Homeland Security, Rasco Industries, Inc., in trying to help our customers, has been looking thru information on requirements for loading dock doors. So far we have not found detailed or specific requirements only generalities.

Here is everything we can find from Homeland Security having to do with a loading dock door:

Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings Fema-426/ BIPS-06/ Edition 2

"Infrastructure protection and disaster management; the overall goal of this program is to enhance the blast and chemical, biological, and radiological (CBR) resistance of our Nation's buildings and infrastructure to meet specific performance requirements at the highest possible level. The information contained in this manual is: **Not mandatory,** Not applicable to all buildings. **Building owners and managers must be the ones to determine their level of risk to each threat and decide from which threats to seek protection.** Decision makers who consider their buildings to be at elevated risk may be able to use this guidance to mitigate the potential risks from hazards or terrorist attacks against their buildings."

The basic approach to site security design promoted is the concept of Layers of Defense. Second or Middle Layers that usually extends from the perimeter of the site to the exterior face of a building. Protective measures consist of natural or **manmade barriers along with a site design strategy of keeping terrorists away from the inhabited building.**

Install blast-resistant doors **or steel doors with steel frames.**

The objective of the access point is to prevent unauthorized access, while at the same time controlling the rate of entry for vehicles and pedestrians.

Vulnerable areas (where suspect material may enter a building), such as lobbies, **loading docks**, mailrooms, and parking garages should be isolated from the rest of the building and **protected by using** reinforced floors, ceilings, and full height walls, and **hardened doors**. No building systems or utilities, other than those directly supporting the function within, should be placed on either side of the walls for these areas. **Both interior and exterior doors to these areas should remain closed when not in use.**

Access control. **Any combination of barriers, gates,** electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.

Entrance control. Operate and enforce a system of access control (vehicle or pedestrian), including inspection of credentials and packages.

2.4.2 Loading Docks and Service Areas:

Loading docks and service areas are commonly kept as unobtrusive as possible, but special entry controls may be required (i.e., a screening area or **gated entry way**). Significant structural damage to the walls and ceiling of the loading dock may be tolerable as long as the areas adjacent to the loading dock do not experience severe structural damage or collapse. Adequate structural design (robust and

redundant load paths) can limit damage to the loading dock area and allow explosive forces to vent to the building exterior.

Design guidelines for loading docks and service access include the following:

Provide an inspection area for screening, either offsite or a significant distance away from the loading dock, before permitting entrance to the loading dock. Locate loading docks and shipping and receiving areas away from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire-suppression water mains, cooling and heating mains, and others. Avoid the placement of driveways within or under buildings. Consider whether areas below the loading dock are occupied or contain critical utilities in determining whether to design the loading dock for blast resistance. Provide signage to clearly mark separate entrances for deliveries

Louvers: Emergency generators located inside buildings require adequate **ventilation**, such as large louvers, for cooling. Similar to windows, the larger the louver the higher the cost to harden against explosive blast. Where accessible from the ground, **louvers should be secured to prevent forced entry.** For protection against malicious acts, **intakes should be covered by screens** so that objects cannot be tossed inside from the ground level. Such screens should be sloped to allow thrown objects to roll or slide off the screen, away from the intake.

Windows: Other general security considerations for the design of glazing and windows include the following: Window openings should be protected with guards, such as grills, **screens, or meshwork,** firmly affixed to the structure.

5.2.3 Physical Barriers

Physical barriers, a core component of security, are manmade or natural features that control, block, contain, restrict, or direct people and vehicles with a purpose to reduce the risks from a potential terrorist attack. **Physical barriers include** site features such as **f**encing, gates, and active and passive vehicle barriers. Building physical barriers include walls, **doors,** windows, and other structural elements. Barriers can also provide ballistic**, forced entry** and blast **protection to a facility**

BUILDINGS AND INFRASTRUCTURE PROTECTION SERIES SECURITY SYSTEM DESIGN GUIDANCE

No barrier should stand alone in a protective posture. For a barrier to be successful, it not only needs to fit the threat scenario, it also requires elements for detection and response. In most common applications, intrusion detection and video assessment systems are used to fulfill the detection elements. Guards are also used to fulfill the detection, delay, assessment, and response functions of a security system. **Physical barriers have been overlooked in the planning and design process in the past.**

5.2.4 Security Systems and Equipment

Physical barriers and electronic security measures are used in conjunction The next layer of physical barriers and electronic security devices would then provide sufficient delay to prevent the aggressor from gaining access to the building.

5.3.2 Application of Security Measures in Layers

The concept of applying multiple security measures in consecutive layers starting as far away from the asset as possible (typically to the site perimeter or further with permission), often referred to as **concentric layers of security, is the basic risk mitigation approach to all security systems**. Planning for security in layers is based on the security industry concept of the "Four Ds" (deter, detect, defend, and defeat). Deterrence is a byproduct of planning for the other three, because you cannot design deterrence. Three basic types of security measures can be used singly or combined in each consecutive layer: Defensive measures, Detection measures and Delaying measure.

5.3.2.1 Defensive Measures

The objective of layers of defense is to create a consecutive number of security layers each more difficult to penetrate. This provides additional time for detection, assessment, and response, and allows building occupants to move into defensive positions or designated safe haven areas. Establishing defensive layers is a key component in the development of protective measures, particularly as the asset value and risks values increase.

Physical barriers, a core component of security are manmade or natural features that control, block, contain, restrict, or direct people and vehicles with a purpose to reduce the risks from a potential terrorist attack. Physical barriers include site features such as fencing, gates, and active and passive vehicle barriers**. Building physical barriers include** walls**, doors,** windows, and other structural elements. Barriers can also provide ballistic, **forced entry** and blast **protection to a facility. A security system is a combination of multiple components** that must work together seamlessly to provide the appropriate level of protection for a facility. Lack of one element can create substantial vulnerabilities to the protective systems and the assets they protect.

BUILDING DESIGN FOR HOMELAND Security
Unit VIII Site and Layout Design Guidance -FEMA

Identify site planning concerns that can create, reduce, or eliminate vulnerabilities and understand the concept of "Layers of Defense."
Compare the pros and cons of barrier mitigation measures that increase stand-off or create controlled access zones.
References: **FEMA Building Vulnerability Assessment Checklist, Chapter 1, page 1-46, FEMA 426 Site and Layout Design Guidance,Chapter 2 -FEMA 426**

Loading Docks/Service Access:
- Ensure separation from critical systems and utility service entrances.
- Avoid driving trucks into or under building. Provide clear signage.

Buildings and Infrastructure Protection Series Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
FEMA-426/BIPS-06/October 2011 Edition 2

2.4.2 Loading Docks and Service Areas
Loading docks and service areas are commonly kept as unobtrusive as possible, but special entry controls may be required (i.e., a screening area or gated entry way). Significant structural

damage to the walls and ceiling of the loading dock may be tolerable as long as the areas adjacent to the loading dock do not experience severe structural damage or collapse. Adequate structural design (robust and redundant load paths) can limit damage to the loading dock area and allow explosive forces to vent to the building exterior.
Design guidelines for loading docks and service access include the following:

- Provide an inspection area for screening, either offsite or a significant distance away from the loading dock, before permitting entrance to the loading dock.
- Locate loading docks and shipping and receiving areas away from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire-suppression water mains, cooling and heating mains, and others.
- Avoid the placement of driveways within or under buildings.
- Consider whether areas below the loading dock are occupied or contain critical utilities in determining whether to design the loading dock for blast resistance.
- Provide signage to clearly mark separate entrances for deliveries.

Protective measures for the second layer of defense:

- Designate entry points for commercial and delivery vehicles away from high-risk areas

Protectives measures for the third layer of defense:

- Ensure that exterior service doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- **Restrict access** to building operation systems.
- Illuminate building access points.
- Limit the number of doors used for normal entry/egress
- Stagger interior doors and offset interior and exterior doors.Use interior barriers to differentiate levels of security.
- Isolate lobbies, mailrooms, **loading docks**, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- **Install** blast-resistant doors or **steel doors with steel frames**
- Physically separate unsecured areas from the main building.