitive areas.
  - Identify a buffer zone extending out from the facility boundary (both land and water areas) that can be used to further restrict access to the facility when necessary. Coordinate with local law enforcement on buffer zone measures.
  - Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement.
- **Barriers**
  - Provide adequate locks, gates, doors, and other barriers for designated secure areas. Inspect barriers routinely for signs of intrusion.
  - Install barriers at heating, ventilation, and air-conditioning (HVAC) systems, hatches, and power substations. Routinely patrol these areas.
- **Communication and Notification**
  - Install, maintain, and regularly test security and emergency communication systems. Ensure functionality and interoperability with local law enforcement.
  - Encourage employees and the public to report any suspicious activity that might constitute a threat.
- **Monitoring, Surveillance, Inspection**
  - Install alarms and intrusion detection devices at the site perimeter. Coordinate with law enforcement.
  - Monitor the activities of on-site contractors and vendors. Inspect all work before releasing them.
- **Infrastructure Interdependencies**
  - Ensure that the facility has adequate utility service capacity to meet normal and emergency needs.
  - Where practical, provide for redundancy and emergency backup capability.
- **Cyber Security**
  - Implement adequate policies and procedures and instill the appropriate culture regarding cyber security.
  - Regularly consult with trade organizations, vendors, or specialists about cyber practices and strategies.
  - Validate the credentials and work of contractors and vendors given access to technology systems.
  - Immediately cancel access for terminated staff.
  - Control physical access to critical technologies.
- **Incident Response**
  - Develop and maintain an up-to-date emergency response plan, incident notification process, and emergency calling trees that cover all staff.
  - Prepare an emergency operations center to coordinate resources and communications during an incident.