MAIL AND PACKAGE HANDLING FACILITIES

POTENTIAL INDICATORS OF TERRORIST ACTIVITY, COMMON VULNERABILITIES, AND PROTECTIVE MEASURES

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

Version: October 5, 2007
Content: June 2007

WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO).** It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza, or locked area offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

For more information about this document, contact:
Protective Security Advisor Duty Desk (703-235-5724 or IPassessments@dhs.gov).

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

Infrastructure Protection Report Series
Mail and Package Handling Facilities

POTENTIAL INDICATORS OF TERRORIST ACTIVITY, COMMON VULNERABILITIES, AND PROTECTIVE MEASURES

Figure 1 Packages on Conveyer at Postal Facility

Mail and package handling facilities (Figure 1), which are part of the Postal and Shipping sector, have the following characteristics: (1) end-to-end integrated acceptance, processing, transportation, and delivery of letters and parcels (weighing less than 150 lb); (2) multi-modal transportation, including aviation, highway, and rail; (3) residential and business collections and delivery; (4) retail storefronts; (5) large, centralized, high-volume automated or semi-automated processing facilities; (6) daily volume of more than 800 million pieces; (7) employees in excess of 1.5 million; and (8) customer base in the hundreds of millions (Collins 2007).

This report presents the following information related to mail and package handling facilities:

- Potential Indicators of Terrorist/Threat Activity
- Common Vulnerabilities
- Standards and Regulations
- Protective Measures
- Reference Material and Other Useful Information

This report is one of a series of documents that address how our nation can better protect its critical infrastructures and key resources. See contact on cover page for additional information.

CHARACTERISTICS OF MAIL AND PACKAGE HANDLING FACILITIES

The following sections provide a summary description of mail and package handling facilities and their configurations and vulnerabilities that could be exploited by terrorists and other adversaries.

Characterization of the Industry

The Postal and Shipping sector receives, processes, transports, and distributes billions of letters and parcels annually. It consists of both private and public components, but primarily comprises the following four large integrated carriers, which operate 93% of the sector's assets, systems, networks, and functions: the United States Postal Service (USPS), United Parcel Service of America, Inc. (UPS), Federal Express (FedEx), and DHL International. 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. Although most of the sector is privately owned, there is a major government presence through the USPS. Each of the four primary carriers is described in the paragraphs that follow.

USPS

The USPS is an independent, self-supporting agency within the Executive Branch of the U.S. government. The USPS uses revenue from the sale of postage and postage-related products to pay expenses. Public subsidy to support the USPS was eliminated in 1982. According to information on the USPS Web site, total USPS annual operating revenue in 2005 was nearly $70 billion.

The USPS delivers 212 billion pieces of mail to more than 144 million homes, businesses, and post office boxes in virtually every state, territory, city, and town in the United States, including Puerto Rico, Guam, the American Virgin Islands, and American Samoa. The USPS transports the mail using a wide range of transportation modes: planes, trains, trucks, cars, boats, bicycles, and even mules. The USPS serves over 7.5 million customers daily at 40,000 post offices. In addition, in 2005, USPS accepted 4.7 million passport applications — 65% of the total processed by the Department of State.

USPS assets are distributed worldwide, but the bulk of these assets are located in and around postal facilities throughout the United States. Of these assets, the most visible are those through which the public acquires products and services. Figure 2 provides an overview of the most apparent postal assets from the perspective of the USPS customer.

About 350,000 USPS collection boxes are used to introduce mail into the USPS mail flow. The USPS has limited means to protect the mail deposited in the collection boxes, which generally are not guarded and not under surveillance. USPS assets not shown in Figure 2 are the millions of bags, boxes, trays, hampers, rolling stock, and various over-the-road and aircraft containers that are in constant service throughout postal operations.

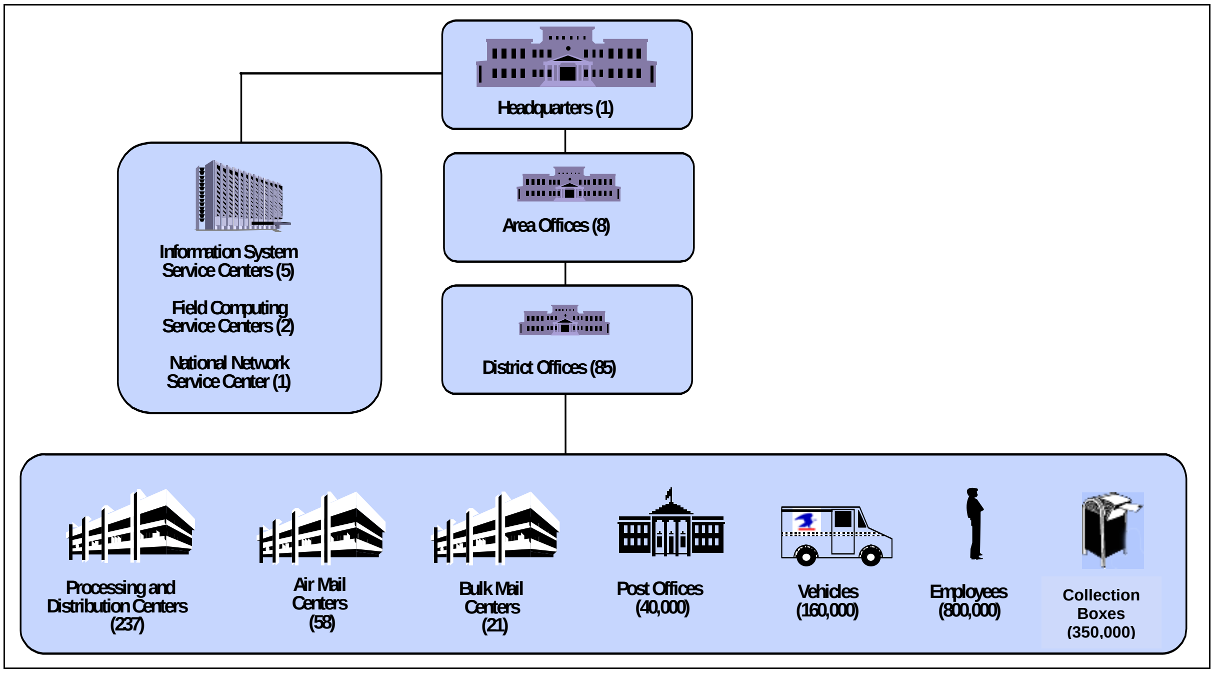

Headquarters (1)
Information System Service Centers (5)
Field Computing Service Centers (2)
National Network Service Center (1)
Area Offices (8)
District Offices (85)
Processing and Distribution Centers (237)
Air Mail Centers (58)
Bulk Mail Centers (21)
Post Offices (40,000)
Vehicles (160,000)
Employees (800,000)
Collection Boxes (350,000)

Figure 2 USPS Customer Service and Administrative Assets

The USPS provides an array of services for a wide variety of mail items. Standard mail types are letters, flats, and parcels. These items may be introduced into the mail stream in many ways. USPS procedures and processes provide some linking mechanisms for certain types of mail to their points of origin and receipt. These mail types include registered, express, certified, insured, postage due, and COD (cash on delivery) mail and any item going through U.S. Customs. Of greater concern with regard to terrorist threats is the mail that is anonymously introduced into the mail stream. Anonymous mail may be collected from mailboxes and collection boxes, as well from thousands of drop points at customer sites, mail facilities, and other locations across the country.

Approximately 90% of the 700,000 USPS career employees are covered by collective bargaining agreements. The USPS labor force is primarily represented by the American Postal Workers Union (APWU), National Association of Letter Carriers (NALC), National Postal Mail Handlers Union (NPMHU), and National Rural Letter Carriers Association (NRLCA). The APWU is the largest postal union, representing about 272,000 USPS career employees and 5,000 transitional employees primarily in the clerk, maintenance, and motor vehicle services crafts. The APWU also represents nearly 2,000 private-sector mail workers. The NALC, which is the second largest postal union, represents more than 224,000 career employees. NALC members deliver mail to residences and businesses along city delivery routes. NRLCA career and part-time relief workers deliver mail to residences and businesses along rural delivery routes. The NPMHU, a division of the Laborers' International Union of North America, represents more than 55,000 career employees engaged in the bulk transfer, loading, and unloading of mail. Union membership figures are as of July 2006, according to the USPS (APWU 2007).

UPS

United Parcel Service of America, Inc. is the world's largest package delivery company, in terms of revenue and volume. In 2006, UPS delivered almost 4 billion packages worldwide — 15.6 million packages each business day for 1.8 million shipping customers to 6.1 million consignees in more than 200 countries and territories. Annual total revenue was about $47.5 billion. Freight is transported by road, rail, ocean, and air. The company operates a fleet of 282 aircraft and 94,500 package delivery vehicles. Freight vehicles consist of 6,800 tractors and 22,800 trailers. Worldwide, UPS has 428,000 employees, 3,000 operating facilities, and 150,000 access points. UPS corporate headquarters are located in Atlanta, Georgia. Latin American and Caribbean regional headquarters are in Miami, Florida (UPS 1994–2006; UPS 2006).

A subsidiary, UPS Air Cargo, provides freight forwarders with direct, airport-to-airport deliveries to more than 150 strategically located airports around the world. UPS Air Cargo maintains a comprehensive hub-and-spoke network in the United States and overseas. The company's all-points international air hub is located in Louisville, Kentucky, with other regional hubs located in strategic cities across the United States. International air hubs are located in Miami, Florida, and four locations outside the continental United States (OCONUS) (UPS 1994–2007).

Fed Ex

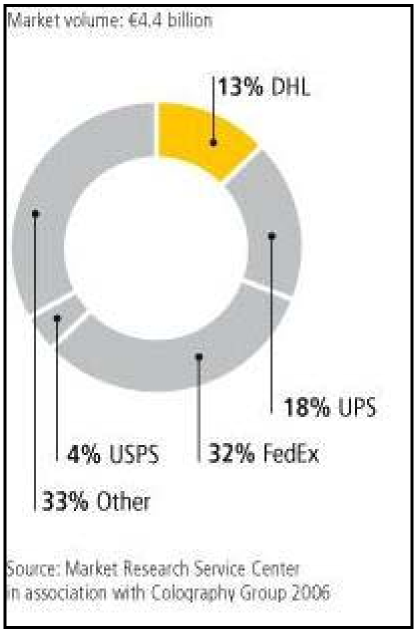
The two package delivery subsidiaries of Federal Express — FedEx Express and FedEx Ground — delivered 6.1 million packages each day in the company's fiscal year ending in May 2006 (FedEx 2006). FedEx Freight delivered an additional 67,000 shipments per day.

The company's FedEx Express unit is the world's number one express transportation company, delivering some 3.3 million packages daily. The FedEx Ground unit provides ground delivery of small packages in North America. Less-than-truckload (LTL) carrier FedEx Freight hauls heavier items throughout the United States, and FedEx Custom Critical specializes in urgent freight deliveries. To boost FedEx Freight's long-haul capabilities, FedEx bought LTL carrier Watkins Motor Lines in 2006 (Hoovers.com 2007).

FedEx's total revenue for shipping and non-shipping components totaled $33.3 billion in the company's fiscal year ending in May 2006. FedEx operated a fleet of 671 aircraft and maintained had an average full-time equivalent (FTE) employee and contractor workforce of 221,677 during the fiscal year ending May 2006. FedEx corporate headquarters are in located Memphis, Tennessee.

DHL

DHL, a subsidiary of the German conglomerate Deutsche Post, operates an air- and ground-based transport network in the United States through which it moves all domestic and international shipments; domestic express products account for more than 90% of the total market. In 2005, DHL occupied third place in the international Courier, Express, and Parcels (CEP) market in the United States (Figure 3).



Source: Market Research Service Center in association with Colography Group 2006

Figure 3 International CEP Market (by Company) in the United States in 2005

Common Facility Characteristics

USPS

The USPS mail processing operation is a complex and diversified system, requiring coordinated efforts by mail processing plants and delivery units across the country. Mail handling operations can be divided into three distinct categories — collection, sorting, and distribution — although the physical processes involved in mail collection and distribution within the delivery units are routinely performed by the same workforce and vehicles.

While much of this processing is labor intensive, involving a large workforce distributed across the country, a large portion of the work required to sort the mail for distribution has been automated by a series of high-volume machines. Table 1 lists some of the more commonly used equipment used to process the anonymous mail within USPS Processing and Distribution Centers (P&DCs).

Figures 4 and 5 show examples of mail processing equipment in P&DCs (optical character reader and bar code sorter). Figure 6 provides a view of the mail handling process, showing collection, sorting, and distribution, as well as interactions between delivery units and processing plants and among the processing plants. Figure 7 provides a more concrete view, illustrating some of the equipment used to perform the processes. Embedded within these operations are plant-to-plant interactions which are depicted in Figure 8.

Table 1 Mail Processing Equipment

Equipment	Estimated Quantity in Operation
Dual-pass rough cull systems "Barney" (DPRCs)	280
Advanced facer canceller system (AFCS)	910
Multiline optical character reader (MLOCR)	875
Letter mail labeling machine (LMLM)	360
Mail processor bar code sorter (MPBCS)	800
Delivery bar code sorter (DBCS)	4,300
Carrier sequence bar code sorter (CSBCS)	3,730
Flat sorting machine (FSM)	470
Small parcel and bundle sorter (SPBS)	350
Tray management system (TMS)	30

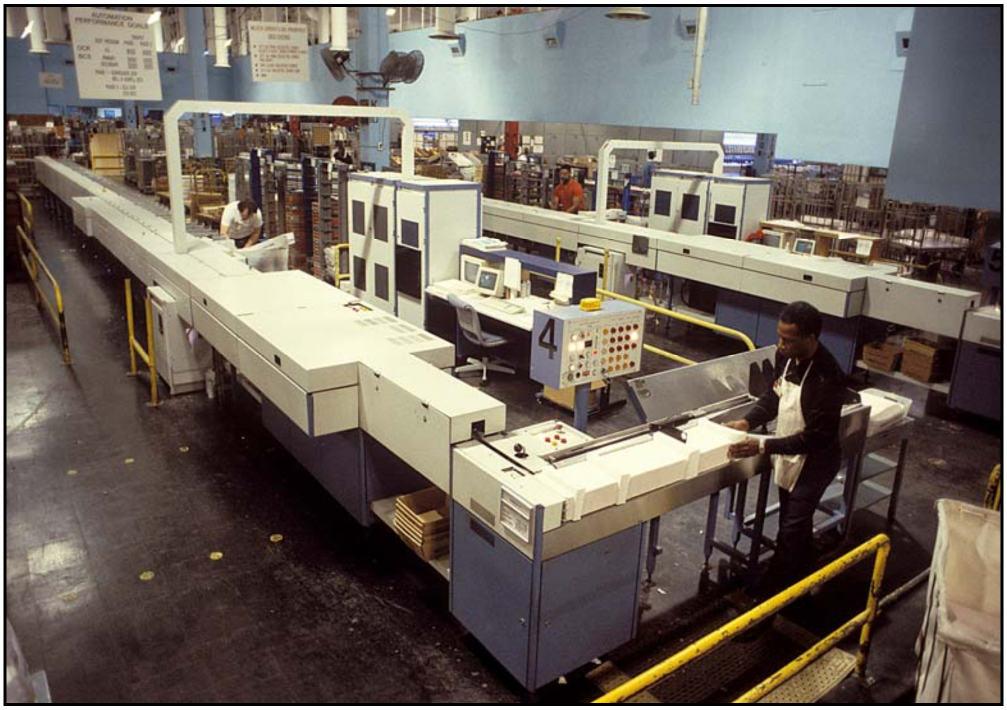


Figure 4 Typical Optical Character Reader

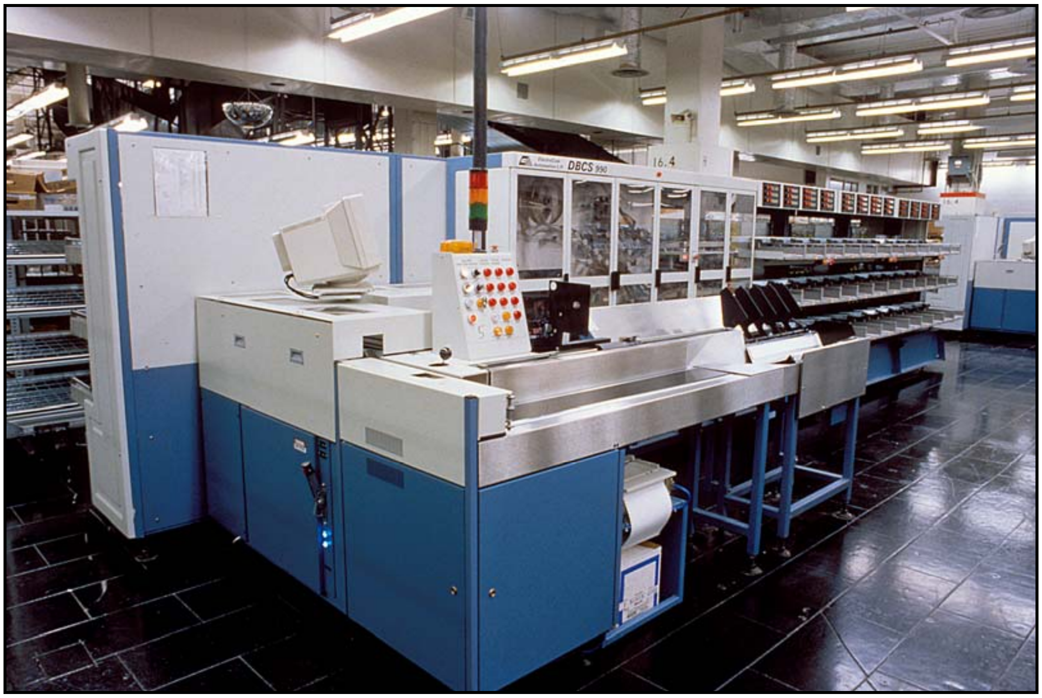


Figure 5 Typical Delivery Bar Code Sorter

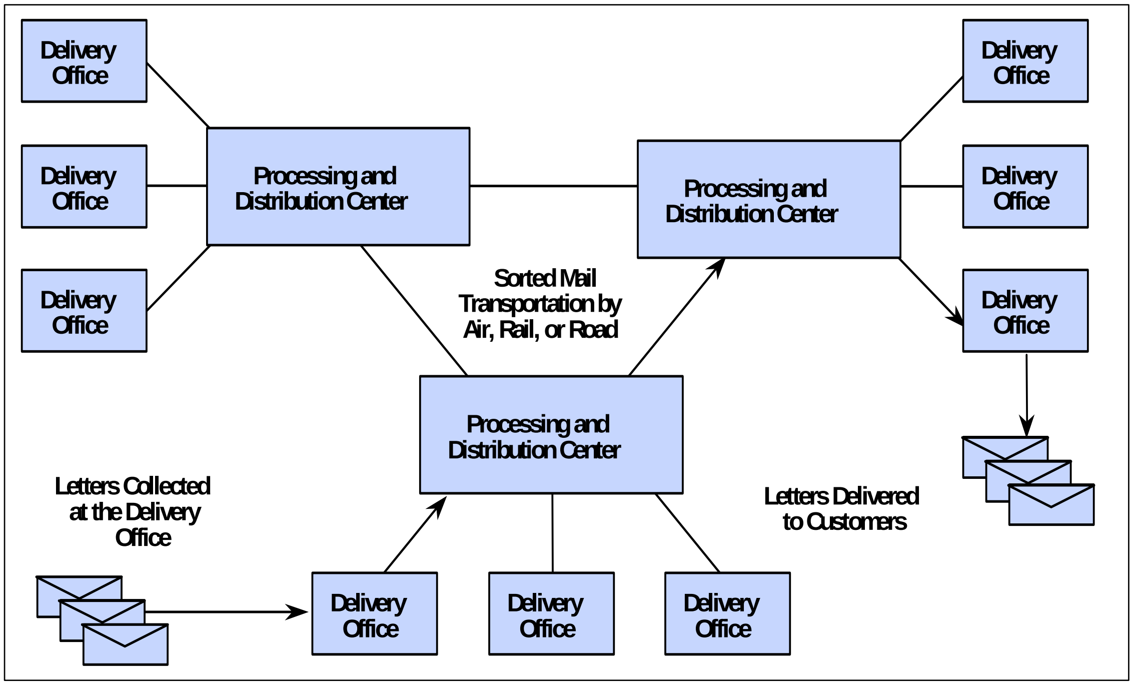

Delivery Office
Delivery Office
Processing and Distribution Center
Processing and Distribution Center
Delivery Office
Delivery Office
Delivery Office
Delivery Office
Sorted Mail Transportation by Air, Rail, or Road
Processing and Distribution Center
Letters Collected at the Delivery Office
Letters Delivered to Customers
Delivery Office
Delivery Office
Delivery Office

Figure 6 Mail Flow Block Diagram

Figure 6 Mail Flow Block Diagram

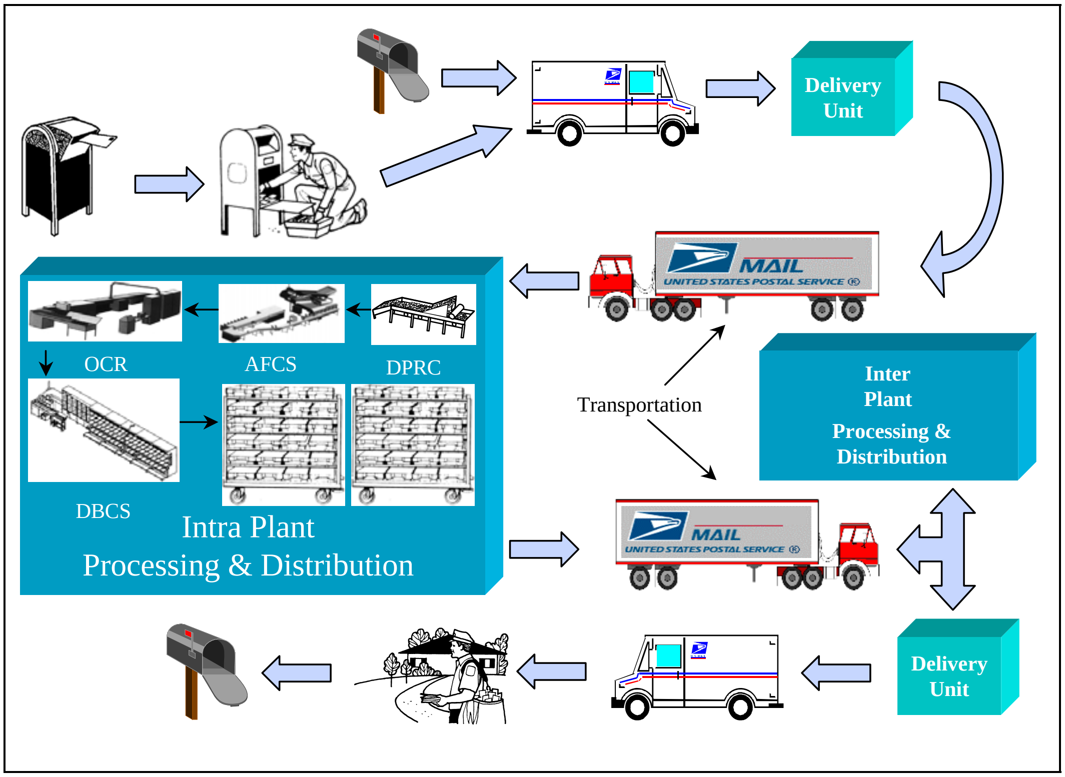

Delivery Unit
OCR
AFCS
DPRC
DBCS
Intra Plant Processing & Distribution
Transportation
Inter Plant Processing & Distribution
Delivery Unit

Figure 7 Mail Handling Overview

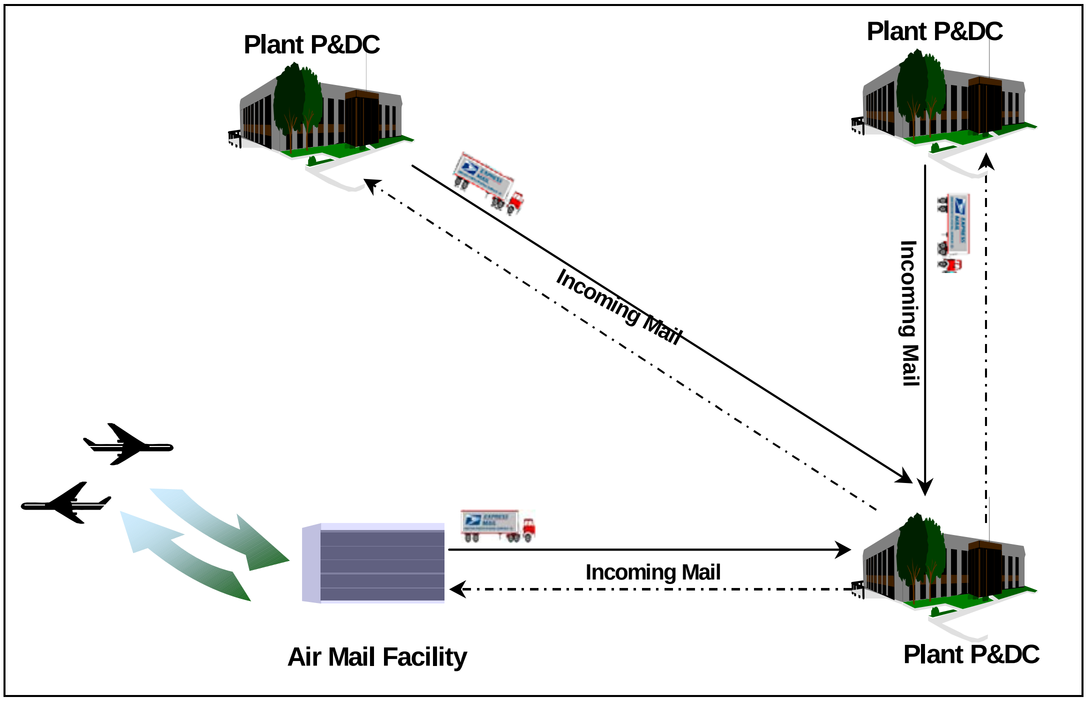
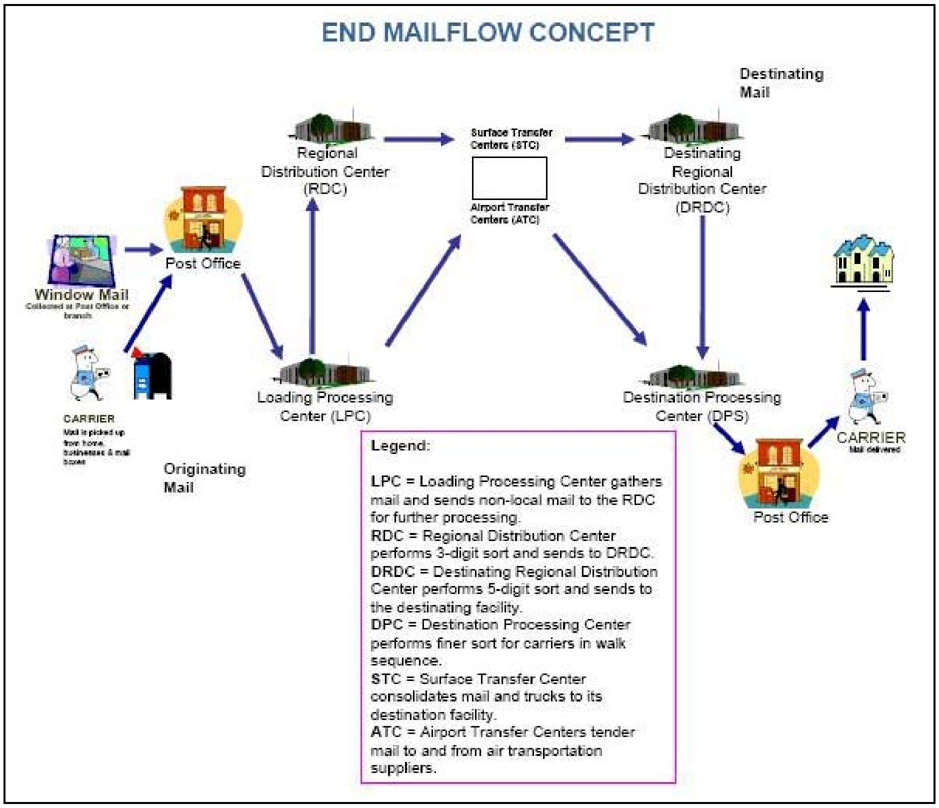


Figure 8 Plant-to-Plant Interaction

In 2003, The President's Commission on the Postal Service said that the USPS had more infrastructure than needed and that many assets were not effectively aligned with changing requirements. The infrastructure included more than 450 mail processing facilities, along with one of the world's largest transportation networks — some 215,000 vehicles and more than $5 billion in annual contracts for highway, air, rail, and water transport. To address this issue, the USPS developed the Evolutionary Network Development (END) initiative to optimize its processing and transportation network. The END initiative contains processes and tools for analyzing the optimal number, location, and functions of mail processing and transportation facilities. The charter of END is to create a flexible logistics network that reduces Postal Service and customers' costs, increases operational effectiveness, and improves consistency of service. The Postal Service is taking an incremental approach to streamlining the mail processing networks using END as a framework. Figure 9 shows the END mail flow concept that is being implemented by the USPS; it also describes the functions of included postal facilities (Vogel 2006).


END MAILFLOW CONCEPT
Destinating Mail
Regional Distribution Center (RDC)
Surface Transfer Centers (STC)
Airport Transfer Centers (ATC)
Destinating Regional Distribution Center (DRDC)
Post Office
Window Mail
Collected at Post Office or branch
CARRIER
Mail is picked up from home, businesses & mail boxes
Loading Processing Center (LPC)
Destination Processing Center (DPS)
Originating Mail
CARRIER
Mail delivered
Post Office

Legend:

LPC = Loading Processing Center gathers mail and sends non-local mail to the RDC for further processing.
RDC = Regional Distribution Center performs 3-digit sort and sends to DRDC.
DRDC = Destinating Regional Distribution Center performs 5-digit sort and sends to the destinating facility.
DPC = Destination Processing Center performs finer sort for carriers in walk sequence.
STC = Surface Transfer Center consolidates mail and trucks to its destination facility.
ATC = Airport Transfer Centers tender mail to and from air transportation suppliers.

Figure 9 USPS's Evolutionary Network Development

Private Shipping Companies

Private postal and shipping companies have their own unique infrastructures for handling, processing, and delivering letters and parcels. Both UPS and FedEx rely on near-real-time data to manage their operations through the use of wireless technology in the field and in their facilities.

FedEx and UPS maintain massive operations involving package centers, sorting facilities, and hubs through which packages, letters, etc., travel. For example, FedEx's main hub in Memphis, Tennessee, handles about 2 million packages a day; the facility comprises a group of runways and buildings that encompass about 1.5 square miles and make the Memphis airport the number one cargo airport in the world. UPS's Worldport hub in Louisville, Kentucky, has a similar scale. Even a small facility, such as the Richmond, California, UPS sorting facility, is a stadium-size maze of belts and funnels through which packages move as they are unloaded from trucks and trains onto other trucks and trains for transshipment (Gruman 2004).

An example of a large UPS consolidation and distribution facility is its 1.9-million-square-foot, state-of-the-art, fully integrated package sorting facility in Chicago, Illinois. The facility has more than 4 million linear feet of wire, 474 devices, and 1,275 motors. The Chicago facility moves an estimated 2 million packages through an intricate system of conveyors, diverters, fixed-position and bar code scanners, printers, and applicators every day. Packages arrive at one of the 122 receiving doors and travel over some of the 30 miles of conveyors to one of the 1,050 shipping doors. Figure 10 shows the interior of a UPS sorting facility (Electrical Systems, Inc. undated).

In sorting facilities, both UPS and FedEx use a device called a ring scanner, which is a bar code reader mounted on two fingers and, traditionally, wired to a terminal strapped to the forearm. Both companies use the same devices, made by Symbol Technologies and Intermec Technologies. But UPS is replacing its model with a new model from Symbol and Motorola that moves the terminal to the waist and uses Bluetooth to communicate with a finger-mounted scanner. Figure 11 shows a traditional UPS Ring Scanner (WindowsForDevices.com 2004).

Figure 10 Conveyors at UPS Sorting Facility (Source: Electrical Systems, Inc. undated)

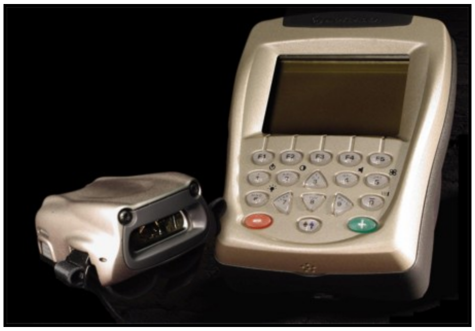


Figure 11 UPS Ring Scanner

Both UPS and FedEx have tens of thousands of couriers roaming the world to pick up and deliver packages, making millions of stops per day. Couriers for both companies use wireless handhelds to carry out their duties. FedEx's 40,000 couriers use a PowerPad device with a Bluetooth radio to send package information scanned during pickup from the 50,000 drop boxes visited each day. The PowerPad also has infrared connectivity, which FedEx uses to send lock and unlock signals to the drop boxes.

The Delivery Information Acquisition Device (DIAD) IV handheld device is UPS's counterpart to FedEx's PowerPad. Functionally, the DIAD IV is analogous to the PowerPad, except UPS's 70,000 handhelds transmit data directly to central UPS operations using a digital cellular connection. Several years ago, FedEx installed cellular transmitters in its trucks to send package data. FedEx chose to keep that infrastructure and simply switched to Bluetooth radios to connect the handhelds to the trucks.

Most mail and package services operate independently of one another using parallel facilities. Many UPS, FedEx, and USPS facilities are located at airports. Figure 12 shows contiguous UPS and FedEx airport facilities (SIU GAO 2006).

An exception is FedEx SmartPost, which is a joint effort with the USPS. Packages are dropped off at FedEx facilities and shipped via FedEx before being handed over to the USPS for residential delivery. The process skips intermediate postal processing centers, minimizing handling. Under this program, packages are delivered to Bulk Mail Centers (BMC), Sectional Center Facilities (SCF), and Destination Delivery Units (DDUs), including local post offices.

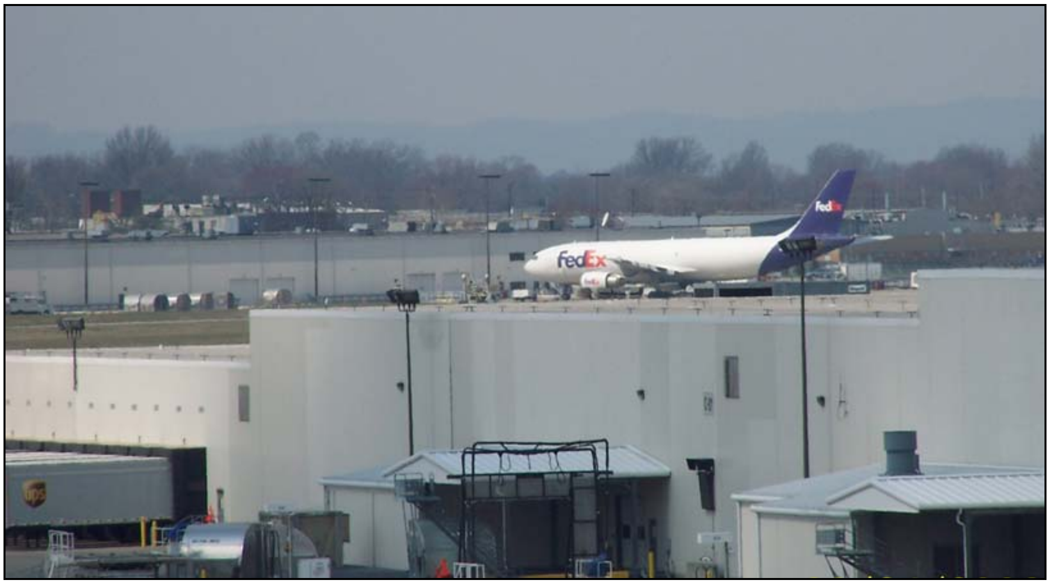


Figure 12 Contiguous UPS and FedEx Facilities

Potential Indicators of Terrorist/Threat Activity

Threats can be posed by an individual or a group that possesses the capability and intent to do harm. Domestic and international terrorists, adversarial nations, disaffected individuals or groups, disgruntled employees, and organized adversarial groups are all potential sources of threat. Threats can originate from individuals or groups with knowledge of the systems and equipment used at a facility. Insider information can be known by disgruntled or compromised employees, and detailed information on equipment and operating procedures can also be gathered from open sources or from active or former employees.

Threats Versus Hazards

Hazards and threats are two distinct entities. Hazards are situations or things that possess inherent and known danger. Empirical databases concerning hazards exist or can be created from historical records to determine the statistical probability of a future event. The effects of an incident involving a hazard can be forecast with relative precision because of the hazard's known attributes. Security threats, however, are more difficult to characterize or quantify than routine hazards. The capabilities and intent of the purveyor of a threat may not be known, and the adaptive, thinking nature of the purveyor makes statistical analysis and calculations of probability a challenge.

The assessment of hazards falls within the discipline of safety, whereas the assessment of threats and the protection against them fall within the discipline of security. Often, the same group within an enterprise manages the responsibility for both sources of risk. Some safety and security efforts are mutually reinforcing; however, safety and security are not synonymous, and the two disciplines are different.

Targeting Objectives

To assess threats, one commonly accepted framework is to identify the threat purveyor's objectives and goals, potential targets, the means by which the threat might be carried out, and the knowledge and tactics required. A clear understanding of these factors, combined with an appreciation of the value of the assets and systems and the impact of unauthorized access and subsequent malicious activity, provides a basis for better defining the investment that might be needed to prevent such access. This process is useful for identifying realistic threats. Attackers have a range of objectives, as shown in Figure 13.

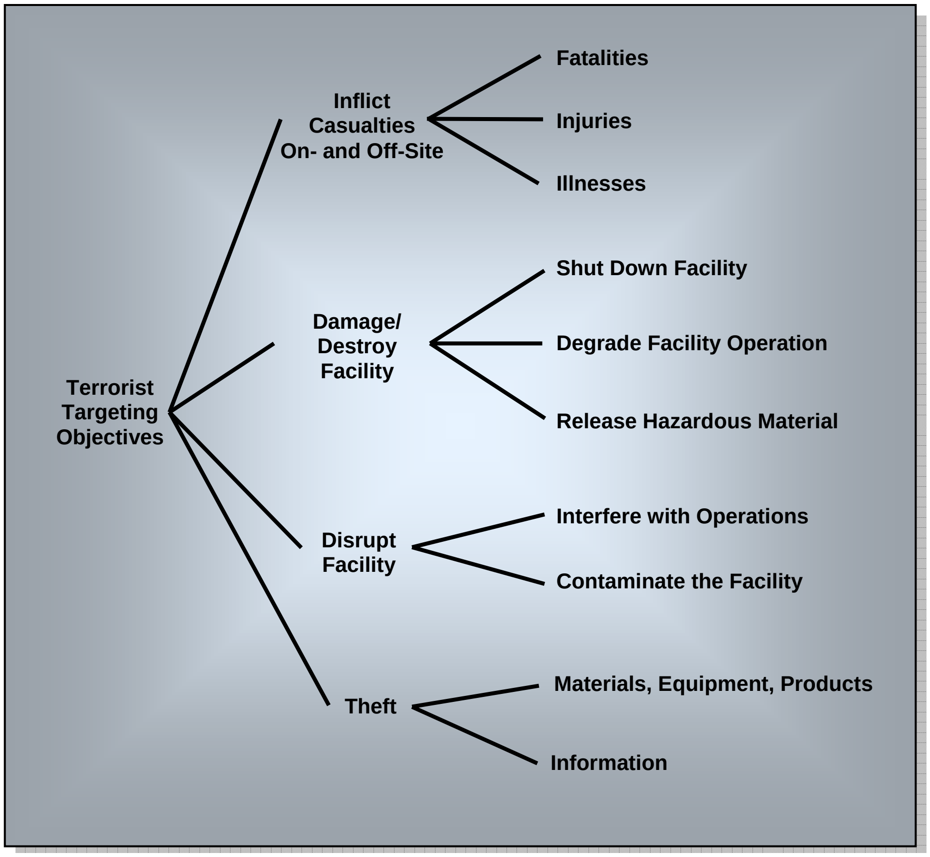

Terrorist Targeting Objectives
Inflict Casualties On- and Off-Site
Fatalities
Injuries
Illnesses
Damage/ Destroy Facility
Shut Down Facility
Degrade Facility Operation
Release Hazardous Material
Disrupt Facility
Interfere with Operations
Contaminate the Facility
Theft
Materials, Equipment, Products
Information

Figure 13 Terrorist Targeting Objectives

Weapons and Tactics

In targeting critical infrastructure, potential adversaries can employ a wide range of weapons, tools, and tactics, including the possible use of explosives. Adversaries have used the shipping of biological and chemical agents to contaminate postal and shipping facilities. They have also used the sector to deliver explosives and hazardous materials (HAZMAT) to other targets. Some antagonists are gaining expertise in the use of less traditional methods, such as cyber attacks. Some weapons, tools, and tactics are discussed in the following sections.

Improvised Explosive Device

An improvised explosive device (IED), or 'homemade bomb,' can be constructed of commonly available materials, construction explosives (e.g., dynamite), or stolen military-grade explosives. An IED can be carried into a facility by an individual (e.g., a suicide bomber) or deposited in an unnoticed location for detonation by a timer or by remote control (Figure 14). Vehicle-borne IEDs (VBIEDs) are loaded into a car or truck or onto a motorcycle. These vehicles can be parked close to the facility and placed where large numbers of people gather, or they can be crashed through barriers and then detonated. They are much larger and more dangerous than IEDs carried by an individual. VBIEDs are very common throughout the world. Letter and package IEDs are a specific threat to postal and shipping networks. While adversaries may direct these devices at postal and shipping facilities, more frequently, the postal and shipping networks are used to deliver IEDs to targeted facilities and individuals.

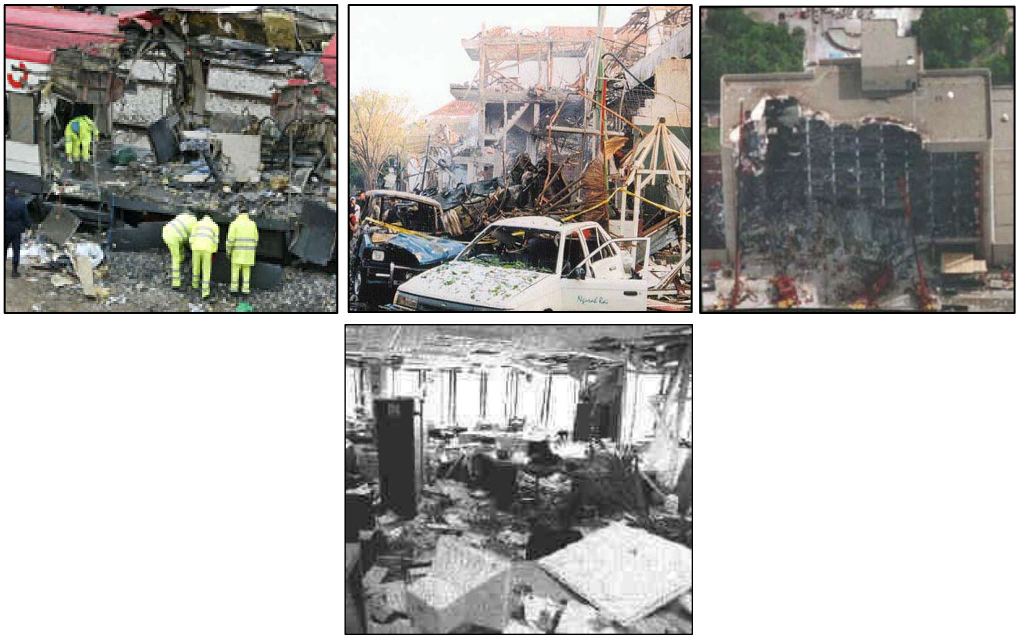


Figure 14 Damage from (clockwise from upper left): Backpack IED, Car-based VBIED, Truck-based VBIED, and Letter Bomb (Source for letter bomb photo: Safecity.com undated)

Arson

Intentional fires can be set by tossing highly flammable materials (such as gasoline) into a facility (see Figure 15). Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson is a threat before, during, and after normal business hours.

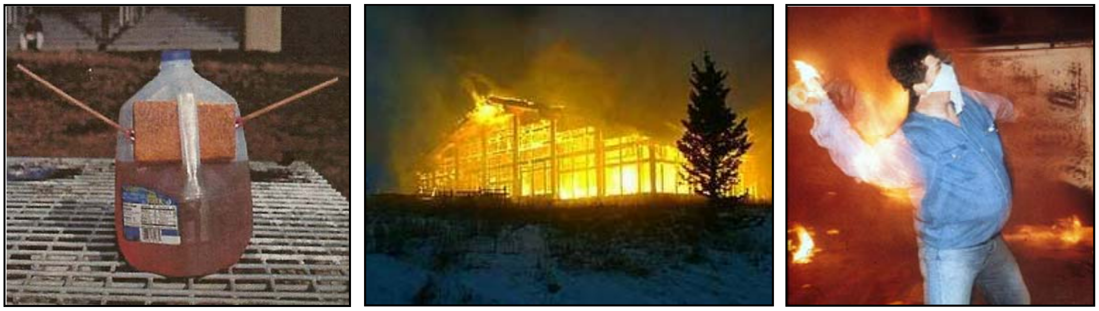


Figure 15 Arson (Left to Right): Mock-up of Arson Device, Vail Ski Resort Fire, and Arsonist

Small Arms Attack

Conventional firearms, automatic weapons, shoulder-carried rocket-propelled grenades, or similar weapons can be used to indiscriminately shoot people or take hostages (Figure 16).

Figure 16 Small Arms Attack (Left to Right): Terrorists with Conventional Small Firearms and Grenade Launchers

Assassination/Kidnapping

Many terrorist acts have involved the assassination of key personnel or the kidnapping of individuals and taking of hostages (Figure 17).

Figure 17 Various Hostage and Kidnapping Situations

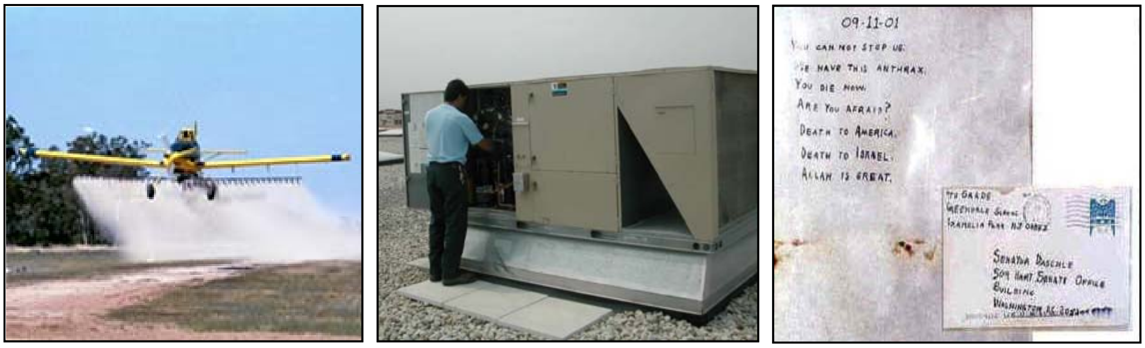
Chemical Attack

Chemicals can be exploited or used by terrorists as a weapon. Such chemicals include toxic industrial chemicals (e.g., ammonia, hydrogen fluoride) already present at the site either as part of a manufacturing process or for use in normal operations (e.g., chlorine stored on site for use in water treatment plants, swimming pools) or chemicals transported by truck or railroad and brought near a facility or large gathering of people, where they could be dispersed by explosives (Figure 18). Chemical warfare agents (e.g., sarin, VX) are another weapon of concern. Although not readily available, they have been procured and used by terrorists. The 1995 sarin gas attack in the Tokyo subway is an example.

Figure 18 Chemical Attacks (Left to Right): Tokyo Sarin Attack, Methanol Plant, and Rail Car for Acids

Biological Attack

Biological pathogens (e.g., anthrax, botulin, plague) can cause disease and are attractive to terrorists because of their potential to cause mass casualties and exhaust response resources. Postal and shipping networks are often used to deliver biological pathogens (e.g., through contaminated letters delivered by mail) (Figure 19) to targeted facilities and individuals. In the process, collateral postal and shipping facilities and personnel are often contaminated. Biological agents also can be dispersed in the atmosphere (e.g., via crop-dusting aircraft); introduced into a facility through its heating, ventilation, and air-conditioning (HVAC) system; or spread by contact (e.g., through infected plants, animals, or human carriers).



09-11-01

YOU CAN NOT STOP US.
WE HAVE THIS ANTHRAX.
YOU DIE NOW.
ARE YOU AFRAID?
DEATH TO AMERICA.
DEATH TO ISRAEL.
ALLAH IS GREAT.

4TH GRADE
GREENDALE SCHOOL
FRANKLIN PARK NJ 08852

SENATOR DASCHLE
509 HART SENATE OFFICE
BUILDING
WASHINGTON D.C. 20510

Figure 19 Biological Attacks (Left to Right): Crop Dusting, Rooftop HVAC Unit, and Anthrax-laced Letter

Nuclear/Radiological Attack

Weapons-grade nuclear material is relatively difficult to obtain. However, some sources of nuclear and radiological material are more readily available (e.g., from medical diagnostic equipment) and are more easily delivered. Radiological agents include radioactive material from various sources, such as medical or industrial equipment (Figure 20). All of these agents could be introduced into a facility either directly (e.g., by spreading them on surfaces where people will have direct contact) or through the HVAC system. Radiological dispersion devices (RDDs), often called ‘dirty bombs,’ have these materials attached to an explosive to create a wide area of contamination.

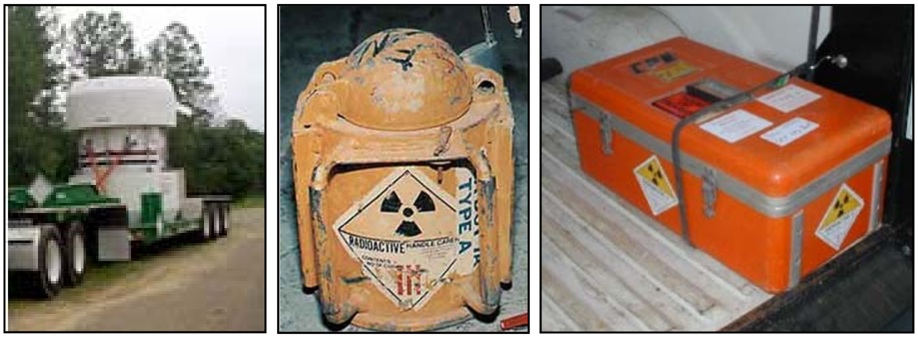


Figure 20 Various Transport Containers for Radioactive Material

Sabotage

The disruption or damage to or destruction of a structure or facility through sabotage (Figure 21), the introduction of HAZMAT into the facility, and the contamination of facility products are of concern. Sabotage can be perpetrated by employees or by outsiders. In some cases, sabotage is designed to release HAZMAT from a facility into the surrounding area or to cause cascading problems across interdependent critical infrastructures.

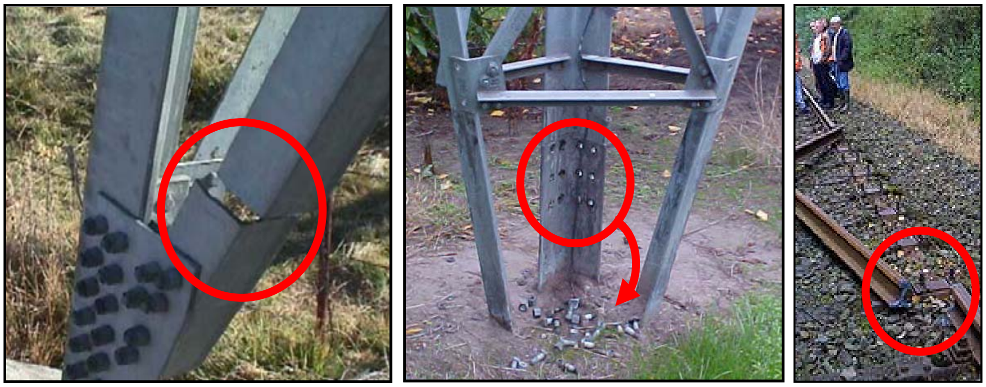


Figure 21 Sabotage (Left to Right): Tower Leg Cut, Bolts Removed, and Tracks Cut

Aircraft Attack

Both commercial and general aviation aircraft can be hijacked and used to deliver attackers, explosives, or HAZMAT to an area or facility. The aircraft themselves can also be used as weapons (Figure 22).

Figure 22 Aircraft Attacks (Left to Right): Used as a Weapon and Used for Hijackings

Maritime Attack

Ships and boats of various sizes or cargo containers can be used to deliver attackers, explosives, or HAZMAT to an area or facility (Figure 23). The vessels themselves can be used as weapons when outfitted as waterborne IEDs (WBIEDs) and maneuvered into position near a target or rammed into a target. Targets include ships, ports, and bridges. The attack on the *USS Cole* is an example of a maritime attack.

Figure 23 Maritime Attacks (Left to Right): *USS Cole* Damage and Cargo Container Operations at a Port

Cyber Attack

Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Information can be altered, corrupted to render it unusable, or stolen. Information systems can be attacked with the intent of overloading the equipment (e.g., denial-of-service attacks). Some information systems can be used to mount attacks on other systems. Supervisory control and data acquisition (SCADA) and other process control systems that are used to control mechanical equipment (e.g., pipelines, railroad switches, industrial process streams) can be infiltrated so that the equipment can be operated in such a way as to cause damage and inflict on-site and off-site casualties (Figure 24).

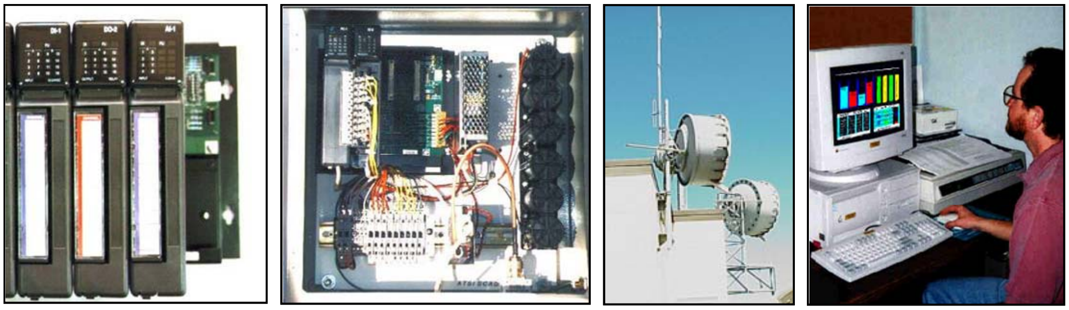


Figure 24 Common SCADA Components (Left to Right): Programmed Logic Controller (PLC), Remote Terminal Unit (RTU), Antenna Systems, and Operator Interface

Al-Qaeda’s Surveillance Objectives

The list of surveillance objectives provided in the next chart is from captured reports on how to ‘case’ target subjects that were developed by al-Qaeda operatives to be used against the U.S. financial sector. While similar reports targeting assets in other sectors have not been recovered to date, the tactics are fairly uniform, and studying the list can help asset owners recognize potential surveillance activities.

Understanding the signature behaviors associated with terrorist operational planning will help infrastructure security personnel better portray real and perceived terrorist surveillance efforts in their reports on suspicious incidents. Improved reports and documentation could ultimately lead to the disruption of terrorist attack planning. While much is unknown about the terrorist threat to the nation, it is known that al-Qaeda and its affiliates remain interested in striking the United States.

SURVEILLANCE OBJECTIVES

These objectives describe the kinds of information that terrorists monitor when planning an attack.

Surveillance and Countersurveillance

- Identity of places where further surveillance can take place
- Identity of places where countersurveillance can be detected

Facility Security

- Presence or absence of security cameras
- Number, location, type, and coverage of security cameras
- Security screening procedures for employees, visitors, and vehicles
- Procedures for changing of the guard
- Opportunities for theft of facility identification (ID) cards or special license plates
- Proximity to first-responder locations
- Security event response times
- Number, gender, ethnicity, location, dress, weapons, and equipment of security/police forces

Facility Access

- Configuration and staffing of control points
- Visitor access procedures
- Availability of tours
- Location of roadways, entrances, parking lots, gates, and access points

Facility Construction

- Construction materials used
- Building shape, height, and setbacks
- Location of vulnerable structural components
- Opportunities for cascading damage effects
- Location of executive offices and employee meeting places
- Location of power and HVAC systems
- Adequacy of emergency exits, escape routes, and fire suppression systems

Target Dynamics

- Opening and closing times
- Lunch and break times
- Shift changes
- Patterns of concentration of people and vehicles; traffic congestion
- Nearby people and vehicle movement throughout the day
- Monitoring of police radio frequencies and recording of emergency response times

Secondary Targets

- Nearby alternative targets
- Nearby collateral targets

Potential Indicators

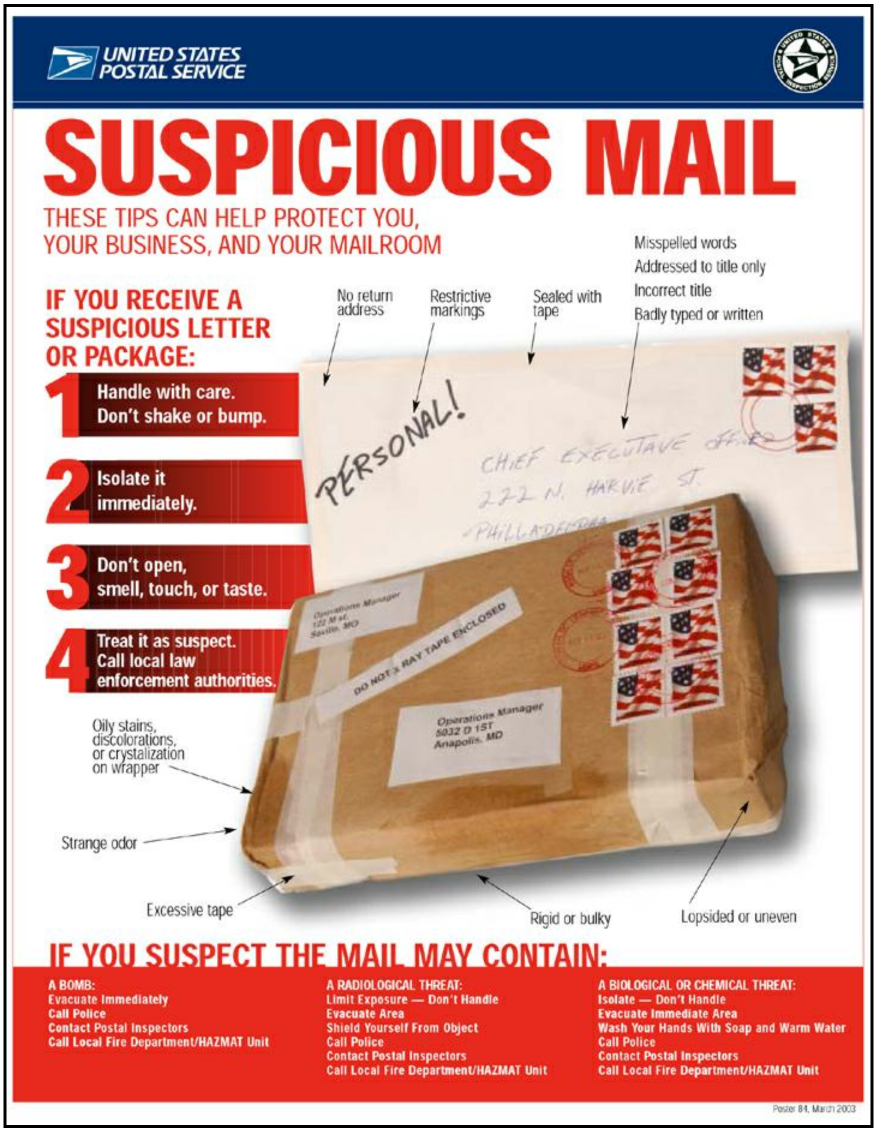
An indicator could be any suspicious activity that warrants a reaction. A reaction could be an investigation, a root-cause analysis, a communication, or an emergency response.

When people look at the normal environment, the unusual should attract their attention. If individuals know their environment, they will more readily notice something out of the ordinary or something that does not quite ‘fit.’ The same idea applies to the threat environment. People operate and inspect facilities and purchase, store, or use industrial products every day. Constant attention to these indicators can help people know when to alert officials of the possibility of an incident.

The section on imminent attack indicators is followed by sections that describe surveillance indicators; transactional and behavioral indicators; and indicators of possible threats from weapons, explosives, or chemical, biological, or radiological (CBR) materials and devices. The charts in these sections outline additional indicators of possible surveillance activity or focus. These charts are fairly detailed; however, their main intent is to give asset owners and employees information about surveillance activities that might be associated with a given asset and to help them recognize (and then report) any unusual events.

Imminent Attack Indicators

Indicators of an imminent attack include people who demonstrate unusual or suspicious behavior, vehicles that demonstrate unusual or suspicious behavior, or unusual or suspicious packages that require an immediate response. Included in this category are practice-run indicators (i.e., activities associated with rehearsing or carrying out exercises for a terrorist attack). IEDs and chemical and radiological agents contained in letters and packages are a specific threat to postal and shipping facilities and their clientele. Figure 25 is a poster prepared by the USPS delineating potential indicators of malevolent packages/letters.



UNITED STATES POSTAL SERVICE

SUSPICIOUS MAIL

THESE TIPS CAN HELP PROTECT YOU,
YOUR BUSINESS, AND YOUR MAILROOM

IF YOU RECEIVE A SUSPICIOUS LETTER OR PACKAGE:

1 Handle with care. Don't shake or bump.

2 Isolate it immediately.

3 Don't open, smell, touch, or taste.

4 Treat it as suspect. Call local law enforcement authorities.

No return address

Restrictive markings

Sealed with tape

Misspelled words
Addressed to title only
Incorrect title
Badly typed or written

Oily stains, discolorations, or crystalization on wrapper

Strange odor

Excessive tape

Rigid or bulky

Lopsided or uneven

IF YOU SUSPECT THE MAIL MAY CONTAIN:

A BOMB:
Evacuate Immediately
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

A RADIOLOGICAL THREAT:
Limit Exposure — Don't Handle
Evacuate Area
Shield Yourself From Object
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

A BIOLOGICAL OR CHEMICAL THREAT:
Isolate — Don't Handle
Evacuate Immediate Area
Wash Your Hands With Soap and Warm Water
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

Poster 84, March 2003

Figure 25 USPS Poster on Suspicious Mail
(Source: University of Wisconsin, Milwaukee 2007)

IMMINENT ATTACK INDICATORS (at or near a postal or shipping facility)

These indicators suggest unusual and suspicious behavior that requires immediate response.

Indicators about Activities (Observed or Reported)

- Persons in crowded areas wearing unusually bulky clothing that might conceal explosives who could be
  - Patting down or feeling under their clothing or concealing weapons
  - Showing electrical wires from under their clothing or tightly clutching an object that could be a trigger device
  - Displaying excessive nervousness or anxiety
  - Wearing excessive amounts of cologne or perfume to mask the scent of explosives
- Persons or teams of people attempting to gain illegal entry (e.g., scaling fences, breaking into doors) or appearing to prepare to launch standoff weapons (e.g., rocket-propelled grenades) at the facility
- Nonmilitary persons seen with military-style weapons and clothing or equipment
- Any type of vehicle illegally located near facility buildings or places with large numbers of people (The vehicle may be unattended or may have a driver [e.g., who could detonate explosives]. A driver may [a] demonstrate nervousness and anxiety, [b] be constantly scanning the area for law enforcement personnel, or [c] be looking for ways to impact the largest number of victims.)
- Unexpected or unfamiliar delivery trucks arriving at the facility
- Vehicles (a) approaching at an unusually high speed or (b) steering around barriers and traffic controls
- Unattended package (e.g., backpack, briefcase, box) that might contain explosives
- Suspicious package and/or letter received by a carrier that might contain explosives or CBR agents (The packages or mail may have (a) no return address, (b) excessive postage, (c) been sent from outside the United States, (d) indications of liquids/powder leaking from them, or (e) unusual odors.)
- Evidence of unauthorized access to HVAC areas of a building (Indications of unusual substances, such as unknown powders, droplets, or mists, may be present near air intakes.)
- Recent damage to a perimeter fence or gate or damage to perimeter lighting, cameras, or sensors

Practice-Run Indicators (Observed or Reported)

- Persons with an unusual interest in security measures, personnel, entry points, access controls, or barriers
- Unusual behavior, such as people staring or quickly looking away or vehicles entering or leaving parking areas
- Training scenarios carried out by paramilitary groups or other organizations advocating violence
- Persons displaying anxiety, such as retracing their steps
- Persons observing security drills or procedures
- Persons mapping routes or timing traffic lights and traffic flow
- Persons questioning security or facility personnel
- Persons wearing disguises to elude detection or gain access to restricted areas (including wearing military, medical, firefighter, or police uniforms or dressing like a pregnant woman)

Surveillance Indicators

Surveillance indicators are persons or unusual activities in the vicinity of a critical infrastructure or key resource that are intended to gather information about the asset and/or its operations, shipments, or protective measures.

Terrorist surveillance may be fixed or mobile. Fixed surveillance is performed from a static, often concealed position, possibly an adjacent building, business, other facility, or high ground. In fixed-surveillance scenarios, terrorists may establish themselves in a public location over an extended period of time or choose disguises or occupations, such as street vendors, tourists, repair or delivery persons, photographers, or even demonstrators, to provide a plausible reason for being in the area.

Mobile surveillance usually entails observing and following key vehicles or human targets, although it can be conducted against non-mobile facilities (i.e., drive-by site observations).

More sophisticated surveillance is likely to be accomplished over a long period of time. This type of surveillance tends to evade detection and improve the quality of gathered information. Some terrorists perform surveillance of a target or target area over a period of months or even years. Public gathering areas provide convenient venues for surveillance activities.

Terrorists are also known to use advanced technology, such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices and global positioning systems (GPSs). It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance refers to information gathering, legal and illegal, by terrorists using off-site computers or other technology. The type of data gathered may include critical asset information, security procedures, or system passwords. Terrorists may use an array of technical means to intercept e-mail, radio, cell phone, and pager traffic.

In addition, terrorists may launch an electronic attack that could affect databases, networks, software, or control systems. Such attacks may be intended to cause direct damage (e.g., delete data records), modify the response of a system (e.g., open a process valve when a command would normally close a process valve), or steal information (e.g., credit card data). An electronic attack could also serve as a preemptive strike intended to create confusion while simultaneously launching a physical attack.

The surveillance indicators listed in following chart are examples of unusual activities that should be noted, with consideration given to the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other experience.

SURVEILLANCE INDICATORS (at or near a postal or shipping facility)
These indicators suggest information gathering activities may be under way.

Indicators about People (Observed or Reported)

- Frequent or unusual use or possession of video, camera, recording. or observation equipment
- Possession of installation photos or diagrams with highlighted areas or notes regarding infrastructure
- Possession or observed use of night-vision devices
- Persons parking, standing, or loitering in the same area over multiple days with no reasonable explanation
- Persons questioning staff off-site about facility practices, or an increase in inquiries about critical features
- Persons not associated with the facility showing an increased interest in the surrounding area
- Staff willfully associating with suspicious individuals
- Computer hackers attempting to access sites for personal information, maps, or other targeting data.
- An employee whose working behavior undergoes an unusual change or who begins to work irregular hours
- Persons showing an unusual interest in receipts or deliveries, especially of HAZMAT
- Unfamiliar cleaning/contract crews with passable credentials; attempts to access unauthorized areas
- Arrest of unknown persons by local police (may be more important if facility is located in a rural area)

Indicators about Activities (Observed or Reported)

- Downloading of materials (e.g., maps, schematics) useful in surveillance or attack-planning activities
- Repeated attempts to access protected computer information from the same organization or country
- Successful penetration and access of protected computer systems with critical information
- Attempts to obtain information about the facility (e.g., building blueprints from public sources)
- Aircraft flyover or boat encroachment into restricted areas
- An abandoned or illegally parked vehicle in the area of a key facility or employee gathering area
- Increased interest in outside components (e.g., electrical equipment) that is less protected or not protected at all
- Unexplained power outages that may be intentionally testing emergency response or recovery plans
- An increase in threats that may be intentionally testing emergency response or recovery plans
- A noted pattern of false alarms requiring a response by law enforcement or emergency services
- Unexplained increase in incidences in which security and safety devices are left unsecured or in unsafe conditions
- Theft of ID cards or uniforms, or unauthorized persons in possession of such items
- An increase in violations of standard operating procedures by security guards at key posts
- Sudden loss or theft of guard force communications equipment, keys, or access cards
- Recent damage to fences or gates or to perimeter lighting, cameras, or sensor devices
- Indications or observations of persons collecting or searching through trash
- Displaced or misaligned manhole covers or open service access doors near critical sites
- Unusual maintenance activities near the facility (e.g., out-of-season road repairs)

Transactional and Behavioral Indicators

Transactional and behavioral indicators are suspicious purchases or sales of materials that could be used in an act of terrorism or criminal activity. These may involve vendors or suppliers, staff, or persons with knowledge of such incidents in the vicinity of a postal or shipping facility.

Transactional indicators are unusual, atypical, or incomplete procedures or events associated with an inquiry about equipment and materials or an attempted purchase or sale of these items.

Behavioral indicators are actions or inactions on the part of a customer, vendor, supplier, or staff member that are inconsistent with normal behavioral patterns.

TRANSACTIONAL AND BEHAVIORAL INDICATORS (at or near a postal or shipping facility)
These are indicators of atypical procedures or actions by customers, vendors, or suppliers.

Transactional Indicators

- Approach from a previously unknown vendor, supplier, or customer whose identity is not clear
- Transaction involving an intermediary agent or consignee that is atypical in light of usual business
- An agent or customer associated with a military-related business, such as foreign armed forces
- Unusual request concerning the shipment or labeling of goods
- Packaging that is inconsistent with the shipping mode
- Unusually favorable payment terms (e.g., too good to be true) when compared with the prevailing market
- Request for excessive confidentiality regarding a purchase, sale, or delivery
- Orders for excessive quantities of personal safety/security devices that are outside normal needs
- Requests for normally unnecessary devices/supplies coupled with an unconvincing explanation for the need
- Vendor, supplier, or customer that uses a different name for different transactions
- Equipment, chemicals, or materials stolen or 'lost' during shipment or shortly after delivery
- Theft or loss of large amounts of cash

Behavioral Indicators

- Intimidating, harassing, bullying, belligerent, or other inappropriate, aberrant, bizarre, or aggressive behavior by an employee
- Excessive anger and/or bitterness expressed by employee regarding a personnel action by employer
- Delivery that is unexpected, out of the norm, without explanation, or associated with suspicious paperwork
- Excessive request for site access by delivery person or delivery vehicle
- Evasive responses or reluctance to give sufficient explanations for use or purpose of materials
- Reluctance to provide location data, such as business address, delivery point, or shipping origin
- Reluctance to provide clear answers to routine commercial or technical questions
- Reason given for purchase or sale does not match the usual business or technological level
- No offer of, request for, or refusal of technical assistance when such action is generally standard
- Equipment or material is said to be for a use that is inconsistent with its design or normal purpose
- Theft of equipment or material that has no practical use outside a legitimate business practice
- Apparent lack of familiarity with the 'business' or its nomenclature or a lack of knowledge of how transactions of this type are handled
- Inconsistency of information that is provided (e.g., phone number or address) with what is known

Weapons, Explosives, and Chemical, Biological, or Radiological Indicators

Suspicious activities involving threats from weapons, explosives, or CBR materials may also warrant reactions such as an investigation, a communication, or an emergency response.

Weapons

Indicators of possible use of weapons against a postal or shipping facility include the purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out an intended action. Items of interest include not only guns, automatic weapons, and rifles, but also ammunition and equipment, such as night-vision goggles and body armor, and relevant training exercises and classes. The following chart expands on this description of weapons indicators.

WEAPONS INDICATORS (at or near a postal or shipping facility)
These indicators provide insights into the use or planned use of weapons.

Indicators about Activities (Observed or Reported)

- Reports of automatic or unusual weapons firing
- People wearing clothing that is not consistent with the local weather
- Training scenarios carried out by paramilitary groups or other organizations advocating violence.
- Theft, transactions, or seizures of large numbers of
  - Automatic or semiautomatic weapons
  - Ammunition capable of being used in military weapons or modified weapons
  - Equipment used to modify weapons (e.g., silencers)
  - Large-caliber sniper weapons
  - Night-vision equipment or
  - Body armor, especially in combination with other indicators

Explosives

Indicators of explosive or incendiary materials and devices that could be used by terrorists include the production, purchase, theft, testing, or storage of any kind of these materials. The next chart describes indicators of those activities in addition to indicators of VBIEDs.

VBIEDs are dangerous because they are inherently mobile and inconspicuous by design, yet they can conceal large amounts of explosives and therefore do not always have to penetrate perimeter security defenses to be effective. The VBIED indicators listed in this next chart are taken from lessons learned in Iraq.

EXPLOSIVE AND INCENDIARY INDICATORS (at or near a postal or shipping facility)

These indicators provide insight into the presence of explosives or explosive devices.

Indicators about People (Observed or Reported)

- Persons stopped or observed with unexplained amounts of explosives
- Unidentified persons making inappropriate inquiries regarding explosives or their construction
- Treated or untreated chemical burns or missing hands and/or fingers

Indicators about Activities (Observed or Reported)

- Thefts, transactions, or seizures of large amounts of smokeless powder, blasting caps, high-velocity explosives, sensitive chemicals, combinations of ingredients for explosives (e.g., fuel oil, high-nitrate fertilizer), containers (e.g., propane bottles), or vehicles (e.g., trucks) that result or could result in IEDs, especially in combination with other indicators
- Modification of a sedan, van, delivery truck, water or concrete truck, or semi-trailer to carry explosives
- Traces of explosive residue on visitor or business vehicles during explosive detection checks
- Unexpected or unfamiliar delivery trucks or deliveries
- Delivery of chemicals or suspicious materials to rental or self-storage units or out-buildings
- Vehicles containing unusual or suspicious parcels or materials
- Suspicious packages (e.g., unexpected deliveries, return-address errors, or excessive postage).
- Unattended packages, briefcases, or other containers
- Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in storage out-buildings, nearby homes, apartments, hotel rooms, or self-storage units
- Reports of explosions, particularly in rural or wooded areas

Indicators about VBIEDs (Observed or Reported)

- Noticeable sagging of the vehicle on its springs, caused by the heavy weight of explosives (Ordinarily, explosives are placed toward the rear of the vehicle, causing it to ride lower in the rear. However, commercial trucks carrying VBIEDs are designed to carry the weight and may not appear to sag.)
- Darkened or covered windows to conceal either the vehicle's contents or the driver's actions
- Unusual vehicle items, such as gas cylinders, wires, leaflets, large bags or boxes, and extra batteries
- Indications of a triggering device (e.g., a switch, radio transmitter, timer, wires, or ropes passing from the front seat to the rear of the vehicle) visible near the driver, under the seat, or within arm's reach
- Additional fuel tanks, used to hide explosives or to provide additional gasoline to fuel an explosion
- Holes made in the vehicle body to hide explosives and then crudely covered
- Evidence that an interior door panel has been removed to hide explosives
- Recent painting of the vehicle to cover body alterations
- Any disturbance to the undercoating or dirt on the bottom of a vehicle
- Additional antennas on the vehicle for radio-controlled devices
- Unusual smells, such as a burning time fuse, gasoline, or fertilizer
- Presence of powder or prills (e.g., small rounded granular material) left when explosives are loaded
- Presence of a vehicle in an area where it should not be, perhaps parked illegally or at an unusual time

Chemical, Biological, and Radioactive (CBR) Materials

Chemical agents, biological species, and hazardous radioactive materials could also be threats to infrastructures, populations, and agriculture. Indicators of the possible presence of those materials are related to production, purchase, theft, testing, or storage and are described in the next chart.

CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL (CBR) INDICATORS (at or near a postal or shipping facility)

These indicators provide insights into the presence of CBR materials.

Equipment Configuration Indicators (Observed or Reported)

- Thefts, transactions, or seizures of sophisticated personal protective equipment (PPE), such as 'A' level Tyvek, self-contained breathing apparatus (SCBA), or sophisticated filtering, air-scrubbing, or containment equipment
- An area under strict security control that is inconsistent or out of character with normal operations
- Suspicious packages (e.g., unexpected deliveries, return-address errors, or excessive postage)
- Unattended packages, briefcases, or other containers
- Unexpected or unfamiliar delivery trucks or deliveries
- Vehicles containing unusual or suspicious parcels or materials

Chemical Agent Indicators (Observed or Reported)

- Thefts, transactions, or seizures of explosives or restricted or sensitive chemicals
- Inappropriate inquiries regarding chemical usage, transactions, storage, or transportation
- Delivery of chemicals or suspicious materials to rental or self-storage units or out-buildings
- Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in storage out-buildings, nearby homes, apartments, hotel rooms, or self-storage units
- Treated or untreated chemical burns or missing hands and/or fingers
- Unusual containers, powders, droplets, or mist clouds near HVAC equipment or air-intake systems

Biological Agent Indicators (Observed or Reported)

- Thefts, transactions, or seizures of large quantities of baby formula (a medium used for growing biological agents), live and/or lethal amounts of agents/toxins/diseases (from medical supply companies or labs), or dispensing systems, such as agricultural sprayers or crop-dusting aircraft or foggers (especially to nonagricultural users)
- Inappropriate inquiries regarding biological agent usage, storage, or transportation
- A break-in at or tampering with a nearby water treatment facility or food processing/warehouse facility
- Multiple, unexplained human or animal illnesses (or deaths), especially illnesses not native to area
- Unusual containers, powders, droplets, or mist clouds near HVAC equipment or air-intake systems

Radioactive Material Indicators (Observed or Reported)

- Thefts, transactions, or seizures of radioactive materials from medical supply companies or labs
- Inappropriate inquiries regarding radiological material usage, storage, or transportation
- A break-in at or tampering with facilities that store radioactive materials or radioactive wastes
- Multiple, unexplained human or animal radiation burns or radiation sickness or radiation deaths

COMMON VULNERABILITIES

Key Vulnerabilities

The following is a list of the key common vulnerabilities associated with postal and shipping facilities. In addition to these vulnerabilities that are specific to postal and shipping facilities, a number of general vulnerabilities that exist at many different infrastructure segments can be identified. These are listed in a later section.

- *Anonymous mail.* Mail can be introduced into the postal and shipping networks anonymously, and it is unmonitored at hundreds of thousands of collection boxes and millions of delivery points. While curtailing such collections would reduce the threat of anonymous hazardous mailings, USPS officials have determined that the resulting inconvenience to customers would be unacceptable.

- *Ease of introducing biological agents.* Anonymous mail is particularly susceptible to being used in biohazard attacks. The small quantities of agent required to mount an attack fit easily into small containers, such as envelopes. The fact that many of these agents have a powdery form means that no bulky hardware is needed for dispersal.

- *Ease of introducing chemical agents and explosives.* Larger packages may be susceptible to attacks using chemicals or explosives. The USPS has instituted procedures to curtail anonymous mailing of packages weighing 1 pound (lb) or more, but smaller packages containing dangerous quantities of chemical agents or explosives may still be mailed anonymously.

- *Large number of points of access to the public.* Publicly accessible mailboxes are susceptible to direct attack from placement, rather than mailing, of explosives.

- *Ease of mail theft.* Mail is susceptible to theft from delivery points, collection boxes, post offices, and P&DCs. Stolen mail containing personal identifying information, account numbers, and blank checks can be used in organized identity theft schemes.

- *Large workforce.* The large number of employees involved in handling the mail makes it difficult to perform complete background checks on all USPS, FedEx, UPS, DHL, and other companies' employees. Some instances of employee malfeasance have been reported.

Previous Incidents

The following is a list of incidents that have involved the Postal and Shipping sector that illustrate some of the vulnerabilities.

Biohazard Attacks

- In October 2001, five anonymous letters containing anthrax were sent, one to each of five recipients: the *New York Post*, NBC News anchor Tom Brokaw, a tabloid newspaper in Florida, and the offices of Senators Tom Daschle and Patrick Leahy. The letters resulted in the deaths of five people, including two postal workers at the Brentwood P&DC in Washington, D.C. That center and the center at Trenton, New Jersey, were found to be widely contaminated with anthrax spores. Several more USPS employees were hospitalized with confirmed or suspected symptoms, and thousands were tested and/or given precautionary antibiotic treatments. Both centers were closed pending completion of a lengthy process of testing, decontamination with chlorine dioxide, and renovation. The USPS subsequently instituted a procedure, which will continue for the foreseeable future, to irradiate mail destined for government agencies in the zip code ranges 202–205, except for mail from “known senders” (i.e., corporate accounts or express/priority mail with postage meter strips or permit indication instead of postage stamps) (USPS 2002a).

- In the 15 days following the October 2001 anthrax attacks, a total of 353 postal facilities were evacuated for various amounts of time as a result of 8,674 hoaxes, threats, and suspicious mailing incidents, averaging 578 per day. Postal inspectors had 20 individuals arrested for anthrax-related hoaxes, including one USPS employee (USPS 2001a).

- In October 2003, a suspicious envelope at the Greenville, South Carolina, Airport Mail Facility was found to contain a small sealed container of ricin with a threatening note. No adverse health effects were reported, and environmental samples were all negative for the presence of ricin in the building (USPS 2003).

- In February 2004, tests of a powdery substance found in Senator Bill Frist’s office were positive for ricin. Three Senate office buildings, the Capitol, and the USPS V Street facility in Washington, D.C., were closed for several days for testing (USPS 2004).

Mailbox/Mail Facility Bombs

- Over a five-day period in May 2002, a Wisconsin college student placed 18 pipe bombs in rural mailboxes over a five-state area. The bombs did not move through the mail but were placed directly into customers’ mailboxes.

They resulted in non-life-threatening injuries to four USPS employees and two customers. Mail delivery in the five states was affected minimally, with customers being asked to keep their mailbox doors open to ensure safety. During the height of the scare, the USPS had 150 postal inspectors working on the case (USPS 2002b).

- In May 2003, agents with the Bureau of Alcohol, Tobacco and Firearms (ATF) arrested a man in front of a UPS store in Walnut Creek, California, after they discovered three bombs in a package that belonged to him (MapReport.com 2003).

- In March 2004, The Dona County Ana (New Mexico) bomb squad searched a suspicious package left in a FedEx mailing bin outside the downtown post office. The package was a coffee can with a note attached reading “death to those who open” (Scanna MSC 2004).

- In May 2004, police closed a two-block stretch in Tacoma, Washington, and called in the bomb squad after a postal worker found a suspicious package in a mail drop box. After being blown apart by the bomb squad, the package — addressed to President Bush and Vice President Cheney — was found to contain rocks (*TheNewsTribune.com* 2004).

- Also in May 2004, three homemade pop bottle bombs were found in mailboxes in Palatine, Illinois. One had detonated (NBC5.com 2004).

- In June 2004, five acid bombs, placed outside four Coral Springs, Florida, homes, damaged three curbside mailboxes and caused mail service in the area to be temporarily suspended. Six other bombs had been found in Coral Springs in the preceding week, and three other mailboxes had been set on fire (*Sun Sentinel* 2004).

- In March 2006, at a trial in London, a prosecution witness testified that a terror cell planned to smuggle bomb ingredients into the United Kingdom by using shampoo and shaving cream bottles and bags of dried fruit. They would be sent to the UK in a parcel via Federal Express (BBC News 2006).

- In May 2007, a suspicious package was found at the USPS San Francisco Bulk Mail Center in Richmond, California. The package contained eight inoperative hand grenades, according to Richmond police (CBS5.com 2007).

Mail Theft/Identity Theft

- In April 2004, mail traps were found in Indiana. Bags of undelivered mail found in a motel trash bin led to the discovery of metal traps painted ‘postal blue’ and apparently mass-manufactured to fit perfectly inside street-corner postal collection boxes. Three people were arrested in an alleged identity theft scheme that involved more than 180 pieces of stolen mail. Checks and account data were allegedly used to manufacture counterfeit drivers' licenses and blank checks (AJC.com 2004).

- In May 2004, a postal clerk in Stamford, Connecticut, was charged with using information obtained at work to obtain credit cards in other people's names. Police found personal identification information for several victims in the clerk's apartment, plus credit card numbers, postal routing codes, phone numbers, proof of residency, and merchandise order information (Campanelli 2004a).

- Also in May 2004, 10,000 pieces of stolen mail were found in bags alongside a roadway in Pennsylvania. Postal inspectors traced the mail to a former temporary employee in the Wilkes-Barre mail processing center (Gulla 2004).

- In June 2004, three men in Delray Beach, Florida, were arrested while rummaging through a post office trash bin. The men had slipped onto the property through a hole in the fence. Inspectors suspected the men were picking out undeliverable mail that had been discarded, removing credit card information and blank checks issued to credit card customers, and using the materials to set up false identities or make unauthorized purchases (Lade 2004).

Disgruntled Employees

- On December 28, 2005, a part-time UPS employee, who had a bipolar disorder, drove to the UPS sorting facility in Livonia, Michigan, at about 3:00 a.m. He had previously been at his job but was sent home because of a lack of work. After lying in wait, he shot and killed a coworker who was leaving the center. The incident was part of a three-city rampage in which he also killed relatives and himself. While his motive was unknown, neighbors blamed mental illness and family and work tensions (Kurth and Lee 2005).

- On January 30, 2006, a former USPS employee opened fire inside the Santa Barbara P&DC in Goleta, California, killing six workers before committing suicide. The woman, who had worked at the Goleta facility, had been granted early retirement on a medical disability in June 2003 because of psychological problems, the USPS said (CBS News.com 2006).

Consequences of an Event

The consequences of a successful attack on the Postal and Shipping sector can be wide-ranging. Consequences include those that follow.

Public Health and Safety Consequences

Actual biohazard attacks have resulted in deaths, illnesses requiring hospitalization, and the need to test or give precautionary treatment to thousands of individuals. Attacks using biohazards, chemicals, or explosives would conceivably have consequences of a similar nature.

Economic Consequences

The USPS is the linchpin of a $900 billion mailing industry that employs 9 million Americans in fields as diverse as direct mailing, printing, catalog production, and paper manufacturing. In 2004, industries that relied on the USPS accounted for nearly 9% of the Gross Domestic Product (U.S. Senate Committee on Homeland Security and Governmental Affairs 2004).

Disruption in mail service has had direct and indirect economic consequences, not just to the USPS, UPS, FedEx, and DHL, but to other segments of the mailing industry and to their customers. USPS mail volume from September 5 through October 8, 2001, was an estimated 6.6% lower than in the same period a year earlier. First-class mail volume was 2% lower, priority mail volume was 15% lower, and standard mail volume was 11% lower (USPS 2001b).

Direct costs to the USPS related to the September 11 attacks and subsequent anthrax attacks were estimated to be $3 billion or more, including damage to facilities and equipment, medical testing and emergency treatment of employees exposed to anthrax, protective equipment for employees, environmental testing, communication and education of employees and customers, purchase of sanitizing equipment, disruption of operations, and implementation of new security procedures. Moreover, declines in mail volume and revenue were estimated to affect the USPS's bottom line by as much as $2 billion in the fiscal year (USPS 2001c).

A study by the Foundation for Paper-based Communication found that if mail volume were to drop 10%, 750,000 postal-related jobs would be at risk, including jobs in several segments of the mailing industry: mailing services; manufacturing; professional, scientific, and technical services; USPS workers; information; transportation and warehousing; and retail trade. According to the study, if mail volume dropped 20% (the foundation's worst-case scenario), 1.5 million jobs in the mailing industry would be at risk (Campanelli 2004b).

Social and Institutional Consequences

Threats to the USPS mission of universal mail service could force both residential and commercial customers to change their daily behaviors and business practices. Anthrax and ricin attacks on the Capitol have degraded mail communications to Washington, D.C. Letters and packages addressed to selected Washington zip codes are collected each day and shipped by truck to an irradiation plant for treatment. The irradiation process destroys anthrax, but it can also damage ink and paper and ruin items like computer disks. Because irradiation does not work against some biohazards, such as ricin, the mail still has to be sent to inspection facilities, where workers open and inspect each piece of mail for biological and chemical agents. The mail is also screened for explosives before being resealed and delivered. In the worst cases, delivery times have sometimes extended to months. Customers have sometimes been forced to choose other delivery methods or other means of communication to ensure timely delivery of their messages (NJ.com undated).

STANDARDS AND REGULATIONS

Chapter 1, Title 39, *Code of Federal Regulations* is the primary legal instrument establishing and regulating the USPS. It also includes provisions regulating private carriers (GPO/NARA undated).

Title 49, Subchapter C, Parts 171–180, *Code of Federal Regulations*, governs the packaging and shipping of dangerous and hazardous items. It applies to the USPS and private carriers (GPO/NARA 2007a).

Title 41, *Code of Federal Regulations,* "Public Contracts and Property Management," Parts 102–192 prescribes policy and requirements related to incoming, internal, and outgoing mail in Federal agencies from all carriers (GPO/NARA 2007b).

The USPS is an independent entity of the executive branch of the federal government. Until 1970, it was a cabinet department of the executive branch. The Postal Reorganization Act of 1970 set up the current statutory framework.

The USPS is overseen by a Board of Governors, comparable to the board of directors of a publicly held corporation. Nine governors are appointed by the President of the United States, with the advice and consent of the U.S. Senate. The governors select the Postmaster General. The governors and the Postmaster General select the Deputy Postmaster General. The appointed governors, plus the Postmaster General and the Deputy Postmaster General, make up the Board of Governors.

The USPS is required by the Government Performance and Results Act of 1993 to provide a variety of reports to Congress. These reports include an annual *Comprehensive Statement on Postal Operations,* an *Annual Performance Plan,* and a *Five-Year Strategic Plan*.

The General Accountability Office and the congressionally created Office of the Inspector General investigate and evaluate USPS programs, operations, and management (GAO 2006). The Postal Rate Commission is an independent establishment of the executive branch of the federal government, created by the Postal Reorganization Act of 1970 for the primary purpose of reviewing postal rate requests and mail classification changes. Its five members are appointed by the President of the United States and confirmed by the U.S. Senate.

Safety and Security

In 2002, at the direction of Congress, the USPS developed an emergency preparedness plan to (1) protect its employees and customers from exposure to infectious biohazard agents, (2) screen and sanitize the mail, (3) decontaminate two mail processing plants that handled anthrax-laden letters, and (4) repair or replace postal facilities affected by the September 11, 2001, terrorist attacks on New York City.

The USPS and the General Services Administration have issued security guidelines for mail centers in federal and other facilities to deal with biological threats, mail bombs, and theft. These facilities, although they are not managed by the USPS, are still significant collection and distribution points for USPS-handled mail and packages.

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 are designed to meet one or more of the following objectives:

Devalue Lower the value of a facility to terrorists; that is, make the facility less interesting as a target.

Detect Spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.

Deter Make the facility more difficult to attack successfully.

Defend Respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack.

Many different protective measures are available for deployment at a facility and in the areas surrounding a facility (buffer zones). Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or a specific threat stream. In addition, some may be tactical in nature, while others may address long-term strategic needs (e.g., redundancy).

Some protective measures are designed to be implemented on a permanent basis to serve as routine protection for a facility. Such measures are sometimes referred to as ‘baseline countermeasures.’ Others are either implemented or increased in their application only during times of heightened alert.

The implementation of a protective measure at any time involves the commitment of resources in the form of people, equipment, materials, time, and money. Facility owners, local law enforcement personnel, emergency responders, and state and local government agencies need to coordinate and cooperate in determining what measures should be implemented, how extensive they should be, and how long they should be kept in force in order to maximize security while staying within the bounds of available resources.

To assist in the decision process, the U.S. Department of Homeland Security (DHS) has developed the color-coded Homeland Security Advisory System (HSAS) to communicate with public safety officials and the public at large so that protective measures can be implemented or expanded to reduce the likelihood or impact of an attack. Table 2 shows the HSAS alert levels.

When the available intelligence allows, HSAS alerts are supplemented by information on the threat stream(s) most likely to be used by terrorists. This information may or may not be very specific, may or may not identify geographic areas of concern, and may or may not offer a time period when attacks might be expected. This level of uncertainty is inherent in dealing with terrorist threats and must be factored into decisions on committing resources to implement protective measures.

Table 2 DHS Advisory System Alert Levels

Alert Level		Description
Red	SEVERE	Severe risk of terrorist attack
Orange	HIGH	High risk of terrorist attack
Yellow	ELEVATED	Significant risk of terrorist attack
Blue	GUARDED	General risk of terrorist attack
Green	LOW	Low risk of terrorist attack

The measures shown on the following charts are designed to provide information and assistance to facility owners, site managers, local law enforcement personnel, and state and local homeland security agencies in making decisions on protective measures. These suggested measures are collated from infrastructure-specific guidance and from experience in a number of localities across the country. The following should be noted regarding the suggested protective measures:

- These measures are intended as a guide; they are not a requirement under any regulation or legislation. In addition, because of the wide variety in the types of facilities, not all suggested measures will be applicable.

- These suggestions are based on practices employed by facilities across the nation. The ability to implement them at any specific facility will vary.

- These suggestions should not be viewed as a complete source of information on protecting facilities. Facility managers and local security personnel should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

The protective measures are grouped into the following categories:

- Planning and Preparedness
- Personnel
- Access Control
- Barriers
- Communication and Notification
- Monitoring, Surveillance, Inspection
- Cyber Security
- Infrastructure Interdependencies
- Incident Response

PLANNING AND PREPAREDNESS

These measures relate to emergency plans and preparations.

- Designate an experienced employee as security director to lead all security-related activities.
- Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis. On the basis of these analyses, develop a comprehensive security plan and emergency response plan for each facility, including procedures to cover all potential and multiple emergency situations; identify security responsibilities and a chain of command in an incident; develop procedures to cover routine security activities by all employees; and develop procedures for dealing with people with special needs.
- Coordinate plans with appropriate agencies and support them with mutual aid agreements.
- Involve employees at several levels in security planning. Consider third-party evaluation of plans.
- Develop business recovery/continuity plans to be implemented in the aftermath of an incident.
- Test security, emergency, and continuity plans regularly with drills and tabletop exercises.
- Establish liaisons and regular communication with local law enforcement personnel and emergency responders, state and federal law enforcement and terrorism agencies, public health organizations, and industry organizations to enhance information exchange, clarify emergency responses, track threat conditions, and support investigations.
- Consider establishing an emergency operations center to coordinate resources during an incident.
- Keep and protect copies of the security and emergency response plans in redundant locations.
- Restrict access to sensitive facility data and information (e.g., building plans; life safety systems).
- Develop policies and procedures for dealing with the media and the general public in the event of an incident to advise them of the situation and to defuse rumors and panic.
- Establish procedures for facility evacuation and for shelter-in-place situations. For shelter-in-place situations, ensure that there is a shelter that is adequately stocked to accommodate the number of people who might need to use it.
- Develop procedures for shutting down a facility in the event the threat is deemed too serious to continue operations.

During Periods of High Alert (HSAS ORANGE):

- Review and implement actions specified in the security and emergency response plans. Adjust as necessary to deal with specific threat information.
- Activate facility emergency operations center as appropriate.

During Periods of Severe Alert (HSAS RED):

- Review available threat information and determine if the facility should be closed or should operate with reduced hours and/or a reduced workforce and/or with reduced activities.

PERSONNEL

These measures relate to personnel.

Employees

- Conduct background checks on all employees. Conduct more detailed checks on those who will have access to critical assets. Develop a list of disqualifying factors.
- Incorporate security awareness and appropriate response procedures for security situations into employee training and refresher programs. Include standard operating procedures (SOPs) in the security and emergency response plans; maintain alertness to and recognize situations that may pose a security threat; develop contact and notification protocols for suspicious situations and emergencies; maintain caution about providing facility information to outsiders; and develop procedures to provide for the safety of employees during an incident.
- Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., irregular work hours, attempts to access restricted areas).
- Determine the need for PPE (e.g., breathing apparatus) for employees.
- Review the personnel files of recently terminated staff to determine if they pose a security risk.
- Watch for warning signs and be wary of circumstances that could precede a violent outburst (disciplinary action, conflict, unsatisfactory review, termination, personal crisis, impending deadline, etc.).

Security Force

- Maintain an adequately sized, equipped, and trained security force.
- Coordinate security force operations with local law enforcement and other agencies.
- Develop a security force patrol schedule that includes both regular and random stops and timing.

Contractors, Vendors, Temporary Employees, Visitors, Patrons

- Provide security information and training to all nonemployees visiting the facility. Advise them to be alert to suspicious activity or items and on how to report such incidents.
- Require contractors, vendors, and temporary employment agencies to vouch for the background and security of their personnel who will visit the facility.

During Periods of High Alert (HSAS ORANGE):

- Provide additional reminders to employees and visitors about the security situation.
- Increase security force presence and extend patrols to a wider perimeter.
- Consider augmenting security with special units (e.g., armed guards, K-9 units).
- Activate the emergency operations center.
- Have employees, especially those working in remote or isolated areas, work in pairs.
- Have employees vary their routines to avoid predictability.
- Limit noncritical travel and business activity outside the facility.

During Periods of Severe Alert (HSAS RED):

- Increase the security force presence to the maximum level sustainable.
- Request support from law enforcement personnel and, if appropriate, from the National Guard.

ACCESS CONTROL

These measures relate to controlling critical facility access.

General Measures

- Define the facility perimeter and areas within the facility that require access control for pedestrians and vehicles. Identify especially critical areas (e.g., control rooms, fuel or chemical storage areas, shipping docks, utility rooms) that require special access controls (e.g., logging of entry/exit).
- Train security staff to identify prohibited items (e.g., firearms, explosives, illegal drugs, cameras). Train personnel to recognize suspicious mail, packages, or deliveries.
- Enforce access control measures (e.g., locking of buildings not in use). Allow no exceptions. Implement rigorous key control procedures. Secure master keys. Secure all tools that could be used to force entry into a critical area (e.g., bolt cutters, cutting torches).

Employees

- Issue photo ID badges to all employees. Require that badges be displayed at all times and verified to gain access to all nonpublic areas of facilities. Utilize an electronic access tracking system to log entry and exit from critical facilities. Collect employee badges and keys when employment is terminated.

Contractors, Vendors, Temporary Employees

- Issue special ID badges to known and expected contractors, crews, vendors, and temporary employees. Require that badges be displayed at all times and verified to gain access to all nonpublic areas of facilities. Escort nonemployees in critical areas. Collect all badges when visits are complete.

Visitors, Patrons, Customers

- If possible, screen visitor requests for special tours and demonstrations of critical areas with local law enforcement personnel. Require that badges be displayed and verified to gain access to the facility. Collect all badges when visits are complete.
- Separate employees from the public (e.g., bullet-proof barriers, other physical barriers).

Vehicles

- Issue employee parking permits for designated areas. Lock facility vehicles when not in use.
- Keep vehicles away from critical areas and areas where crowds congregate. Deny access to suspicious (e.g., heavily overloaded) vehicles. Approach illegally parked vehicles and require moving or towing.

During Periods of High Alert (HSAS ORANGE):

- Reduce the number of site access points and increase the security force presence.
- Delay nonessential contractor work.
- Restrict parking to areas away from critical assets.
- Accept deliveries only during daytime hours and away from critical facilities.

During Periods of Severe Alert (HSAS RED):

- Consider closing facility until threat has been reduced.
- Halt contractor work, special tours, and nonessential mail, shipments, and deliveries.
- Freeze all movement of vehicles on-site except for security and emergency response.

BARRIERS

These measures relate to physical barriers and barricades.

Facility Site Perimeter Barriers

- Evaluate the need for perimeter barriers (e.g., fences, walls) around critical areas.
- Maintain a clear area at perimeter barriers to enable continuous monitoring and to inhibit concealment of people or packages. Inspect perimeter barrier regularly.
- Install alarms and intrusion detection equipment at unstaffed perimeter barriers.

Building Barriers

- Establish a clear zone adjacent to critical buildings. Keep zone free of vegetation and other obstructions to allow for continuous monitoring and to inhibit concealment of people or packages.
- If appropriate, install building perimeter barriers (e.g., fences, bollards, large flower pots) around critical buildings in addition to installing site perimeter barriers.
- If appropriate, install interior building barriers (e.g., internal locked doors) to protect sensitive or critical areas or corridors within a building.
- Ensure that exterior doors have hinge pins that cannot be removed from the outside and that there are no gaps between the door and jamb that would allow for the door to be compromised.
- Install barriers at HVAC systems (e.g., screens on intakes, filters) to prevent the introduction of CBR agents into the building. Train staff in emergency shut-off procedures for HVAC systems.

Vehicle Barriers

- Evaluate vehicle traffic patterns in the facility. Design and implement traffic control strategies and barriers (e.g., road alignment, serpentine traffic routing, swing gates, speed bumps) to control vehicle speed and approaches to critical assets and places where crowds congregate.
- Install bollards on pedestrian walkways to keep vehicles off them.

During Periods of High Alert (HSAS ORANGE):

- Deploy temporary barriers (e.g., Jersey barriers, heavy vehicles and equipment, empty containers) to increase the standoff distances from critical areas.
- Deploy temporary barriers to slow the flow of traffic into the facility and within the facility.
- Relocate critical items (e.g., specialized equipment, important records) to areas of the facility with higher physical security.

During Periods of Severe Alert (HSAS RED):

- Increase the number and security of barriers to the maximum extent possible consistent with the operating level of the facility.

COMMUNICATION AND NOTIFICATION

These measures relate to communications.

Communications Equipment

- Install systems that provide communication with all people at the facility, including employees, the security force, emergency response teams, and visitors. Provide redundant communication channels and backup sources of power for these systems. Test systems regularly.
- Install systems that provide communication channels with local law enforcement personnel and emergency responders. Test the systems regularly.
- Provide communication capability for employees who are at remote locations.
- Provide communication security (e.g., encryption, multiple frequencies) that will prevent unauthorized interception of information. Train employees not to discuss sensitive information over communication channels that are not secure (e.g., cell phones).
- Provide the ability to record incoming telephone calls to identify potential threats.

Communication Protocols

- Develop a notification protocol that outlines who should be contacted in emergencies. Regularly test notification protocol through drills and exercises.
- Provide a simple and straightforward means for people to communicate the presence of a potential threat or an emergency (e.g., a hotline number, internal 9-1-1 capability).
- Develop a process to update on- and off-duty employees about the current security situation.
- Establish call-in procedures for employees who work in remote or isolated locations.
- Develop a process for communicating with the public and the media regarding security issues. Provide adequate information to quell rumors and dispel unnecessary alarm. Take steps to restrict the release of information that might compromise the security posture of the facility.

Information Sharing

- Monitor industry and government information on threats, incidents, and response procedures. As appropriate, share information on the facility's experiences.

During Periods of High Alert (HSAS ORANGE):

- Increase frequency of communications with local law enforcement.
- Increase communication with employees and visitors about the security situation.
- Increase the frequency of reporting from employees working in remote areas.

During Periods of Severe Alert (HSAS RED):

- Maintain communication with local law enforcement personnel as continuously as is sustainable.
- Provide employees and visitors with as much information as possible as frequently as possible to keep them apprised of the security situation.
- Activate backup equipment so it is ready to use in the event of an incident.

MONITORING, SURVEILLANCE, INSPECTION

These measures relate to procedures and equipment used to monitor the movements of people, vehicles, and materials.

Equipment

- Provide visual surveillance capability for critical areas. Train staff to watch for unusual activities.
- Install video surveillance equipment (e.g., closed-circuit television [CCTV]). Provide coverage for critical areas, roadways, parking lots, and entrances. Install intrusion, motion, and other detectors (e.g., fire, smoke) as appropriate. Maximize the recording time. Establish procedures to secure video and other incident data for forensic purposes. Test regularly.
- If appropriate, install GPS equipment on facility vehicles to monitor their location. Train employees monitoring the GPS feeds to recognize potential security-related events and how to respond.

Buildings and Facility Assets

- Regularly inspect the site perimeter, buildings, equipment, and critical areas for signs of security issues. Implement random and scheduled inspections. Include assets not used frequently.

People

- Monitor people entering and leaving the facility. Train monitors to detect suspicious behavior. Monitor the activities of contractors, delivery personnel, and vendors for unusual behavior.
- Provide inspections of people entering and leaving critical areas.

Vehicles

- Monitor vehicles approaching the facility for signs of threatening behavior.

Deliveries and Mail

- Supervise the unloading of materials and equipment. Verify the shipper and delivery details. Conduct more thorough inspections of deliveries involving HAZMAT or sensitive materials.
- Inspect mail for unusual signs. Provide PPE to all staff.
- Advise key employees to check deliveries and mail at home for suspicious material.

Materials

- Maintain a thorough inventory and accounting of all sensitive items and their storage and use.

During Periods of High Alert (HSAS ORANGE):

- Increase monitoring, surveillance, inspections, and lighting. Reassign staff to assist.
- Isolate or remove any HAZMAT that might increase the impacts of an attack.

During Periods of Severe Alert (HSAS RED):

- Increase the frequency and thoroughness of surveillance, monitoring, and inspection activities to the maximum level. Request additional support from local law enforcement agencies.
- Close nonessential facilities. Inspect mail/deliveries. Postpone nonessential deliveries.

CYBER SECURITY

These general measures relate to protecting data, process controllers, computers, and networks.

- Implement adequate policies, procedures, and culture regarding cyber security.
- Maintain a well-trained computer security staff with the appropriate knowledge and experience to deal with cyber security issues. To secure specific devices and systems, regularly consult with trade organizations, vendors, or specialists about cyber security practices, standards, and strategies. Conduct thorough background checks on employees serving as system administrators.
- Validate the credentials and work of contractors and vendors given access to technology systems.
- Install and maintain up-to-date cyber security techniques, software patches, and strategies:
  - Ensure systems and networks have sufficient defense-in-depth mechanisms.
  - Provide audit and forensic capability, with easy tools for detecting inappropriate activity.
  - Ensure critical host computers do not have inappropriate applications (e.g., games) installed.
  - Enforce password procedures (e.g., frequency of change, strength, and password reuse).
  - Provide adequate control over remote access and modems (e.g., land-line and wireless).
  - Back up data and configuration files regularly. Maintain backups in a separate/secure location.
  - Develop redundancy in technology hardware and software to keep critical systems operating.
  - Develop a recovery plan to return systems to full functionality after an incident.
  - Regularly review facility Web site to ensure no sensitive information is provided.
- Provide training to all employees who use computer systems on cyber security policy, procedures, responsibilities, threats, and incident reporting. Immediately cancel access for terminated staff.
- Control physical access to critical technology facilities and devices (e.g., computer rooms).
- Regularly test cyber security measures (e.g., audits, penetration testing, war-dialing, tabletop exercises).

During Periods of High Alert (HSAS ORANGE):

- Delay scheduled maintenance and upgrades; increase frequency of system backups.
- Increase system monitoring; ask employees to increase vigilance with regard to unusual activities.
- Reduce access to the Internet; restrict instant messaging and peer-to-peer applications.
- Commit the time of technical support personnel to deal with any problems.

During Periods of Severe Alert (HSAS RED):

- Increase computer security to maximum levels.
- Reduce access to the Internet and other portals to the absolute minimum.
- Have technical support available on-call 24/7.
- Consider disabling the facility's Web site.

INFRASTRUCTURE INTERDEPENDENCIES

These measures relate to the protection of vital utilities that support operations at the facility.

- Ensure that the facility has adequate utility service capacity to meet normal and emergency needs. Identify all utility service points that support the facility. Establish regular communication channels with utility service providers (e.g., electric, gas, water, telecommunications, trash collection companies) to review existing systems, capacity expansion needs, and actions to be taken in response to loss of service from primary supply sources and during other emergencies.
- As much as practical, put utility supply facilities that are potentially hazardous (e.g., liquid fuel tanks, high-voltage power lines) a safe distance from buildings and areas where large numbers of people congregate.
- Ensure that employees are familiar with how to shut off utility services (e.g., electricity, natural gas) in emergency situations.
- Provide adequate physical security (e.g., fencing, locks, protective enclosures, access restrictions) for utility services, fuel storage containers, trash dumpsters, and HVAC systems. Include installation of special locking devices on utility access points (e.g., manhole covers, HVAC vents).
- Where practical, provide for redundancy and emergency backup capability for critical utility services (e.g., backup electric power generators, multiple utility feeder lines). Where possible, locate the redundant and backup equipment in a part of the facility that is different from the one that houses the primary supply equipment. Inspect and maintain redundant and backup equipment regularly.
- Provide for regular monitoring and inspection of utility services (e.g., security patrols, CCTV).
- Secure dumpsters and other trash containers to prevent the hiding of explosives or other HAZMAT and to prevent unauthorized access to discarded papers and records.

During Periods of High Alert (HSAS ORANGE):

- Increase monitoring, inspection, testing, and patrols of all utility services. Request assistance from local law enforcement personnel.
- Establish communication with utility service providers to review plans for responding to any disruptions.

During Periods of Severe Alert (HSAS RED):

- Provide continuous monitoring of all utility services. Consider providing a continuous security guard presence at critical utility points.

INCIDENT RESPONSE

These measures relate to preparations for responding to an actual incident.

- Develop and maintain an up-to-date emergency response plan (see Planning and Preparedness), incident notification process, and emergency 'calling trees' that cover all staff.
- Ensure that there are backup personnel who can execute emergency response functions if primary personnel are unavailable. Ensure that equipment and supplies are adequate to support emergency response requirements; keep them secure and check their status periodically.
- Prepare an emergency operations center to coordinate resources during an incident.
- Conduct regular training, drills, and tabletop exercises with emergency response teams. Involve local emergency responders in drills and exercises.
- Encourage employees to participate in community and other outside organization emergency preparedness and response training.
- Identify entry and exit points to be used in emergencies. Ensure that they are free of obstructions and can be fully utilized. Train all employees on the location of these points.
- Establish procedures for facility evacuation and for shelter-in-place situations. Identify rendezvous points for employees and visitors to gather for 'head counts' after an evacuation.
- Ensure that local law enforcement and emergency responders know the names of and contact information for security and crisis management leaders at each facility.
- Develop policies and procedures for dealing with the media and the general public in the event of an incident to advise them of the situation and to defuse rumors and panic.
- Develop plans to assist the families of facility response teams in the event the teams must be away from home for extended periods.
- Develop plans to provide counseling to employees in the aftermath of an incident.
- Implement procedure for capturing lessons learned and revising response plans after an incident.

During Periods of High Alert (HSAS ORANGE):

- Review and implement emergency response plans. Adjust as necessary for conditions.
- Activate facility emergency operations center as appropriate; notify law enforcement personnel.
- Delay leave or travel for critical facility personnel.
- Pre-position emergency response personnel and equipment to enable rapid response.
- Review and prepare contingency plans that may be needed (e.g., review procedures with employees assigned to direct facility traffic, direct crowd control, guide first responders [if they are needed], or shut off utilities during an incident).

During Periods of Severe Alert (HSAS RED):

- Review available threat information; determine whether the facility should be closed/restricted.
- Bring emergency operations center up to full capability on a 24/7 basis.
- Cancel all leave and travel for facility personnel.

REFERENCE MATERIAL

AJC.com (*Atlanta Journal Constitution*), 2004 [http://www.ajc.com].

APWU (American Postal Workers Union), 2007 [http://www.apwu.org/about/index.htm].

BBC News, 2006, *Cell 'Had Bomb-Smuggling Plans,'* March 28 [http://news.bbc.co.uk/2/hi/uk_news/4853312.stm].

Campanelli, M., 2004a, *Postal Clerk Accused of Identity Theft,* on DMNews.com, May 4, [http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=27363].

Campanelli, M., 2004b, *Mail Study Shows Where the Jobs Are,* on DMNews.com, May 6 [http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=27422].

CBS News.com 2006, *Postal Shooter's Bizarre Behavior*, Feb. 2 [http://www.cbsnews.com/stories/2006/02/02/national/main1272077.shtml].

CBS5.com, 2007, *Hand Grenades in Package at SF Bulk Mail Center*, May 12 [http://cbs5.com/topstories/local_story_132163217.html].

Collins, R., 2007, *Postal and Shipping Sector Security,* presentation by the Branch Chief, Postal and Shipping Sector Security Office, Transportation Security Administration, May 19 [http://mcaa.com/pdf/2007_ace/Rick%20Collins%20MCAA%20Conference%20Presentation.ppt#677,1,Postal and Shipping Sector Security].

Electrical Systems, Inc, undated, *Material and Package Handling Systems* [http://www.esipower.com/Material_Handling.htm].

FedEx, 2006, *FedEx Annual Report* [http://images.fedex.com/us/investorrelations/downloads/annualreport/2006annualreport.pdf?link=4].

GAO (United States Governmental Accountability Office), 2006, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sector's Characteristics,* GAO-07-39, Oct. [http://www.fbiic.gov/reports/d0739.pdf].

GPO/NARA (Government Printing Office, National Archives and Records Administration), undated, Title 39, Code of Federal Regulations, *Chapter I — United States Postal Service,* [http://www.gpo.gov/nara/cfr/waisidx_01/39cfrv1_01.html].

GPO/NARA, 2007a, Title 49, Electronic Code of Federal Regulations, *Chapter 1 – Transportation,* June 27 [http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=585c275ee19254ba07625d8c92fe925f&c=ecfr&tpl=/ecfrbrowse/Title49/49cfrv2_02.tpl].

GPO/NARA, 2007b, Title 41, Code of Federal Regulations, *Public Contracts and Property Management*: *Part 102–192: Mail Management*, June 27 [http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div6&view=text&node=41:3.1.1.7.46.1&idno=41].

Gruman, G., 2004, *UPS versus FedEx: Head-to-Head on Wireless*, on CIO.com, June 1 [http://www.cio.com/article/32312/Wireless_UPS_Versus_FedEx_Head_to_Head_on_Wireless].

Gulla, T., 2004, *U.S. Postal Service Recovers Stolen Mail*, on CitizensVoice.com, May 20 [http://citizensvoice.com/site/index.cfm?newsid=11756765&BRD=2259&PAG =461&dept_id=455154&rfi=8].

Hoovers.com, 2007, *Fed Ex Corporation* [http://www.hoovers.com/fedex/--ID__10552--/free-co-factsheet.xhtml].

Kurth, J., and A. Lee, 2005, *"I'm Going to Die, I'm Going to Die,"* on Detroit News.com, Dec. 29 [http://www.detroitnews.com/apps/pbcs.dll/article?AID=/20051229/METRO/512290360].

Lade, D.C., 2004, *3 Arrested at Delray Post Office, Suspects Hired By Theft Group, Investigators Say*, June 5 [http://pqasb.pqarchiver.com/sun_sentinel/search.html].

MapReport.com, 2003, *Arrested for Bomb Possession: Walnut Creek*, Feb. 17 [http://www.mapreport.com/na/west/ba/news/citysubtopics/walnut_creek_concord_pleasant_hill-c-o.html].

NBC5.com, 2004 [http://www.nbc5.com/index.html].

NJ.com, undated [http://www.nj.com/printer/printer.ssf?/base/news-15/1087109564209440.xml].

Safecity.com, undated, "Bomb Threats, Emergency Response Fire Terrorism Prevention, Building Evacuation, Training Courses Australia" [http://www.safecity.com.au/buieva.htm].

Scanna MSC, 2004, *Suspicious Package in FedEx Drop-off*, March 20 [http://www.scanna-msc.com/news_marapr2004.htm#fedex].

SIU GAO (Southern Illinois University Global Aviation Organization), 2006, photo of collocated UPS and FedEx airport facilities, March 24 [http://www.aviation.siu.edu/gao/UPS_trip/100_0761.JPG].

Smith, T., et al., 2005, *Critical Infrastructure Protection in the National Capital Region, Risk-Based Foundations for Resilience and Sustainability, Final Report, Volume 4: Transportation/ Postal and Shipping Sectors,* University Consortium for Infrastructure Protection, George Mason University, Sept. [http://cipp.gmu.edu/archive/Vol-04-Transportation-Postal-Shipping.pdf].

Sun Sentinel, 2004 [http://www.sun-sentinel.com/news/local/broward/].

The News Tribune.com, 2004 [http://www.thenewstribune.com/search/].

University of Wisconsin, Milwaukee, 2007, *Suspicious Mail Alert Poster*, May 16 [http://www.uwm.edu/Dept/EHSRM/EMERGENCY/uspsposter.jpg].

UPS, 1994–2006, *Business Description* [http://investor.shareholder.com/ups/profile/charter.cfm].

UPS, 1994–2007, *UPS Air Cargo* [http://www.ups.com/aircargo/].

UPS, 2006, *UPS Annual Report: Synchronizing Global Commerce*, [http://files.shareholder.com/downloads/UPS/127817364x0x87221/b13becd7-d1ad-4277-a4e1- b1d19bceb334/UPS_AR_06.pdf].

USPS, 2001a, *Security of the Mail: Postal Service Employee Arrested on Charges Related to Anthrax Hoax,* Nov. 5 [http://www.usps.com/news/2001/press/pr01_1105arrest.htm].

USPS, 2001b, *Security of the Mail: Battling on Many Fronts and with Finances Worsening, USPS Remains Resolute,* Nov. 6 [http://www.usps.com/news/2001/press/pr01_1106 finances.htm].

USPS, 2001c, *Security of the Mail: USPS Tallies Terror Costs for Congress,* Nov. 8 [http://www.usps.com/news/2001/press/pr01_1108aid.htm].

USPS, 2002a, *Security of the Mail: Washington, D.C.,* March 25 [http://www.usps.com/communications/news/security/wdc.htm].

USPS, 2002b, *Latest Facts Update: Inspectors Believe All Bombs Found* and *Bomb Suspect Arrested,* May 8 [http://www.usps.com/news/facts/lfu_050802.htm].

USPS, 2003, *Postal News: Suspicious Envelope in Greenville, SC,* Oct. 23 [http://www.usps.com/communications/news/press/2003/pr03_1023sc.pdf].

USPS, 2004, *Postal News: Washington, DC's V Street Facility Negative for Ricin; Operations Resume,* Feb. 4 [http://www.usps.com/communications/news/press/2004.htm].

U.S. Senate Committee on Homeland Security and Governmental Affairs, 2004, *Postal Reform: Sustaining the 9 Million Jobs in the $900 Billion Mailing Industry*, Hearings on March 9 and 11 [http://www.senate.gov/~govt-aff/index.cfm?Fuseaction=Hearings.Detail&HearingID=156 and http://www.senate.gov/~gov_affairs/index.cfm?Fuseaction=Hearings.Detail&HearingID=157].

Vogel, P.E., 2006, *Management Advisory – Status Report on the Evolutionary Network Development Initiative* (Report Number NO-MA-06-001), USPS Office of the Inspector General, March 20 [http://www.uspsoig.gov/foia_files/NO-MA-06-001.pdf].

WindowsForDevices.com, 2004, *UPS Delivers with Windows CE/Bluetooth Ring Scanners,* July 15 [http://www.windowsfordevices.com/news/NS6853848656.html].

OTHER USEFUL INFORMATION

The White House, 2003, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. [http://www.whitehouse.gov/pcipb/physical.html].

The White House, 2003, *The National Strategy to Secure Cyberspace*, Feb. [http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf].

The White House, 2003, Homeland Security Presidential Directive/HSPD-7, Dec. 17 [http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html].

Virginia Tech, *Workplace Violence* [http://www.ehss.vt.edu/Programs/OSD/Emergency%20 Planning/workplaceviolence.htm].

University of California, San Diego, *UCSD Workplace Violence Employee Handbook* [www.police.ucsd.edu/docs/handbook.pdf].

University of Vermont, *Indicators of Potential Workplace Violence* [http://siri.uvm.edu/ppt/ wrkplviolence/sld037.htm].

U.S. Department of Homeland Security

DHS (U.S. Department of Homeland Security) [http://www.dhs.gov].

DHS, 2006, *Overview of Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures for Critical Infrastructure and Key Resources*, Risk Management Division, Office of Infrastructure Protection, April.

DHS, 2007, *Homeland Security Completes Framework for Infrastructure Protection* [http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm#3].

DHS, 2006, *National Infrastructure Protection Plan (NIPP)* [http://www.dhs.gov/xlibrary/ assets/NIPP_Plan.pdf].

Other U.S. Government Agencies

Agency for Toxic Substances and Disease Registry [http://www.atsdr.cdc.gov/].

Centers for Disease Control and Prevention [http://www.cdc.gov/].

Federal Bureau of Investigation [http://www.fbi.gov/].

Other Organizations

American Red Cross, 2006, *Terrorism: Preparing for the Unexpected* [http://www.redcross. org/services/disaster/0,1082,0_589_,00.html].

Defense Intelligence College, *Introduction to Terrorism Intelligence Analysis, Part 2: Pre-incident Indicators*, Counterterrorism Analysis Course [http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm].

United Kingdom Home Office, 2005, *Protecting against Terrorism*, Civil Contingencies Secretariat [http://www.ukresilience.info/publications/protecting.pdf].

Note: Information presented here is subject to copyright laws and other terms of use as set forth in the respective references.

DHS Reader Satisfaction Survey

Mail or Fax to:
Argonne National Laboratory
Infrastructure Assurance Center
9700 South Cass Avenue, Building 900
Argonne, IL 60439
Fax: 1- 630-252-9559

Dear Reader,

Please take a few minutes to complete this survey. Your input will be used to evaluate the quality and value of DHS products. It is important that this report series on Common Vulnerabilities (CV), Protective Measures (PM), and Potential Indicators of Terrorist Activity (PI) remain responsive to your needs.

Thank you.

Circle your response accordingly:

1	Strongly Disagree
2	Disagree
3	Neither Agree or Disagree
4	Agree
5	Strongly Agree
NA	Not Applicable

Quality

1	2	3	4	5		Information in this report is presented clearly and logically.
1	2	3	4	5		The content and documented sources make this report reputable.
1	2	3	4	5	NA	The LENS web site is easy to access.
1	2	3	4	5	NA	Information on the LENS web site is easy to navigate and find.

Value

1	2	3	4	5	NA	This report is relevant to your mission, programs, priorities, or initiatives.
1	2	3	4	5	NA	This report enhanced your knowledge of infrastructure protection.
1	2	3	4	5	NA	This report will likely result in changes to your existing protection practices.
1	2	3	4	5	NA	This report will likely result in more informed protection decisions.
1	2	3	4	5		I will recommend that colleagues review this report.

Comments

Title or type of report: ____________________________Organization or reader name: ________________________

____

____

____