

Risk Management Series

Insurance, Finance, and Regulation Primer

for Terrorism Risk Management in Buildings

December 2003



FEMA

RISK MANAGEMENT SERIES

Insurance, Finance, and
Regulation Primer *for*
Terrorism Risk Management
in Buildings

PROVIDING PROTECTION TO PEOPLE AND BUILDINGS



FEMA

Federal Emergency Management Agency
www.fema.gov

FOREWORD AND ACKNOWLEDGEMENTS

This primer is a part of the Multihazard Risk Management Series of publications that addresses terrorism risk in buildings. The objective of this primer is to introduce the building insurance, finance, and regulatory communities to the issue of terrorism risk management in buildings and the tools currently available to manage that risk.

ACKNOWLEDGEMENTS

Principal Authors:

Frederick Krimgold, Virginia Tech
David B. Hattis, Building Technology Inc.
William I. Whiddon, Building Technology Inc.

Contributors:

Michael T. Chipley, UTD Incorporated
Wesley W. Lyon, UTD Incorporated
Michael J. W. Kaminskas, UTD Incorporated
Mark Hester, UTD Incorporated

Project Advisory Panel:

Bernard M. Brown, Insurance Advisors, Inc.
Mary Pat Denney, Freddie Mac
Joseph Donovan, Carr America
Dottie Harris, New York State Department of State
Lawrence H. Mirel, DC Department of Insurance and Securities Regulation
Matt S. Munter, EMG Corporation

Technical Review:

Deborah McKinnon, Mortgage Bankers Association
Don Glitz, GMAC Commercial Mortgage

FEMA Advisory Panel:

Christopher Arnold, Building Systems Development
Wade Belcher, General Services Administration
Curt Betts, Army Corps of Engineers
Jim Caulder, U.S. Air Force – Civil Engineer Support Agency
Joseph Coughlin, FEMA
Marcelle Habibion, Department of Veterans Affairs
Joseph Hartman, Army Corps of Engineers
Eve Hinman, Hinman Consulting Engineers
Rick Jones, Naval Facilities Engineering Service Center
Kurt Knight, Department of Veterans Affairs
Howard Leikin, FEMA
Eric Letvin, URS Corporation
John Lynch, Naval Facilities Command (NAVFAC) Criteria Office
Terry Pruitt, Department of Homeland Security

Christopher Rojhan, Applied Technology Council
Lloyd Siegel, Department of Veterans Affairs

Project Officer:

Milagros Kennett, FEMA, Building Sciences Technology Branch,
Mitigation Division

CHAPTER 1

Introduction	1-1
Intervening in the Building Investment Process	1-2
Primer Organization	1-4
Insurance	1-4
Finance	1-5
Regulation	1-5
Due Diligence for Terrorism Vulnerability Assessment	1-6
Guide to Expertise and Tools	1-7

CHAPTER 2

Insurance and Terrorism Risk	2-1
Role of Insurance	2-1
Terrorism Risk for Insurers	2-1
Building Insurance Industry.....	2-2
Actuaries	2-4
Insurance Industry Infrastructure.....	2-4
Insurance Product Lines.....	2-6
World Trade Center Insurance Experience	2-8
Property and Liability	2-8
Business Interruption	2-9
Workers' Compensation, Health, and Life	2-10
Insurance Losses.....	2-11
Current Insurance Situation	2-11
Terrorism Risk Insurance Act of 2002	2-12
Participation and Reimbursements	2-13
Limitations	2-13
Insurance Risk Management Models.....	2-14
Data Needs for Insurance	2-15
Lack of Actuarial Information	2-16
Future Developments.....	2-16

CHAPTER 3

Finance and Terrorism Risk	3-1
Terrorism Risk Threat to Lenders	3-1
Building Finance Community	3-1

Lenders Concerns	3-2
Terrorism Impact	3-2
Current Finance Situation	3-4
Lender Risk Management Models	3-6
Future Developments	3-7
CHAPTER 4	
Building Regulation and Terrorism Risk	4-1
Terrorism Risk for Regulators	4-1
Regulation of Terrorism Risk	4-1
Balancing Stakeholder Interests	4-1
Implications for Building Regulation Enforcement	4-1
Current Building Regulation Situation	4-3
Code Relation to Terrorist Threats	4-3
Regulatory Activities Related to Terrorism Risk	4-4
Building Regulation Management Models	4-5
Future Developments	4-6
CHAPTER 5	
Due Diligence: Estimating Vulnerability	5-1
Fundamental Changes	5-1
Due Diligence Assessment of Vulnerability to Terrorist Attack	5-1
Mitigation of Vulnerability	5-2
Process Model for Terrorism Risk Reduction Used in	
Federal Facilities	5-2
Protection Priority	5-3
Threat Assessment	5-4
Defining Threats	5-5
Identifying Likely Threat Event Profiles and Tactics	5-6
Assigning a <i>Threat Rating</i>	5-10
Alternative: Assigning a <i>Level of Protection Against Threat</i>	5-11
Vulnerability Assessment	5-12
Initial Vulnerability Estimate	5-13
Visual Inspection	5-13
Design Documents Review	5-14
Organization and Management Procedures Review	5-14
Assessment of Vulnerability to Expected Methods	
and Means of Attack	5-14
Vulnerability Estimate Screening	5-15

‘Site’ Questions	5-16
‘Architectural’ Questions	5-17
‘Structural and Building Envelope Systems’ Questions	5-18
‘Utility Systems’ Questions	5-19
‘Mechanical Systems’ Questions	5-20
‘Plumbing and Gas Systems’ Questions	5-21
‘Electrical Systems’ Questions	5-22
‘Fire Alarm Systems’ Questions	5-23
‘Communications and Information Technology Systems’ Questions	5-24
Additional Sources of Detailed Facility Information	5-25
Vulnerability Reduction Cost Information and Estimates	5-25
CHAPTER 6	
Guide to Expertise and Tools	6-1
Terrorism Risk Insurance Act of 2002	6-1
Building Vulnerability Assessment Screening	6-1
General Glossary	6-2
Chemical, Biological, and Radiological Glossary	6-2
Acronyms	6-2
Associations and Organizations	6-2
Bibliography	6-3
APPENDIX A	
Terrorism Risk Insurance Act of 2002	A-1
APPENDIX B	
Building Vulnerability Assessment Screening	B-1
APPENDIX C	
General Glossary	C-1
APPENDIX D	
Chemical, Biological, and Radiological Glossary	D-1
APPENDIX E	
Acronyms	E-1
APPENDIX F	
Associations and Organizations	F-1
APPENDIX G	
Bibliography	G-1

This primer, FEMA 429, *Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings*, is a part of the Multihazard Risk Management Series of publications that addresses terrorism risk in buildings. The objective of this primer is to introduce the building insurance, finance, and regulatory communities to the issue of terrorism risk management in buildings and the tools currently available to manage that risk. Insurance, finance and regulation are considered the 'change levers' of the built environment. They are the principal mechanisms for the evaluation and management of risk exposure in buildings. These change levers play a critical role in introducing and maintaining standards for risk management and public safety.

CHANGE LEVERS FOR TERRORISM RISK REDUCTION

Risk management in the built environment is a complex issue that involves a range of decision-makers in all phases and at all levels in the building development, design, construction, and management process. The traditional market mechanisms for estimating, pricing, and distributing risk are the insurance and finance industries. The established mechanism for defining society's acceptable risk levels in the physical environment is the public regulation of development, including zoning and building regulation.

Risks related to hazards such as fire, earthquake, flood, asbestos, and lead paint have been dealt with through these mechanisms. These risks have been identified and assessed, and applicable actuarial data has been collected. Physical measures for risk reduction have been developed and defined. Residual risks have been quantified and mechanisms for risk transfer are in place.

The process of understanding and managing of terrorism risk is at its very beginning. All of the mechanisms of the traditional

Change Levers:

Insurance—those entities that will share some or all of the risks that a building owner faces.

Finance—lenders (such as banks and corporate entities) and fiduciaries (such as pension funds and trustees), which provide the resources for owner investments in buildings.

Regulation—governmental entities (federal, state, and local) that regulate building design, construction, and use in order to achieve public health, safety, welfare, and other social objectives.

TERRORISM

The term 'terrorism' refers to intentional, criminal, malicious acts. There is no single, universally accepted definition of terrorism. Officially, terrorism is defined in the Code of Federal Regulations as "...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (28 CFR, Section 0.85). The Federal Bureau of Investigation (FBI) further characterizes terrorism as either domestic or international, depending on the origin, base and objectives of the terrorist organization. However the origin of the terrorist causing the threat is less relevant to terrorism risk management than the hazard itself and its consequences.

The categories of terrorism threats are varied. The principal threats that have been considered in the available literature include:

- Armed Attack
- Arson/Incendiary Attack
- Biological Agents
- Chemical Agents
- Conventional Bomb
- Cyber Terrorism
- Hazardous Material Release
- Nuclear Device
- Radiological Agents
- Surveillance
- Unauthorized Entry

Management of terrorism risk includes the assessment and consideration of this range of threats and their varied delivery modes.

building risk management process must be engaged to address the issue of terrorism risk. They must understand the threat, develop the measures for risk reduction, and motivate the implementation of appropriate risk reduction measures. The building design and management communities must develop the physical and operational solutions. But it is the change levers of finance, insurance, and regulation that can motivate and reward the implementation of those solutions.

INTERVENING IN THE BUILDING INVESTMENT PROCESS

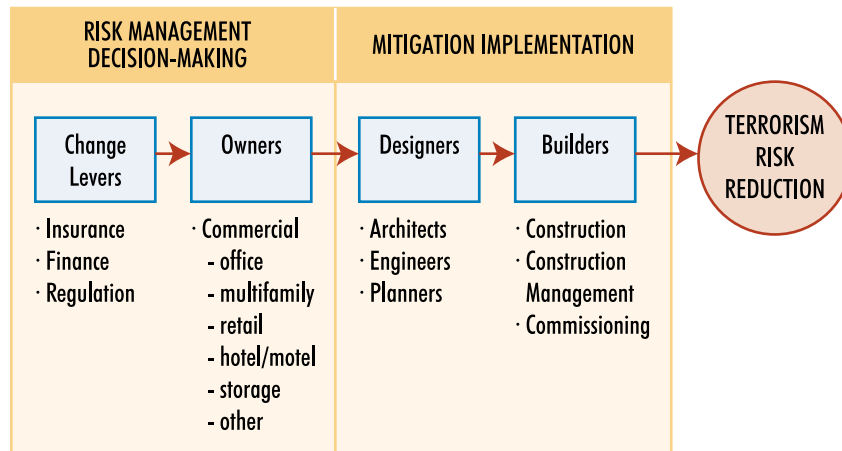
It is necessary that guidance on the design, construction, and rehabilitation of buildings to reduce terrorism risk be made available to architects, engineers, and constructors. The other publications of the FEMA *Multihazard Risk Management Series* provide this guidance. However, architects, engineers, and constructors implement the programs and directives of their clients—building developers and owners—who must be aware of the opportunity and the benefits of investing in terrorism risk reduction measures before they decide to make such investments.

What motivates building owners to make investment decisions about their buildings? Most owners view their buildings as revenue generators, not as instruments of social policy. Owners invest in buildings in order to realize an economic re-

turn. How can owners be persuaded that investments to reduce their vulnerability to terrorist attack will make business sense?

Figure 1-1 is a schematic representation of the building process as it addresses the issue of terrorism risk reduction. Buildings are the final product of this process. Designers and builders are key actors in the implementation of physical mitigation of risk, but

Figure 1-1: Terrorism Risk Reduction Decision-Making



building owners and change levers are the key decision-makers regarding management of risk in buildings. In order to introduce physical or operational change in buildings (to reduce terrorism risk), it is necessary to intervene at several points.

Builders who actually construct the buildings must be guided by the plans and specifications developed by the design professionals (architects and engineers). The design professionals are, in turn, guided by the programs and demands of their clients, the owners. Building owners have functional, financial, and esthetic objectives that may or may not specifically include risk management. It is the change levers that are most sensitive to risk management needs and are in a position to effectively leverage owner interests that are communicated to designers and builders.

It is of key importance that owners demand appropriate mitigation measures in design, that designers have the specific technical guidance to provide required mitigation measures, and that builders have the technical capability to implement appropriate designs. However, highest in this causative chain of decision-making are the change levers that influence the entire process that ultimately determines the end product.

If investments cannot result directly in added profit in the form of increased rents or reduced operating costs, they will not be

made, unless owners are induced or forced to make them by the change levers. The change levers must create an environment that demands and rewards investment in safety.

Regulators force such changes through laws that mandate terrorist resistant building design and construction. Lenders induce such changes by requiring them as conditions of the loan to acquire or construct the building, or by adjusting interest rates or other terms of the loan. Insurers can motivate such changes by relating premiums to risk and rewarding effective mitigation

In order to introduce these changes, it is necessary for the change levers to understand the character of terrorism risk, understand available risk reduction measures, and be able to evaluate related costs and benefits. This primer provides this information.

PRIMER ORGANIZATION

Insurance

Chapter 2 of this primer provides information on terrorism risk management for the insurance industry.

The insurance industry consists of three primary segments, each of which has a unique role in the assessment of terrorism risk, and therefore can benefit from familiarity with the information in this primer:

- Direct insurers
- Reinsurers
- Agents/brokers

The industry is supported by a complex infrastructure, each component of which will be able to use this information:

- Overseers/regulators
- Technical support
- Think tanks (risk modelers)

- Lobbying groups
- Independent advisors and consultants

The industry also segments itself by product lines. Some of these lines have a direct relationship to building safety features, and others may have an indirect relationship:

- Property, liability, and business interruption
- Workers' compensation
- Health (and health maintenance organizations)
- Life

Buyers of insurance are represented by various associations such as the Risk and Insurance Management Society (RIMS), and the Apartment and Office Building Association (AOBA).

Finance

Chapter 3 of this primer provides information that will be of use to both commercial and multifamily lenders, including:

- Loan originators
- Loan servicers
- Secondary markets
- Bond markets

Regulation

Chapter 4 provides information on terrorism risk management for the building regulatory community.

There are four categories of building regulation that have the potential to address terrorism risk reduction, and each has its own array of audiences:

- Zoning and planning regulations
- Property maintenance codes
- Building rehabilitation codes

FEDERAL RESOURCES FOR TERRORISM RISK MANAGEMENT

Terrorism risk in the past has primarily been the concern of the Department of Defense and Federal intelligence agencies. Before the attacks of September 11, 2001 the bulk of terrorism experience was outside the United States. The Federal Emergency Management Agency of the Department of Homeland Security is now providing broad public access to available materials and methods previously developed for the assessment and management of terrorism risk. Much of this material was originally intended for "Official Use," but is now deemed to be of critical value for the management of terrorism risk in the domestic civilian sector.

The core reference document of the FEMA *Multihazard Risk Management Series* is FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. FEMA 426 includes reference to the terrorism risk management and mitigation materials developed by:

- General Services Administration
- Naval Facilities Engineering Service Center
- Naval Facilities Command Criteria Office
- U.S. Army Corps of Engineers Protective Design Center
- Department of Veterans Affairs
- National Institute for Occupational Safety and Health
- Department of Justice, Office of Domestic Preparedness
- U.S. Air Force, Civil Support Agency

- Construction codes (building, mechanical, plumbing, electrical)

All four categories of building regulation include extensive reference to voluntary standards that are developed by a wide array of organizations.

These regulations are enforced by a variety of local and/or state agencies, each represented by trade associations, including:

- Building officials and building departments
- Fire marshals and fire prevention bureaus
- Health departments
- Planning and community development departments and agencies

Due Diligence for Terrorism Vulnerability Assessment

Chapter 5 provides information on due diligence for terrorism vulnerability assessment for individual buildings and facilities.

Methods for threat assessment and vulnerability assessment are described and a framework for a qualitative terrorism risk 'vulnerability estimate' is presented.

Guide to Expertise and Tools

Chapter 6 provides reference to resources, including:

- The Terrorism Risk Insurance Act of 2002
- Building Vulnerability Assessment Screening
- A general glossary
- A chemical, biological, and radiological glossary
- A list of acronyms

- A list of associations and organizations related to terrorism risk management
- A bibliography

ROLE OF INSURANCE

Insurance plays a critical role in society in the management of risk. Insurance provides a mechanism for spreading risk, which allows individuals to accept risks that would otherwise be unacceptable. Insurance also provides the service of pricing risk. On the basis of actuarial data and analysis insurers attempt to quantify risks and to set rates for the financing of risks.

This chapter presents a discussion of terrorism risk. It is directed at all segments and components of the insurance industry so that they can begin to determine how to establish an actuarial basis for insuring against terrorism risk. The specific intent of this chapter is to help the insurance industry utilize its considerable influence on the building industry to encourage investments in terrorism risk mitigation.

Property insurance has worked very well for a range of familiar hazards such as fire and windstorm. Not only has insurance served to transfer risks, it has also provided the database for identifying and reducing risks.

Loss data has contributed to general understanding of perils and has led to the development of effective mitigation measures. Recognition of the effectiveness of those mitigation or risk reduction measures has been reflected in differential premiums that provide a direct incentive for mitigation investment. Risk based access to insurance and risk based pricing of insurance make it a very effective change lever strongly influencing building design and management practices.

Terrorism Risk for Insurers

Terrorism risk is new to the United States. The threat is not well defined. There is very limited experience or actuarial data. There is even less experience of the effectiveness of protective measures in buildings. The insurance industry is now struggling to digest this new threat. Traditional means of analysis are so far ineffective in providing the basis for pricing the risk.

Lacking greater experience it is difficult to gauge the accuracy of terrorism risk perception on the part of key participants in the real estate industry. Potential buyers of terrorism risk coverage must have a reasonable basis for estimating their insurance needs. At the same time, those selling insurance must have a defensible basis for pricing terrorism risk coverage. In the absence of data or other means of determining premiums, and in light of

the catastrophic loss potential of the risk, insurers left the market. In response to this crisis in the insurance market the federal government has taken extraordinary measures to provide temporary support for the insurance market. These measures are discussed later in this chapter.

Insurance pricing and availability are also driven by market capacity and competition. Even without actuarially based rates the pricing mechanism of the market will come into play. Demand for terrorism risk insurance is driven in part by building owners' perception of their risk and in part by the risk perception of their lenders. Both owners and lenders rely on the insurance industry to price such risks.

Evaluation of terrorism vulnerability in planned and existing commercial buildings can provide valuable input to the rating of relative risk for specific buildings. Criteria for the evaluation of relative terrorism risk in buildings can eventually contribute an important component of the ratemaking equation. Recognition by the insurance industry of effective risk reduction measures should provide guidance and incentive for investment in terrorism risk reduction.

Some aspects of terrorism risk may be approached through community rating systems, such as that used in the National Flood Insurance Program, which reflect the target priority and the state of security organization of a community. Because of the relationship of terrorism risk to national security policy it may prove reasonable that the federal government role be extended.

Building Insurance Industry

The insurance industry consists of three primary segments, each of which has a unique role in the assessment of terrorism risk, and therefore can benefit from familiarity with the information in this primer:

- Direct insurers
- Reinsurers
- Agents/brokers

Direct insurers are the front line of the insurance industry. The direct insurer writes the policy, collects the premium and pays the claim to the insured. Direct insurers are now required by state insurance regulators to offer terrorism risk insurance. It is the responsibility of the direct insurer to set premium rates based on an analysis of exposure and risk. This rate structure must be reviewed and ultimately approved by the various state insurance commissioners in most state jurisdictions.

Ideally, direct insurers need basic information on the frequency and severity of terrorist events and on the vulnerability of particular properties to terrorist attack in order to set specific premiums. They must also know the effectiveness of specific mitigation measures in order to modify premium rates appropriately.

Reinsurers provide insurance for direct insurers. That is, direct insurers are able to purchase reinsurance to cover some part of their exposure. Reinsurers are not regulated by state insurance commissioners and are not required to provide reinsurance for terrorism risk. Following the World Trade Center (WTC) attack most major reinsurers excluded terrorism risk from new treaties with direct insurers. This created a temporary crisis in insurance markets in that direct insurers were required to provide terrorism risk insurance but they were no longer able to transfer part of that risk to reinsurers.

Ideally, reinsurers need information on the frequency and severity of expected terrorist attacks on a global scale. They also need to be able to evaluate the effectiveness of the property risk assessment methodologies of their clients, the direct insurers.

Insurance agents and brokers are the key connection between insurance buyers and sellers. Agents typically represent the seller and brokers typically represent the buyers. Agents and brokers communicate directly with the policyholder or the building owner. It is necessary for agents and brokers to understand the specific exposure and insurance needs of the client as well and the policy conditions and exclusions of the insurer. In the case of terrorism risk this will require understanding of the physical and

operational aspects of buildings that indicate vulnerability to terrorist attack.

Actuaries

Actuaries are the foundation of the insurance business, and they provide services for each of the primary segments of the industry. The actuary assesses the available loss data to quantify the risk as the basis for pricing risk and setting premiums. Actuarial data and analysis is the basis for the pricing of risk and evaluating the solvency of insurance companies. The key problem in the assessment of terrorism risk is the lack of actuarial data. There are very few examples of terrorist attack losses in the United States. It is very difficult to generalize or project expected losses on the basis of this documented experience. Terrorism is not a well-defined or stable phenomenon. Without actuarial data it is difficult to price the risk and it is difficult to defend proposed rates.

Insurance Industry Infrastructure

The industry is supported by a complex infrastructure, each component of which will be able to use this information:

- Overseers/regulators (historically, insurance is regulated at state level by insurance commissioners)
- Technical support: Insurance Services Office (ISO), National Workers Compensation Commission, Association for Cooperative Operations Research and Development (ACORD), and others
- Think tanks (risk modelers) and risk control consultants: EQECAT, Risk Management Solutions (RMS), Applied Insurance Research (AIR), and others
- Lobbying groups: American Insurance Association (AIA), National Association of Insurance Brokers (NAIB), Reinsurance Association of America (RAA), Risk and Insurance Management Society (RIMS), and others

State insurance commissioners have a primary responsibility to ensure the solvency of insurance companies and their ability to

pay claims when required. This means they have a strong interest in the quality of actuarial data and analysis used in rate setting and they review both the forms and the pricing. They are also concerned with ensuring access to insurance at reasonable rates. For this reason insurance regulators need to know how to evaluate rates proposed by insurers for terrorism risk cover. They also need to know the value of risk reduction measures (risk modification factors) that might be considered to qualify for premium reductions.

Insurance regulation is concerned with the viability of insurance companies as a consumer protection issue. Regulators want to ensure that premiums are sufficient to pay insurance losses and that insurers remain in business. Insurers are required to project future risk and to show a plausible investment strategy.

For the most part, insurance regulators do not set rates-companies propose and regulators evaluate justification of rates. Insurance rating agencies are exempt from anti-trust so that data can be shared. The rating agencies analyze all available data. They are mathematicians and statisticians, not modelers.

Technical support organizations help to translate research into new tools for the insurance industry. This includes the development of standard procedures and forms and guidance on rate making. Technical support organizations have a very important role in providing analysis and technical support for many direct insurers. Such technical service organizations provide a valuable channel for the processing of information and the development of insurance services. They can provide a valuable link in the development of insurance products and practice to deal with terrorism risk.

Worthy of particular note are the services provided by the Insurance Services Office (ISO). Every year, ISO gathers information from insurance companies on hundreds of millions of policies including the premiums the companies collect and the losses they pay. ISO submits summaries of that information to insurance regulators, as required by law, to help the regulators evaluate the

price of insurance in each state. ISO also uses the information in its database to prepare products and services that help insurers compete in the marketplace. They provide a wealth of related products and services, including standardized policy language, rating and underwriting rules, and site surveys of individual properties.

Think tanks are risk management organizations staffed by scientists and engineers as well as insurance specialists who carry out and apply research on perils and vulnerability of insured properties. Over the past twenty years much progress has been made in developing refined understanding of complex perils including natural and environmental hazards. Loss estimation models have been developed that help the insurance industry deal with low frequency, high consequence events, like earthquakes. These research-based think tanks are currently working on the modeling of terrorism risk to provide loss estimates for rate setting and mitigation actions.

Lobbying organizations that represent the insurance industry in public policy circles, and are also acutely interested in understanding the character of terrorism risk. As a highly regulated industry, insurance is very much subject to legislative and regulatory decisions. The Terrorism Risk Insurance Act of 2002 (discussed later in this chapter) is an example of a significant federal response to a crisis affecting the insurance industry. Future exposure to and management of terrorism risk is a major issue of public/private policy discussion.

Insurance Product Lines

The insurance industry segments itself by product lines, some of which have a direct relationship to building safety features, and others of which may have an indirect relationship:

- Property, liability, and business interruption
- Workers' compensation
- Health (and health maintenance organizations)
- Life

Table 2-1: Relationship of Terrorist Threats to Particular Lines of Insurance

Threat/Hazard	Property/ Liability	Business Interruption	Workers' Compensation	Health	Life
Armed attack	●	○	○		●
Arson/incendiary	●	●	○		●
Biological agent	○	●	●	○	●
Chemical agent	○	●	●	○	●
Conventional bomb	●	●	●	○	●
Cyber-terrorism		●			
HAZMAT release	○	●	●	○	○
Nuclear device	●	●	●	○	●
Radiological agent	○	●	●	●	●
Surveillance		●			
Unauthorized entry		●			

LEGEND: ● = Probable relationship

○ = Potential relationship

Various terrorist threats may cause losses that are covered by different insurance product lines. Some terrorist threats may cause losses that are not covered by any insurance. Table 2-1 suggests the relevance of recognized terrorist threats to the various lines of insurance. It is important to note that aside from bomb blast and arson most of the threats do not necessarily imply physical damage to buildings.

World Trade Center Insurance Experience

The strongest image of terrorist attack is the collapsing towers of the World Trade Center. Clearly, terrorism risk is a major concern for property and liability insurers. However, significant claims have resulted for many other lines of insurance as a result of terrorist attacks. September 11, 2001 is the costliest day in insurance history. Total losses are estimated to be three times the largest previous insurance loss in Hurricane Andrew (\$18 billion in 1992).

Insurance losses resulting from the World Trade Center attack fall into various categories:

- Property losses to the WTC and surrounding buildings, incurred by building owners.
- Business income and rent loss due to the inability to use the destroyed facilities, incurred by building owners and tenants.
- Workers compensation, life and health insurance losses resulting from the death and injury of victims, incurred by tenants.
- Liability losses for claims due to inadequate fire prevention and evacuation procedures, incurred by building owners.
- Financial losses associated with the mortgage notes of various lenders and investors in mortgage-backed securities.

Terrorism risk insurance before the WTC attacks was included in “all-risk” policies at no added cost. Most policies include a standard “war exclusion” clause. Such exclusion clauses often refer to “declared” war by a “nation” or “sovereign state” but not to “terrorist action” or “terrorism.” Reference to the attacks as an “act of war” was inadvertently threatening to commercial property owners and lenders as it may have activated the war exclusion and released insurers from damage claims.

Property and Liability

In the case of property and liability insurance coverage for the buildings damaged in the attack, the principal claimant is the

building owner. The extent of the claim is dependent on several factors including the future rebuilding plans and the characterization of the incident. First, if the buildings are not rebuilt or repaired the insurer applies actual cash value rather than replacement cost. Actual cash value is defined as replacement cost minus physical depreciation. For older buildings like the WTC towers the loss recovery would be considerably less if they were not rebuilt.

Most property policies are written on an “occurrence” basis. That is, the full limit applies for each occurrence with no maximum aggregate. In the case of the WTC there were two airplanes that struck two buildings at different times, but they were all part of one terrorist attack. The difference between one event and two is about \$3.5 billion for the owner and the insurer. The specific definition of the terrorist event is of critical importance in terms of what is covered and what is excluded. Because terrorism risk is a new concern in the United States many of these definitions remain to be established and interpreted by the courts.

Business Interruption

Aside from physical damage or fire insurance there are other insurance questions that are closely associated with building performance and are of direct interest to building owners and tenants. Business interruption insurance, which covers lost business income and rental income, presents special problems for insurers, owners and lenders in the case of terrorist attack. Loss of income policies (generally included within a standard fire policy) are written by insurers either for a specified time period or on the basis of “actual loss sustained,” which requires insurers and owners or tenants to agree on actual losses. The scale of destruction at the WTC was probably considerably greater than anything anticipated by insurers or insured. It is very unlikely that reconstruction will be completed within the coverage period of most business interruption policies.

Problems also arise in the case of adjacent buildings. Usually, business loss is insurable if the building is first damaged by an in-

surable peril. Without such damage there is no coverage. In the case of the WTC many adjacent, undamaged buildings were evacuated by order of civil authorities. Evacuation in response to civil authority can be an excluded peril or covered for a limited time period. Denial of access without physical building damage, as in the case of bio-terrorist attack or radiological attack, is currently excluded from insurance coverage.

Workers' Compensation, Health, and Life

Workers' compensation insurance as well as group and private life and health insurance cover injured and deceased workers. Building owners and tenants must provide statutorily required workers' compensation cover for employees. Lenders must, in accordance with standard loan documents, verify that building owners and management companies carry workers' compensation insurance.

Most lenders and owners set up a single-purpose entity that holds the asset when a loan is made on a particular property. These entities typically do not have employees per se. Employees are usually legally employed in the owner's management company. Failure to carry sufficient workers' compensation coverage could affect all operations of the owner including the single purpose borrowing entity. Death and injury due to building failure resulting from terrorist attack can be a major financial concern for building owners, lenders and insurers, aside from the human cost.

Life insurance claims have been a significant source of insurance loss due to terrorist attack. Group benefits are typically a multiple of salary and most people carry individual insurance as well. These losses are directly associated with building failure in either structural or mechanical systems. Large group insurers are now careful to avoid concentration of exposure by restricting coverage at any one site or building.

Insurance Losses

Liability Losses. Based on past litigation it is likely that building owners can be held liable for contributing to the loss of life by failure to provide appropriate protective measures or direction in the case of evacuation. Facilities management is on the front line in managing terrorism risk and response in commercial buildings. Standards of acceptable practice are not yet available.

Financial Losses. Mortgage holders and investors are the subject of losses in the case of defaults caused by business failure resulting from terrorist attack. The WTC complex was controlled under a 99-year leasehold. A CMBS (commercial mortgage backed security) securitization was completed for part of the leasehold consideration paid to the owners of the WTC. Default insurance was not in place for the securitization. This means that investors in those securities could only indirectly depend on the traditional property and liability insurance to be collected by the leaseholder. Mortgage holders and investors in mortgage backed securities must be concerned with the vulnerability of the underlying asset. This vulnerability now includes terrorism risk. Terrorism risk evaluation and management is of particular importance for so-called 'trophy buildings' or buildings in close proximity to likely terrorist targets.

CURRENT INSURANCE SITUATION

Following the WTC attack the major burden of the property and liability loss was passed on to the major international reinsurers. In response to this unprecedented loss the major reinsurers excluded terrorism risk from their renewal treaties. This action in turn led direct insurers to file for exclusions for terrorism risk. The unavailability of terrorism risk insurance at feasible prices led to an insurance 'crisis' that particularly affected large-scale real estate and lending investment in what were perceived to be target cities.

Terrorism Risk Insurance Act of 2002

On November 26, 2002 the president signed into law a federal program that requires property and liability insurers in the United States to offer coverage for incidents of international terrorism, and reinsures a large percentage of that insured risk. PUBLIC LAW 107-297, the Terrorism Risk Insurance Act of 2002 (TRIA), produced some immediate effects on commercial insurance coverage and will continue as a significant feature of the domestic insurance market through 2005. See Appendix A for the full text of TRIA.

The Act addresses only a defined category of terrorism losses. An act of terrorism must be certified as such by the Secretary of the Treasury and must have the following characteristics:

- It must be a violent act or an act that is dangerous to human life, property, or infrastructure.
- It must have resulted in damage within the United States, or on the premises of any U.S. Mission abroad.
- It must have been committed by someone acting on behalf of a “foreign person or foreign interest, as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the U.S. Government by coercion.”
- It must produce property and casualty insurance losses in excess of \$5 million.

It is also important to note that chemical, biological, and radiological perils are excluded from terrorism risk cover.

Acts that might otherwise meet these criteria but that occur in the course of a declared war cannot be certified as acts of terrorism under the Act, except with respect to workers' compensation claims.

Participation and Reimbursements

Participation in the program is mandatory for all insurers covering commercial lines property and casualty insurance, including excess insurance, workers' compensation and surety.

Under TRIA, the federal government reimburses insurers for losses caused by terrorism, paying 90% of covered terrorism losses exceeding a deductible paid by the insurance companies. The deductible is prescribed by statute and phases in over several years based on an insurance company's earned premiums in the prior calendar year. The Act establishes a cap on annual liability of \$100 billion for both the government and insurance industry.

Coverage of claims is triggered when the Secretary of the Treasury, in concurrence with the Secretary of State and the Attorney General, certifies an event to be an "act of terrorism." A key element of terrorism is the involvement of a foreign interest, thus excluding acts of domestic terrorism, such as the Oklahoma City bombing. Also excluded from the definition of terrorism are acts committed in the course of war and losses under \$5 million.

Under TRIA, insurers are required to provide "clear and conspicuous" disclosure to policyholders of the premium charged for terrorism insurance. Existing terrorism exclusions are voided to the extent they would deny coverage for acts of terrorism as defined by the Act, unless the policyholder affirmatively declines terrorism coverage within 30 days of receiving the insurer's notice, or the policyholder fails to pay any additional premium required by the insurer.

Limitations

TRIA is an interim solution to the management of terrorism risk.

The act establishes a temporary federal program that provides for a transparent system of shared public and private compensation for insured losses resulting from acts of terrorism in order to:

1. Protect consumers by addressing market disruptions and ensure the continued widespread availability of property and casualty insurance for terrorism risk; and
2. Allow for a transitional period for the private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses, while preserving state insurance regulation consumer protections.

This law gives emphasis to the impact of terrorism risk on insurance and finance as well as on commercial building owners, and suggests the critical role that insurance, finance, and regulation will play in the adjustment to terrorism risk in the U.S.

The law assumes that the private insurance market for terrorism risk coverage will stabilize over the next three years and that property and casualty insurers will develop reliable models for pricing such insurance. While there have been signs of market pricing mechanisms developing, it is not clear that a period of three years will provide adequate time to resolve the issues associated with such a complex phenomenon. So far, the anecdotal evidence is that many property owners are not buying terrorism insurance post-TRIA.

INSURANCE RISK MANAGEMENT MODELS

The major loss modeling organizations have been quick to develop probabilistic terrorism insurance models. These models have typically begun with the general format of the loss estimation models developed for natural hazards such as earthquakes and hurricanes. The most significant challenge in terrorism modeling is the characterization of the hazard. Unlike the case of earthquakes or hurricanes, we do not have clear definitions of the phenomenon and we do not have hundreds of years of frequency/severity data.

Currently available terrorism insurance models cover the major recognized risk sources, including bomb blast, aircraft impact, and chemical, biological, nuclear, and radiological threats. Most

models set priorities for targets in all major cities and states and then simulate attacks with various types of weapons. The models include modeling of impact on adjacent buildings based on comprehensive national building inventories.

These models are intended to enable insurers and reinsurers to price and manage accumulated exposures to terrorism losses from multiple perils. The models claim to provide industry or portfolio-specific loss probability distributions, expected annual loss and scenario losses for workers' compensation and property exposures.

The models are very good at estimating loss from defined scenario events such as a given size blast at a given location. The critical weakness of all models to date has been the credibility of the hazard characterization. Typically the modelers have assembled teams of experts with backgrounds in national defense and domestic security. The ability to properly portray all of the potential terrorist events and their impact is central to the efficacy of a terrorism model. So far, this ability has not been convincing for the insurance industry or the real estate industry.

DATA NEEDS FOR INSURANCE

TRIA requires insurers to include terrorism risk cover, and then disclose the cost of the added coverage as a percentage of the total premium. So far the reported costs for terrorism risk as a percentage of the total premium range from 0% to 80% with many averaging 9% to 11%.

Most insurers charge 0% to 10% in order to avoid returning premiums to insureds at a later date when better information is available (and terrorism risk may be discounted). Some insurers are reportedly setting the level high, 20% to 50%, depending on how much terrorism risk coverage they want to write and the characteristics of the property (e.g., location, prominence, significance).

Lack of Actuarial Information

Actuaries are the key for insurance rate setting. Actuarial prediction of future losses is highly specialized and very influential. In the absence of data temporary solutions like TRIA will be necessary.

Without actuarial data it is not possible to set actuarially sound rates for insurance cover. It is equally not possible for insurance regulators to evaluate rates proposed by insurers. However, for terrorism risk to be an insurable risk there must be data. Models may be helpful in the interim but real data will take time to collect and will unfortunately result from more terrorist attacks.

FUTURE DEVELOPMENTS

Actions such as improved building standards and operational mitigation could result in reduced terrorism risk exposure for the public, building owners, and the insurance industry. Tools for the evaluation of building vulnerability to known terrorist threats, such as those discussed in Chapter 5, will allow for the determination of relative risk between buildings and for development of a risk hierarchy based on the physical and operational characteristics of individual properties. Development of standards of practice will also provide a useful baseline for determination of liability related to terrorist attack.

TERRORISM RISK THREAT TO LENDERS

The building finance community distinguishes between two major areas of lending activity: single-family residential and commercial/multifamily. The residential sector is less affected by terrorism risk considerations. However, since the WTC attack federal officials have issued specific warnings for elevated terrorism risk in shopping malls, banks, and multifamily housing.

This chapter discusses the potential retained risk that real estate lenders may be exposed to by the current condition of terrorism insurance. The specific intent of this chapter is to help the building finance community utilize its considerable influence on the building industry to encourage investments in terrorism risk mitigation.

Building Finance Community

While many owners are unwilling to make the extra expenditure now required for terrorism risk insurance, lenders prefer to require adequate cover for all relevant perils. To date, apartment lenders have taken the most relaxed view because it is most difficult for apartment owners to pass through the added insurance costs to tenants. Exposed owners might perceive risk, but most owners do not voluntarily want to pay for the insurance. Commercial building owners and lenders take a stricter view. They issue temporary waivers, but require insurance when loan balances are over a certain threshold (e.g., \$10 million) and for trophy properties or properties that are identified as having higher risk due to location, building tenant, or historic/national recognition.

Each sector consists of its own array of financial interests:

- Loan originators
- Loan servicers
- Secondary markets
- Bond markets

The commercial/multifamily sector includes: loan originators, loan servicers, life insurance companies, pension funds, the multifamily secondary market (Fannie Mae and Freddie Mac), Wall Street, and financial institutions as direct lenders.

Lenders Concerns

Building lenders and loan servicers are concerned about the adequacy of property insurance to cover potential loss of the asset and the potential default of the borrower. Lenders are also concerned with other types of insurance—workers' compensation, liability, and business interruption—as they relate to the solvency of the borrower.

Both assets and borrower solvency are threatened by terrorism risk. The terrorist acts of September 11, 2001 resulted in pervasive uncertainty in the insurance markets regarding insurance associated with future terrorist attacks. The commercial/multi-family real estate industry is very concerned about the availability of terrorism risk coverage as it relates to the asset value and financial health of borrowers. The Terrorism Risk Insurance Act of 2002 ensures the current availability of basic terrorism insurance, but significant questions remain as to the comprehensiveness of the coverage and whether a viable terrorism insurance market will develop in the future.

Terrorism Impact

The potential impact of terrorism risk for the real estate finance industry lies in six key areas:

Loss of asset (collateral). The traditional approach to asset risk on the part of lenders is to require the borrower to purchase adequate insurance cover for all relevant perils. The terrorism risk exclusions following the WTC attack presented a major problem for lenders. Their profit is based on extending more loans but without insurance cover new loans also expand their credit risk.

Default of borrower. The primary concern of the lender is the ability of the borrower to meet the conditions of the loan. Protection of the underlying asset is of key importance to maintaining the business operation of the borrower in addition to providing collateral for the loan. Terrorism risk includes modes of attack that will directly damage the building such as bomb blast and arson as well as those that may not physically damage the building such as biological, chemical, or radiological attack. Such 'non-

building' threats can destroy the borrowers ability to pay and can deny access to the asset for extended periods of time. Even without physical damage, asset value can be destroyed.

Rating of securities. In the case of mortgage backed securities for both residential and commercial real estate the value of the security is influenced by the evaluation of rating agencies. These ratings take into account a range of risks, which will necessarily include terrorism risk. The exposure of the underlying assets to terrorist attack and the extent of related insurance coverage will influence securities ratings. Perception of portfolio risk affects rating of securities: securities based on a single asset in a "high risk" location will receive a lower rating. Securities based on multiple or dispersed assets are generally less negatively affected by terrorism risk. Aside from New York City and Washington DC, the cities of greatest concern for terrorism are Los Angeles, Seattle, Chicago, Houston, and Atlanta.

Retained risk. In the aftermath of the WTC attack and the terrorism risk exclusions, many lenders chose to temporarily waive insurance requirements. This action was deemed necessary to continue real estate financing and to foster new construction in the economy. However, waiving the terrorism insurance requirement left the lenders exposed to an as yet undefined risk.

Lenders have traditionally relied on the insurance industry to price and provide coverage for such risks. In this case the lack of consensus on terrorism risk pricing and the withdrawal of the reinsurance industry have left lenders in an awkward position. Even with TRIA, lenders remain concerned with risks related to domestic terrorism, attacks involving chemical, biological, or radiological materials and the designation of terrorism events by the Secretary of the Treasury.

Cost of capital. One approach to dealing with increased risk has been to "cover" the risk with increased interest rates. This increase in the cost of capital is not desirable because it impacts the volume of lending and who receives a loan if terrorism is not covered or the cost is prohibitive.

Regulation. Financial institutions and lending institutions are subject to regulation regarding standards for lending and management of risk, including terrorism risk. Banks and financial institutions must meet the regulatory standards of the Comptroller of the Currency and the Securities and Exchange Commission.

CURRENT FINANCE SITUATION

Following the WTC attack and the withdrawal of the insurance industry from provision of terrorism risk cover, real estate finance institutions faced a serious dilemma. In the absence of available or reasonably priced reinsurance, investments and lending in major projects (those over \$30 – \$50 million) were delayed in what were believed to be the primary target cities of New York and Washington. Difficulty in acquiring insurance for recognized trophy buildings also impacted refinancing in some cases.

The key concern for lenders is borrower insurance coverage, so they also have a keen interest in the TRIA. The continued health of the real estate sector of the economy requires adequate and affordable property and liability insurance coverage against terrorism risk. The enactment of TRIA is an important milestone for the real estate finance industry because it ensures the availability of basic insurance coverage. However, the real estate finance industry has several serious concerns with the federal program created under the statute:

- Acts of domestic terrorism are not covered.
- It is not clear whether or how carriers will cover terrorist acts with aggregate losses below \$5 million that are not reinsured under TRIA.
- Carriers are not required to notify lenders if a borrower rejects coverage under TRIA, either by affirmative statement or by failing to pay any premium for such coverage imposed by the carrier.

- Carriers are not required to offer terrorism coverage for nuclear, chemical or biological attacks if they do not typically offer property and liability insurance for nuclear, chemical and biological perils.

Following TRIA, lenders have many borrowers out of compliance with loan insurance requirements. Lender and servicer procedures vary. Some large servicers have instituted a requirement for mandatory terrorism risk coverage.

Following TRIA there have been limited reports of substantial premium increases, particularly in Manhattan and Washington DC. For the most part post-TRIA rate increases for required terrorism risk coverage have been in the 0% – 10% range, but some have been much higher.

The terrorist threat is a dynamic phenomenon. Government and commercial response to the threat is also dynamic in ways independent of the underlying phenomenon. For these reasons change is inevitable. More experience is needed to understand the nature of the threat and more time is needed to understand the implications of market and policy responses to the threat.

Key real estate finance industry associations suggest that several factors must be monitored over time:

- The Department of the Treasury rule-making process for TRIA relating to the acceptance and rejection of terrorism risk insurance by owners, and the availability of insurance for acts of terrorism not covered by TRIA.
- The declining financial strength ratings for some insurers that have produced difficulties for borrowers in obtaining coverage that complies with underlying loan documents.
- The development of a useable insurance certificate that provides an accurate and comprehensive summary for lenders and servicers of the coverage afforded by the underlying insurance policy.

What happens after TRIA? It is important to see if the insurance market for terrorism risk cover does in fact stabilize over the three year period stipulated in the Act. If the market does not find an acceptable means to price terrorism risk there may need to be a longer term federal role in this area.

LENDER RISK MANAGEMENT MODELS

As mentioned above the traditional practice of lenders has been to rely on required insurance purchase by borrowers of adequate cover for relevant perils. The breakdowns in terrorism insurance availability and risk pricing by insurers have necessitated the temporary intervention of the federal government pending the stabilization of the insurance market. Lenders are dependent on the insurance industry to transfer terrorism risk. In lieu of an insurance solution the real estate finance industry will have to consider alternative approaches to terrorism risk management. These may include addressing questions of risk identification and risk reduction directly. Tools for the assessment of terrorism vulnerability of specific buildings may be developed and introduced into the standard process of due diligence and property condition assessment, as discussed further in Chapter 5.

Each sector of the real estate finance industry (originators, servicers, secondary markets, and bond markets) may assess its exposure to terrorism risk in a particular way. Useful analogies may be found in considering how these sectors address other building risks, such as natural disasters and environmental hazards.

Each sector of the real estate finance industry should also consider terrorism risk in relation to the risks traditionally covered by the various lines of insurance.

As standards for building siting, construction, and property management are developed to address terrorism risk reduction, it will become possible for both insurers and lenders to rate buildings in terms of their exposure to terrorism.

FUTURE DEVELOPMENTS

The real estate finance industry needs tools for the evaluation of building vulnerability and for the evaluation of physical and operational measures for risk reduction. These include:

- Rapid screening methods for the evaluation of portfolios of properties
- Detailed guidelines for due diligence on individual buildings
- Legally accepted standards for risk reduction measures and management practices related to terrorism risk

TERRORISM RISK FOR REGULATORS

Following the attack of September 11, 2001 the definition of building hazards in the United States has changed to include intentional attack. Protection of civilian population from acts of terrorism has become a major national priority.

Though historically focused on fire safety, the building regulatory system does address natural disaster mitigation (floods, earthquakes, windstorms, snow storms), some man-made risks (e.g., HAZMAT storage), and specific societal goals (energy conservation, accessibility). The regulation of all these areas is supported by well-established and accepted reference standards, regulations, inspection and assessment techniques, plan review methods, and quality control.

This chapter discusses terrorism risk as it relates to the building regulatory system. It is intended to provide information to building regulators in four categories, zoning, property maintenance, building rehabilitation, and building construction, so that they can initiate the process of developing regulations that will mandate cost-effective building investments in terrorism risk mitigation.

Regulation of Terrorism Risk

For a similar regulation of building-related terrorism risks, it will have to be shown that the development and implementation of such tools will be cost-effective. Some jurisdictions require rigorous cost/benefit analyses to support regulatory change. These determinations will require an understanding by the regulatory authorities of the potential occurrences and damages related to terrorism risk.

Balancing Stakeholder Interests

The codes and standards development process, involves thorough review and balloting by all interested stakeholder groups. This consensus process provides for the balance of diverse commercial and social priorities. It has the advantage that once a regulation or standard is promulgated it is likely to be widely accepted and used. It is thus an effective change lever. However, the consensus process is time consuming.

Implications for Building Regulation Enforcement

Zoning and planning regulation define land use, building density, transportation systems, and utility systems. They are usually

adopted by local governments, but state planners may provide guidance. For existing vulnerable properties, these regulations can address specific access-control measures. This will require a prioritization of hazards and buildings. For future developments, these regulations can, at the extreme, result in commercial development resembling military installations. How should such a decision be made when zoning and planning at the local level is the most political of the building regulatory processes?

Property maintenance codes govern the use and maintenance of existing buildings. Housing codes and fire codes are two examples. They are developed by model code and consensus standards organizations and adopted as regulations by local government agencies. These can be effective at addressing all building vulnerabilities. They will require extensive inspections, and enforcement will be burdensome unless targeted to highly prioritized vulnerabilities, and accompanied by financial incentives.

Building rehabilitation codes address health, safety, and welfare in existing buildings that are undergoing voluntary improvements. These are a relatively new development. They have been enacted by some state or local government agencies. These can be effective at addressing vulnerabilities in existing buildings in which rehabilitation investments are otherwise being made. They should be carefully calibrated, since these codes all have the objective of "encouraging the reuse of existing buildings" rather than risk reduction.

Construction codes (building, mechanical, plumbing, electrical) address health, safety, and welfare in new buildings. They are developed by model code organizations (ICC, NFPA) and adopted as regulations by state or local government agencies. Rarely does the federal government regulate construction requirements. Two recent examples of federal regulation are the Americans with Disabilities Act (ADA) enforced by the Dept. of Justice and the Fair Housing Act enforced by the Dept. of Housing and Urban Development. Construction codes can be effective at addressing the problem of vulnerability at its margin, that is, new buildings

to be built. Unlike the preceding three categories of regulation, these may be the easiest to accomplish ("words on paper are cheap compared to bricks and mortar in place"). However, many jurisdictions may require cost/benefit analysis to justify even these regulations.

CURRENT BUILDING REGULATION SITUATION

Current codes are effective at mitigating the effects of fire and, as discussed above, natural disasters. They also regulate aspects of indoor air quality and the installation of mechanical, plumbing, electrical, and communication systems.

Code Relation to Terrorist Threats

Bomb blast is not addressed in the codes, but some of the earthquake and windstorm provisions in the building codes may have a beneficial effect on mitigation of this hazard. Code-regulated earthquake design requires the building's structural system to have toughness, ductility, and redundancy, all of which may also contribute to the mitigation of blast effects. Code-regulated hurricane design requires the fenestration to resist the effects of impact of windborne debris, which may also mitigate the hazards of glass in explosions.

Progressive collapse, which is one of the effects of blast (but not the only one), is discussed in The American Society of Civil Engineers standard, ASCE 7 (the structural loads standard referenced in building codes). Some qualitative guidance is provided, but no design criteria are specified. ASCE 7 and the American Concrete Institute standard, ACI 318 (the reinforced concrete design standard reference in building codes) have references to structural integrity but not as a set of criteria for resisting progressive collapse.

Chemical, biological, and radiological agents are not addressed in the codes, but certain details of the design of building heating, ventilating, and air conditioning (HVAC) systems, as regulated by mechanical codes, may mitigate the effects of these agents.

Armed attack may be addressed to a limited extent insofar as the codes regulate the design and construction of correctional facilities, but the phenomena of incarceration and of terrorist attack are quite different in many respects.

Regulatory Activities Related to Terrorism Risk

The Federal Emergency Management Agency (FEMA) has published *The World Trade Center Building Performance Study* "to examine the damage caused by these events, collect data... and identify studies that should be performed."

The New York City Department of Buildings, soon after the WTC attack, initiated an effort to analyze the code as it relates to terrorist threat. In February 2003, the task force issued a report of findings and 21 specific recommendations for code, code administration, and code enforcement changes.

The American National Standards Institute (ANSI) established a Homeland Security Standards Panel (HSSP) in February 2003, in response to The National Strategy for Homeland Security. The proposed mission of the HSSP is to catalog, promote, accelerate and coordinate the timely development of consensus standards within the national and international voluntary standards system intended to meet identified Homeland Security needs, and communicate the existence of such standards appropriately to governmental units and the private sector.

The National Fire Protection Association (NFPA), a standards organization active in the field of fire safety, established a committee on Premises Security before 9/11. It plans to produce two standards by 2005: NFPA 730, *Guide to Premises Security*; and NFPA 731, *Security System Installation Standard*.

The American Society for Testing and Materials (ASTM), a standards organization active in the field of materials, specifications, and test methods, many of which are referenced in building codes, is considering the creation of a Homeland Security Committee, or Subcommittee.

The American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE), a standards organization active in the field of mechanical systems and indoor air quality in buildings, may initiate activities addressing chemical and biological agents in buildings.

The American Society of Mechanical Engineers (ASME), a standards organization active in the field of boilers & pressure vessels, elevators, and other building equipment, has developed a program of seminars for engineers entitled “Strategic Responses to Terrorism,” which cover a range of topics including biological and chemical terrorist attacks.

The National Institute of Standards and Technology (NIST) is conducting an extensive review and analysis of the WTC collapse. It is anticipated that it will lead to code changes related to structural safety and fire safety in high-rise buildings.

The General Services Administration (GSA) published PBS-PQ100.1, *Facilities Standards for the Public Buildings Service*, June 14, 1996. Chapter 8, Security Design, contains building design criteria for blast resistance, progressive collapse, and chemical, biological and radiological attack. These criteria cover the design and construction of all GSA buildings, and will be applied to all government-leased buildings as well.

The Department of Defense (DoD), has a similar standard to GSA's entitled *Unified Facilities Criteria, DoD Minimum Antiterrorism Standards for Buildings*, UFC 4-010-01, 31 July, 2002.

BUILDING REGULATION MANAGEMENT MODELS

The four categories of building regulations, zoning, property maintenance, building rehabilitation, and building construction, have the potential, between them, to address all the physical aspects of terrorism risk, including common terrorist tactics and delivery systems as well as terrorist attack devices. Development of a specific typology that allocates specific risks to the specific regulation requires additional analysis. Table 4-1 is a matrix that can be used to begin this analysis.

In order to implement changes in the building regulatory system to address terrorism risk, it is important to recognize that there are four ways that regulatory change can take place:

- Federal preemption
- State mandate or preemption
- Local prerogative
- Model code and voluntary standards

Initiation of changes in each of the four categories of building regulations must be carefully analyzed for political acceptability and the availability of resources.

FUTURE DEVELOPMENTS

Development of codes and standards to deal with terrorism risk in both new and existing buildings will require broad acceptance of the character of the risk and the effectiveness of the mitigation measures as well as some form of societal cost/benefit assessment.

Table 4-1: Building Regulation Applicability to Terrorist Tactics and Threats/Hazards

Common Tactics	Zoning	Property Maintenance	Rehab	Construction
ATTACK DELIVERY				
Ballistic weapons				
Covert entry	●	●	●	●
Mail			●	●
Moving vehicle	●			
Stand-off weapons	●		●	●
Stationary vehicle	●	●	●	●
Supplies		●	●	●
ATTACK MECHANICS				
Airborne		●	●	●
Blast effects		●	●	●
Waterborne		●	●	●
THREATS/HAZARDS				
Armed attack		○	●	●
Arson/incendiary		●	●	●
Biological agent		●	●	●
Chemical agent		●	●	●
Conventional bomb	●	●	●	●
Cyber-terrorism			○	○
HAZMAT release	○	●	●	●
Nuclear device				○
Radiological agent		○	○	○
Surveillance				
Unauthorized entry				

LEGEND: ● = Applicability to designated type of regulation. ○ = Possible applicability.

FUNDAMENTAL CHANGES

Vulnerability assessment methodologies developed by DoD and other federal agencies are currently the best available resources for terrorism risk assessment. In order for these resources to be feasible and relevant in commercial buildings, they must be significantly simplified and civilianized.

This chapter provides basic information on the current state of knowledge on the terrorist threat and measures to reduce vulnerability to that threat in commercial buildings. An initial vulnerability estimate process and checklist is proposed. Insurers, lenders, and owners can apply this information to encourage investments in terrorism risk mitigation.

Bringing government experience and expertise regarding terrorism risk and building security to the commercial sector will involve two fundamental changes in the way buildings are designed, managed, and operated, and in the way that due diligence is used to evaluate existing buildings for acquisition or refinancing.

First, businesses will need to carefully evaluate functional aspects of their operations in order to prioritize security requirements. Second, tradeoffs will be required in the level of security provided to ensure continued viability of business operations.

Reducing vulnerability to terrorist threat will involve both physical measures to modify a facility and operational changes. Mitigation will consist mainly of measures to thwart tactics that terrorists might use in attacking organizations and facilities.

DUE DILIGENCE ASSESSMENT OF VULNERABILITY TO TERRORIST ATTACK

Due diligence procedures are employed to assess valuations for property acquisition or financing and to identify risks related to the deal. Such procedures may also be used as part of insurance underwriting. Due diligence often includes both detailed property inspection and rigorous audits of available financial and construction documentation. At the same time, due diligence is a highly specialized field requiring both expertise and extensive prior experience to render sound judgments and recommendations to decision makers.

A Property Condition Assessment (PCA) is used (at levels of detail and rigor appropriate to the investment being considered) as part of due diligence to help make prudent investment decisions. The assessment consists of analysis and assessment of physical conditions of a property by an on-site inspection and review of available construction and operations documentation. Investigators use professional judgment to identify items needing further expert investigation and those that can be readily evaluated by inspection.

Vulnerability to terrorist attack should become a distinct element of due diligence condition assessments in the future. Professionals conducting property condition assessments of vulnerability to terrorist attack must have competency in building systems, operations, and security disciplines.

For terrorism risk and security concerns, a due diligence assessment should also include a property condition assessment investigation of operational procedures and the vulnerability of those procedures to terrorist attack.

MITIGATION OF VULNERABILITY

Strategies for reducing exposure to terrorism risk may be in the form of operational actions or construction projects (either new or existing building renovation). They could include reorganization of land uses, reorientation of roadways, security improvements to site entries, and improvements to the facility, including the existing structure and surrounding site area. For some strategies, the process may include the identification of multiple scenarios, or alternatives, for achieving the desired goal.

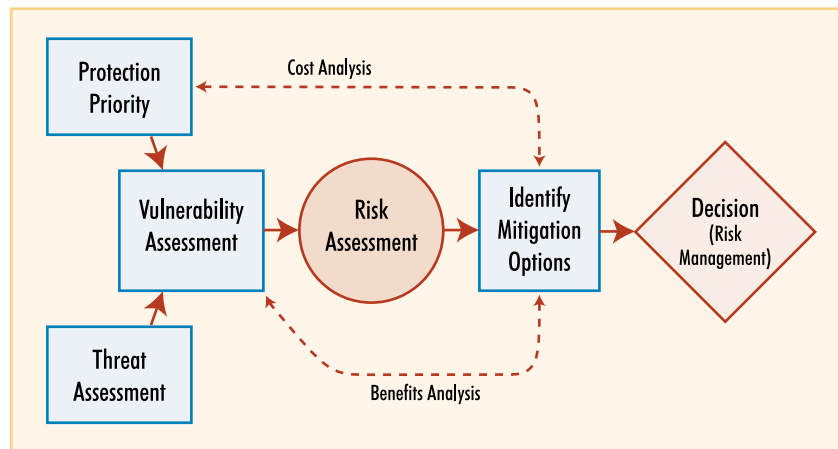
PROCESS MODEL FOR TERRORISM RISK REDUCTION USED IN FEDERAL FACILITIES

United States military services and government agencies have long been involved in assessing vulnerabilities and protecting facilities, especially for off-shore installations. Terrorism and

terrorist attack have been a part of the assessment of threat and vulnerability of government facilities for several decades.

While each government agency has used its own procedures, the general approach has been elaborated and presented in FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*.

Figure 5-1: The Terrorism Risk Reduction Process Model



The terrorism risk reduction process starts with establishment of protection priorities and proceeds to assessment of threats, both providing information to a vulnerability assessment. The vulnerability assessment in turn leads to identification of mitigation options and risk management decisions based on a comparative evaluation of risk, liabilities, and mitigation costs and benefits.

PROTECTION PRIORITY

The first step of the process to assess risk to terrorist attack is to identify the relative importance of the people, business activities, goods, and facilities involved in order to prioritize security actions. This applies to both new and existing facilities. Three actions are recommended in accordance with FEMA 426:

- Define and understand the core functions and processes of the business or institutional entity.

- Identify critical business infrastructure:
 - Critical components (people, functions, and facilities)
 - Critical information systems and data
 - Life safety systems and safe haven areas
 - Security systems
- Assign a relative protection priority, as simple as high, medium, or low, to the occupants, business functions, or physical components of the facility (note that FEMA 426 describes a 9-step scale of values for describing asset values; the 3-step variation presented here is a simplified process):
 - **High Priority.** Loss or damage of the facility would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time.
 - **Medium Priority.** Loss or damage of the facility would have moderate to serious consequences, such as injuries, or impairment of core functions and processes.
 - **Low Priority.** Loss or damage of the facility would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.

THREAT ASSESSMENT

Military experience indicates that the terrorist threat is from people with the intent to do harm, who are known to exist, have the capability for hostile action, and have expressed the intent to take hostile action.

Threat assessment is a continual process of compiling and examining information concerning potential threats. Information should be gathered from all reliable sources. The assessment process consists of:

- Defining threats

- Identifying likely threat event profiles and tactics

Defining Threats

Defining threats involves analysis of information regarding terrorist existence, capability, history, intention, and targeting:

- **Existence** is the assessment of who is hostile to the organization, or community of concern.
- **Capability** is the assessment of what weapons have been used in carrying out past attacks.
- **History** is the assessment of what the potential terrorist has done in the past and how many times.
- **Intention** is the assessment of what the potential terrorist hopes to achieve.
- **Targeting** is the assessment of the likelihood a terrorist (the specific one may not be known) is performing surveillance on the particular facility, nearby facilities, or facilities that have much in common with the particular organization.

The Homeland Security Advisory System is a color-coded hierarchy of threat conditions. The threat level for a specific business facility could be similarly developed in coordination with local law enforcement, intelligence, and civil authorities.

Table 5-1: Homeland Security Advisory System Related to Threat Analysis Factors

Threat Conditions	Threat Analysis Factors				
	Existence	Capability	History	Intention	Targeting
Severe (Red)	●	●	●	●	●
High (Orange)	●	●	●	●	○
Elevated (Yellow)	●	●	●	○	
Guarded (Blue)	●	●	○		
Low (Green)	●	○			

LEGEND: ● = Factor must be present. ○ = Factor may or may not be present.

Adapted from the Commonwealth of Kentucky Office of Homeland Security.

Identifying Likely Threat Event Profiles and Tactics

Identifying the likelihood of specific threats and tactics involves evaluation of attack intentions, hazard event profiles, and the expected effects of an attack on the facility and organization. Table 5-2, based on FEMA 426, presents general event profiles for a range of possible forms of terrorism attack. The profiles describe the mode, duration, and extent of the effects of an attack, as well as mitigating and exacerbating conditions that may exist. These and more specific descriptions can be used to identify threats of concern to individual organizations. (Potential threats are listed in alphabetical order in the table.)

Table 5-2: Event Profiles For Terrorism and Technological Hazards

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Agriterrorism	Direct, generally covert contamination of food supplies or introduction of pests and/or disease agents to crops and livestock.	Days to months.	Varies by type of incident. Food contamination events may be limited to discrete distribution sites, whereas pests and diseases may spread widely. Generally no effects on built environment.	Inadequate security can facilitate adulteration of food and introduction of pests and disease agents to crops and livestock.
Armed Attack - Ballistics (small arms) - Stand-off weapons (rocket propelled grenades, mortars)	Tactical assault or sniping from remote location.	Generally minutes to days.	Varies, based upon the perpetrators' intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Arson/Incendiary Attack	Initiation of fire or explosion on or near target via direct contact or remotely via projectile.	Generally minutes to hours.	Extent of damage is determined by type and quantity of device /accelerant and materials present at or near target. Effects generally static other than cascading consequences, incremental structural failure, etc.	Mitigation factors include built-in fire detection and protection systems and fire-resistive construction techniques. Inadequate security can allow easy access to target, easy concealment of an incendiary device and undetected initiation of a fire. Non-compliance with fire and building codes as well as failure to maintain existing fire protection systems can substantially increase the effectiveness of a fire weapon.
Biological Agents - Anthrax - Botulism - Brucellosis - Plague - Smallpox - Tularemia - Viral hemorrhagic fevers - Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins)	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents but higher winds can break up aerosol clouds; the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Chemical Agents <ul style="list-style-type: none"> - Blister - Blood - Choking/lung/pulmonary - Incapacitating - Nerve - Riot control/tear gas - Vomiting 	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/containers; or munitions.	Chemicals agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation of liquids. Humidity can enlarge aerosol particles, reducing inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target are to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place can protect people and property from harmful effects.
Conventional Bomb <ul style="list-style-type: none"> - Stationary vehicle - Moving vehicle - Mail - Supply - Thrown - Placed - Personnel 	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the time duration of the hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Energy decreases logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc., can provide shielding by absorbing and/or deflecting energy and debris. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
Cyberterrorism	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
<p>Hazardous Material Release (fixed facility or transportation)</p> <ul style="list-style-type: none"> - Toxic Industrial Chemicals and Materials (Organic vapors: cyclohexane; Acid gases: cyanogens, chlorine, hydrogen sulfide; Base gases: ammonia; Special cases: phosgene, formaldehyde) 	Solid, liquid, and/or gaseous contaminants may be released from fixed or mobile containers.	Hours to days.	Chemicals may be corrosive or otherwise damaging over time. Explosion and/or fire may be subsequent. Contamination may be carried out of the incident area by persons, vehicles, water, and wind.	As with chemical weapons, weather conditions will directly affect how the hazard develops. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place can protect people and property from harmful effects. Non-compliance with fire and building codes as well as failure to maintain existing fire protection and containment features can substantially increase the damage from a hazardous materials release.
Nuclear Device	Detonation of nuclear device underground, at the surface, in the air or at high altitude.	Light/heat flash and blast/shock wave last for seconds; nuclear radiation and fallout hazards can persist for years. Electromagnetic pulse from a high-altitude detonation lasts for seconds and affects only unprotected electronic systems.	Initial light, heat and blast effects of a subsurface, ground or air burst are static and are determined by the device's characteristics and employment; fallout of radioactive contaminants may be dynamic, depending on meteorological conditions.	Harmful effects of radiation can be reduced by minimizing the time of exposure. Light, heat, and blast energy decrease logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc., can provide shielding by absorbing and/or deflecting radiation and radioactive contaminants.
<p>Radiological Agents</p> <ul style="list-style-type: none"> - Alpha - Beta - Gamma 	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Surveillance - Acoustic - Electronic eavesdropping - Visual	Stand-off collection of visual information using cameras or high powered optics, acoustic information using directional microphones and lasers, and electronic information from computers, cell phones, and hand-held radios. Placed collection by putting a device "bug" at the point of use.	Usually months.	This is usually the prelude to the loss of an asset. A terrorist surveillance team spends much time looking for vulnerabilities and tactics that will be successful. This is the time period that provides the best assessment of threat as it indicates targeting of the facility.	Building design, especially blocking lines of sight and ensuring the exterior walls and windows do not allow sound transmission or acoustic collection, can mitigate this hazard.
Unauthorized Entry - Forced - Covert	Use of hand or power tools, weapons, or explosives to create a man-sized opening or operate an assembly (such as a locked door), or use false credentials to enter a building.	Minutes to hours, depending upon the intent.	If goal is to steal or destroy physical assets or compromise information, the initial effects are quick, but damage may be long lasting. If intent is to disrupt operations or take hostages, the effects may last for a long time, especially if injury or death occurs.	Standard physical security building design should be the minimum mitigation measures. For more critical assets, additional measures, like closed circuit television or traffic flow that channels visitors past access control, aids in detection of this hazard.

Assigning a Threat Rating

The ultimate product of a threat assessment is the assignment of a *threat rating* to each hazard of concern to a particular organization. The threat rating, like *protection priority*, is based on expert judgment and may be as simple as high, medium, or low.

- **High Threat.** Known terrorists or hazards, capable of causing loss of or damage to a facility exist. One or more vulnerabilities are present and the terrorists are known or reasonably suspected of having intent to attack the facility.
- **Medium Threat.** Known terrorists or hazards that may be capable of causing loss of or damage to a facility exist. One or

more vulnerabilities may be present. However, the terrorists are not believed to have intent to attack the facility.

- **Low Threat.** Few or no terrorists or hazards exist. Their capability of causing damage to a particular facility is doubtful.

An organization may reasonably be concerned only with high threat ratings in the near term, but may want to consider addressing medium threats over time.

Alternative: Assigning a Level of Protection Against Threat

In the absence of experience, assessing terrorist threat is the most difficult aspect of planning to resist terrorist attack. An effective alternative approach may be to select a level of desired protection for a business operation based on management decision-making, and then proceed to a vulnerability assessment. The Department of Defense correlates *levels of protection* with potential damage and expected injuries. The GSA and Interagency Security Committee (ISC) also use the level of protection concept, though the definitions differ slightly. The following levels are based on DoD definitions:

- **High Protection.** Facility superficially damaged; no permanent deformation of primary and secondary structural members or non-structural elements. Only superficial injuries are likely.
- **Medium Protection.** Damaged, but repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Some minor injuries, but fatalities are unlikely.
- **Very Low Protection.** Heavily damaged, onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities.

Note that the ‘very low’ level is not the same as doing nothing. No action could result in catastrophic building failure and high loss of life.

VULNERABILITY ASSESSMENT

A terrorism vulnerability assessment evaluates any weaknesses that can be exploited by a terrorist. It evaluates the vulnerability of facilities across a broad range of identified threats/hazards and provides a basis for determining physical and operational mitigation measures for their protection. It applies both to new building programming and design and to existing building management and renovation over the service life of a structure.

The useful product of a vulnerability assessment is the assignment of a *vulnerability rating* of all appropriate aspects of building operations and systems to the defined threats for the particular facility. As with protection priority and threat ratings, vulnerability can be cast as high, medium, or low.

- **High Vulnerability.** One or more significant weaknesses have been identified that make the facility highly susceptible to a terrorist or hazard.
- **Medium Vulnerability.** A weakness has been identified that makes the facility somewhat susceptible to a terrorist or hazard.
- **Low Vulnerability.** A minor weakness has been identified that slightly increases the susceptibility of the facility to a terrorist or hazard.

The Building Vulnerability Assessment Checklist, presented in abbreviated form in Appendix B, compiles a comprehensive list of questions to be addressed in assessing the vulnerability of facilities to terrorist attack. A subset of the checklist, discussed in the following section, is particularly useful in the initial screening of existing facilities to identify and prioritize terrorism risk reduction needs. Such an assessment can be integrated into a due

diligence assessment associated with acquisition, refinancing, or insurance underwriting.

INITIAL VULNERABILITY ESTIMATE

Because of the uncertainty of the threat, many insurers, lenders, and owners need a quick, qualitative assessment of the vulnerability of existing buildings to terrorist attack. As experience is gained and more robust vulnerability assessment tools are developed, the rigor of data collection and analysis will increase. For now, the estimate of vulnerability to a simple qualitative scale (high, medium, or low as defined by the vulnerability ratings described above) may provide useful information.

Answering even basic questions concerning vulnerability to terrorist attack may involve three means of data collection:

- Visual inspection
- Document review
- Organization and management procedures review

Visual Inspection

A property condition assessment of vulnerability to terrorist attack includes an onsite visual inspection encompassing evaluation of the site and all facility systems including architectural, structural, building envelope, utility, mechanical, plumbing and gas, electrical, fire alarm, communications and information technology systems. Equipment operations and maintenance procedures and records and security systems, planning, and procedures should also be scrutinized. The investigation may need to go beyond the site to vulnerability of utility and other infrastructure systems.

"There are no universal solutions to preclude terrorist attacks, since the threat is largely unpredictable and certainly will change over time."

(Installation Force Protection Guidelines, USAF)

"No matter how many measures are implemented risk is always present."

(Structural Engineering Guidelines for New Embassy Office Buildings, U.S. Department of State, Bureau of Diplomatic Security)

Design Documents Review

The on-site inspection team should work with the property owner to obtain plans, specifications and related construction documents as necessary. Equipment operation and maintenance procedures and records as well as security procedures should also be scrutinized. All documents should be reviewed assessing concerns related to terrorism vulnerability.

Organization and Management Procedures Review

Because of the transitory nature of the terrorist threat and its uncertain duration, the most effective approaches to terrorism risk reduction in facilities may emphasize reorganization of operational functions and procedures rather than modification of physical systems. The vulnerability assessment team must scrutinize business and operational practices to identify opportunities to reduce exposure to attack. This will involve scrutinizing both owner and tenant operations at the building site.

Assessment of Vulnerability to Expected Methods and Means of Attack

Each building system and business procedure should be assessed on its vulnerability to a range of terrorist attack methods and means.

Based on military experience, common terrorist tactics include the use of moving or stationary vehicles, covert entry, and/or disguise in mail or shipping materials to deliver destructive weapons.

At present, terrorist attacks might include blast effects, airborne contamination, waterborne contamination, or some combination of attack mechanisms. For additional information, see FEMA 426 and FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*.

VULNERABILITY ESTIMATE SCREENING

The following screening tool tables provide guidance for initial vulnerability assessment. The intention of this assessment is to distinguish facilities of high, medium, or low vulnerability to terrorist attack. The implication is that high vulnerability facilities should receive more detailed analysis. Specific strategies for risk reduction should be developed.

These quick, qualitative 'vulnerability estimate' questions were selected from the Building Vulnerability Assessment Checklist in FEMA 426. Each question is characterized by how information concerning the question will likely be collected (visual inspection, design documentation, and/or review of organizational/management procedures), and common terrorist attack tactics (delivery by moving, stationary vehicles, or covert entry, disguised in the mail or in supply materials; and blast pressure, airborne, or waterborne attack mechanisms).

For this initial assessment, subjective ratings by qualified professionals familiar with the facility are appropriate. Assigning a "high, medium, or low" vulnerability rating to the responses to vulnerability questions for each building system will provide a solid preliminary basis for estimating the overall vulnerability of a particular facility to terrorist attack. The answers to the questions will also indicate areas of opportunity for mitigation actions to reduce terrorism risk.

'Site' Questions

A vulnerability assessment of the 'Site' will look at surrounding structures, terrain, perimeter controls, traffic patterns and separations, landscaping elements and features, lines of site, etc.

'Site' questions focus primarily on visual inspection to develop ratings. The questions emphasize vulnerability to moving vehicle, stationary vehicle, and covert entry tactics. Vulnerability to blast is the primary concern addressed.

Table 5-3a: FEMA 'Site Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What major structures surround the facility?	□	●	●									
What critical infrastructure, government, military, or recreation facilities are in the local area that impact transportation, utilities, and collateral damage (attack at this facility impacting the other major structures or attack on the major structures impacting this facility)?	□	●	●	●								
What are the adjacent land uses immediately outside the perimeter of this facility?	□	●	●									
What are the site access points to the facility?	□	●			●		●					
What is the minimum distance from the inspection location to the building?	□	●			●		●			●		
Is there any potential access to the site or facility through utility paths or water runoff?	□	●	●				●					
What are the existing types of vehicle anti-ram devices for the facility?	□	●			●					●		
What is the anti-ram buffer zone standoff distance from the building to unscreened vehicles or parking?	□	●			●							
Are perimeter barriers capable of stopping vehicles?	□	●	●		●							
Does site circulation prevent high-speed approaches by vehicles?	□	●			●							
Is there a minimum setback distance between the building and parked vehicles?	□	●				●				●		
Does adjacent surface parking maintain a minimum standoff distance?	□	●				●				●		
Do site landscaping and street furniture provide hiding places?	□	●					●					

LEGEND: □ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Architectural' Questions

Assessing 'Architectural' vulnerability will investigate tenancy, services, public and private access, access controls, activity patterns, exposures, etc.

'Architectural' questions focus equally on visual inspection and evaluation of organizational and management procedures to develop ratings. The questions emphasize vulnerability to moving vehicle, stationary vehicle, and covert entry tactics. Vulnerability to blast is the primary expressed concern.

Table 5-3b: FEMA 'Architectural Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What major structures surround the facility?	<input type="checkbox"/>	●	●	●								
Do entrances avoid significant queuing?	<input type="checkbox"/>	●		●								
What are the adjacent land uses immediately outside the perimeter of this facility?	<input type="checkbox"/>	●		●								
Are public and private activities separated?	<input type="checkbox"/>	●					●					
Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking?	<input type="checkbox"/>	●	●	●	●	●	●			●		
Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	<input type="checkbox"/>	●	●	●						●		
Is high visitor activity away from critical assets?	<input type="checkbox"/>			●			●					
Are critical assets located in spaces that are occupied 24 hours per day?	<input type="checkbox"/>			●								
Are assets located in areas where they are visible to more than one person?	<input type="checkbox"/>			●								
Do interior barriers differentiate level of security within a facility?	<input type="checkbox"/>	●	●	●								
Are emergency systems located away from high-risk areas?	<input type="checkbox"/>	●	●	●								

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Structural and Building Envelope Systems' Questions

A vulnerability assessment of 'Structural Systems' will look at construction type, materials, detailing, collapse characteristics, critical elements, etc. An assessment of 'Building Envelope' will involve investigating strength, fenestration, glazing characteristics and detailing, anchorage, etc.

'Structural and Building Envelop Systems' questions rely on review of construction documents and visual inspection to develop ratings. Vulnerability to blast is the primary concern.

Table 5-3c:
FEMA 'Structural & Building Envelope Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What type of construction?	<input type="checkbox"/>	●	●							●		
Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system?	<input type="checkbox"/>	●	●							●		
What are the floor-to-floor heights?	<input type="checkbox"/>	●	●							●		
Is the structure vulnerable to progressive collapse?	<input type="checkbox"/>	●	●									
Are there adequate redundant load paths in the structure?	<input type="checkbox"/>	●	●							●		
What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	<input type="checkbox"/>		●							●		

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Utility Systems' Questions

A vulnerability assessment of 'Utility Systems' will look at the full range of source and supply systems serving the facility including water, fuel, and electricity supply; fire alarm and suppression, communications, etc.

'Utility Systems' questions rely equally on information obtained from visual inspection, review of construction documents, and organizational and management procedures to develop ratings. Vulnerability to waterborne contaminants is expressly considered.

Table 5-3d: FEMA 'Utility Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)	<input type="checkbox"/>	●	●									●
How many gallons and how long will it allow operations to continue?	<input type="checkbox"/>	●	●	●								●
What is the source of water for the fire suppression system? (local utility company lines, storage tanks with utility company backup, lake, or river)	<input type="checkbox"/>	●	●									
Are there alternate water supplies for fire suppression?	<input type="checkbox"/>	●	●	●								
Are the sprinkler and standpipe connections adequate and redundant?	<input type="checkbox"/>	●	●									
What fuel supplies do the facility rely upon for critical operation?	<input type="checkbox"/>	●	●	●								
Where is the fuel supply obtained?	<input type="checkbox"/>			●								
Are there alternate sources of fuel?	<input type="checkbox"/>			●								
Can alternate fuels be used?	<input type="checkbox"/>		●	●								
What is the normal source of electrical service for the facility?	<input type="checkbox"/>	●	●									
What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested?	<input type="checkbox"/>	●	●	●								
By what means does the main telephone and data communications interface the facility?	<input type="checkbox"/>	●	●	●								

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Mechanical Systems' Questions

A vulnerability assessment of 'Mechanical Systems' will investigate air supply and exhaust configurations, filtration, sensing and monitoring, system zoning and control, elevator management, etc.

'Mechanical Systems' vulnerability questions and ratings rely primarily on information obtained from review of construction documents and visual inspection. Vulnerability to airborne contaminants is the primary consideration, including contamination from Chemical, Biological, and Radiological attack.

Table 5-3e: FEMA 'Mechanical Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure)	□	●	●									●
Are there multiple air intake locations?	□	●	●									●
How are air handling systems zoned?	□	●	●									●
Are there large central air handling units or are there multiple units serving separate zones?	□		●									●
Are there any redundancies in the air handling system?	□		●	●								●
Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)	□	●										

LEGEND: □ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Plumbing and Gas Systems' Questions

A vulnerability assessment of 'Plumbing and Gas Systems' will look at the liquid distribution systems serving the facility including water and fuel distribution, water heating, fuel storage, etc.

'Plumbing and Gas Systems' questions rely primarily on information from review of construction documents to develop ratings. Vulnerability to waterborne contaminants is expressly considered.

Table 5-3f: FEMA 'Plumbing & Gas Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What is the method of water distribution?	<input type="checkbox"/>		●									●
What is the method of gas distribution? (heating, cooking, medical, process)	<input type="checkbox"/>		●									
What is the method of heating domestic water?	<input type="checkbox"/>	●	●	●								
Are there reserve supplies of critical gases?	<input type="checkbox"/>		●	●								

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Electrical Systems' Questions

A vulnerability assessment of 'Electrical Systems' will evaluate transformer and switchgear security, electricity distribution and accessibility, emergency systems, etc.

'Electrical Systems' questions primarily on information from visual inspection and review of construction documents to develop ratings. No particular attack mechanism is emphasized.

Table 5-3g: FEMA 'Electrical Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Are there any transformers or switchgears located outside the building or accessible from the building exterior?	<input type="checkbox"/>	●										
Are they (transformers or switchgears) vulnerable to public access?	<input type="checkbox"/>	●										
Are critical electrical systems located in areas outside of secured electrical areas?	<input type="checkbox"/>	●	●	●								
Does emergency backup power exist for all areas within the facility or for critical areas only?	<input type="checkbox"/>	●	●									

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Fire Alarm Systems' Questions

A vulnerability assessment of 'Fire Alarm Systems' will look at detection sensing and signaling, system configurations, accessibility of controls, redundancies, etc.

'Fire Alarm Systems' questions rely both on information from review of construction documents and review of organizational and management procedures to develop ratings. No particular attack mechanism is emphasized.

Table 5-3h: FEMA 'Fire Alarm Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Is the fire alarm system stand-alone or integrated with other functions such as security and environmental or building management systems?	<input type="checkbox"/>		●	●								
Is there redundant off-premises fire alarm reporting?	<input type="checkbox"/>		●	●								

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Communications and Information Technology Systems' Questions

A vulnerability assessment of 'Communications and Information Technology Systems' will evaluate distribution, power supplies, accessibility, control, notification, backups, etc.

'Communications and Information Technology Systems' questions rely on information from visual inspection, review of construction documents, and review of organizational and management procedures to develop ratings. No particular attack mechanism is emphasized.

Table 5-3i: FEMA 'Communication and IT Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Where is the main telephone distribution room and where is it in relation to higher risk areas?	<input type="checkbox"/>	●	●	●								
Where are communication systems wiring closets located? (voice, data, signal, alarm)	<input type="checkbox"/>	●	●									

LEGEND: ☐ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

ADDITIONAL SOURCES OF DETAILED FACILITY INFORMATION

The foregoing questions provide a framework for a qualitative estimate of facility vulnerability to terrorist attack. A more detailed and quantitative evaluation will involve significantly more review of information in all areas, including additional information concerning 'Equipment Operations and Maintenance' (up to date drawings, manuals, and procedures, training, monitoring, etc.); 'Security Systems' (perimeter and interior sensing, monitoring, and control, security system documentation and training, etc.); and the 'Security Master Plan' (currency, responsibilities, etc.).

Appendix B presents the complete list of detailed questions from FEMA 426 that should be considered in fully evaluating vulnerability to terrorist threats. The means of data collection that should be employed and the particular terrorist tactics and attack mechanisms addressed by each question are identified in the appendix so that specialized checklists can be created to assess vulnerability to terrorist tactics of particular concern to an individual organization.

VULNERABILITY REDUCTION COST INFORMATION AND ESTIMATES

Typically, a property condition assessment for due diligence would be followed by consideration of the anticipated costs and timing of needed upgrades of facility systems. Certainly, estimates of expected costs of mitigation of system vulnerability to terrorist attack will become important at some point in the decision-making process.

However, an assessment using the questions described above does not include the level of information needed to project costs. The qualitative analysis described simply determines broad preliminary options for reducing terrorism risk in a particular existing facility and does not give insight to expected costs of risk reduction. At some point in the future, fully capable due dili-

gence tools for assessing vulnerability to terrorist attack will very likely include such information and detail. For further discussion of costs related to blast mitigation, see FEMA 427, Chapter 8.

Terrorism risk management is a new and evolving field with inputs from a diverse range of disciplines and organizations. This chapter introduces several key documents and resources for further exploration in the field.

This chapter introduces reference information related to terrorist threat in commercial buildings. It describes information included in the appendices to this primer.

Terrorism Risk Insurance Act of 2002

Appendix A presents the full text of the TRIA as signed into law on November 26, 2002.

TRIA is the basis for the current Federal program to provide re-insurance cover for claims resulting from defined categories of terrorism-caused damage. The full text of the law provides the key definitions and detailed conditions of the program.

Building Vulnerability Assessment Screening

Appendix B provides a tool for the comprehensive assessment of terrorism vulnerability in buildings, including both qualitative and quantitative measures. This screening tool contains a list of vulnerability questions that provide the basis for systematic due diligence related to both physical and operational vulnerability assessment.

The vulnerability questions presented in Appendix B correspond to those in the Building Vulnerability Assessment Checklist provided in FEMA 426. The FEMA 426 checklist includes further guidance and commentary related to the application of each question to assessments of building and building system vulnerability.

Each question included in the Appendix B list is identified by type (either rapid estimation or detailed assessment), required methods of data collection, and common terrorist tactics (methods of delivery, and primary threat mechanisms). The appendix master list of questions can be re-sorted to create specialized lists of questions focused on a single parameter or multiple parameters.

The final five appendices are republished directly from reference materials in FEMA 426.

General Glossary

Appendix C presents a general glossary of terrorism risk and building security related terms in common use within federal agencies and the research community.

This glossary is intended to provide help in understanding the more specialized literature of the field and to assist in communication with specialized security consultants. The glossary includes terms related to physical security and to the organization and management of building security.

Chemical, Biological, and Radiological Glossary

Appendix D presents separate glossaries of chemical terms, biological terms, and radiological terms in common use within federal agencies and research communities.

The specialized terminology of chemical, biological and radiological threats is new to many otherwise experienced in building security and condition assessment. This specialized glossary is intended to provide help in understanding CBR issues and in communicating with specialized consultants.

Acronyms

Appendix E lists acronyms for government and private sector agencies as well as technical terms frequently used in the building security field.

The list is intended to facilitate use of background federal documents and to help in communication with public authorities concerned with various aspects of homeland security..

Associations and Organizations

Appendix F provides a listing of associations and organizations which are active in various aspects of homeland security.

Many of these organizations produce materials on the subject of terrorism risk management. These references may be of value for building owners and tenants in search of further information or

guidance. URLs are provided to access organizational homepages.

Bibliography

Appendix G is a bibliography of publications on a range of topics related to terrorism vulnerability and risk management in buildings.

These publications have been prepared by government agencies, trade associations, professional societies, and other technical information providers. These publications provide access to the currently available expertise on terrorism risk management.

116 STAT. 2322

PUBLIC LAW 107–297—NOV. 26, 2002

Public Law 107–297 107th Congress

An Act

Nov. 26, 2002
[H.R. 3210]

To ensure the continued financial capacity of insurers to provide coverage for risks from terrorism.

Terrorism Risk
Insurance Act of
2002.

15 USC 6701
note.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Terrorism Risk Insurance Act of 2002”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—TERRORISM INSURANCE PROGRAM

Sec. 101. Congressional findings and purpose.

Sec. 102. Definitions.

Sec. 103. Terrorism Insurance Program.

Sec. 104. General authority and administration of claims.

Sec. 105. Preemption and nullification of pre-existing terrorism exclusions.

Sec. 106. Preservation provisions.

Sec. 107. Litigation management.

Sec. 108. Termination of Program.

TITLE II—TREATMENT OF TERRORIST ASSETS

Sec. 201. Satisfaction of judgments from blocked assets of terrorists, terrorist organizations, and State sponsors of terrorism.

TITLE III—FEDERAL RESERVE BOARD PROVISIONS

Sec. 301. Certain authority of the Board of Governors of the Federal Reserve System.

15 USC 6701
note.

TITLE I—TERRORISM INSURANCE PROGRAM

SEC. 101. CONGRESSIONAL FINDINGS AND PURPOSE.

(a) FINDINGS.—The Congress finds that—

(1) the ability of businesses and individuals to obtain property and casualty insurance at reasonable and predictable prices, in order to spread the risk of both routine and catastrophic loss, is critical to economic growth, urban development, and the construction and maintenance of public and private housing, as well as to the promotion of United States exports and foreign trade in an increasingly interconnected world;

(2) property and casualty insurance firms are important financial institutions, the products of which allow mutualization of risk and the efficient use of financial resources and enhance

the ability of the economy to maintain stability, while responding to a variety of economic, political, environmental, and other risks with a minimum of disruption;

(3) the ability of the insurance industry to cover the unprecedented financial risks presented by potential acts of terrorism in the United States can be a major factor in the recovery from terrorist attacks, while maintaining the stability of the economy;

(4) widespread financial market uncertainties have arisen following the terrorist attacks of September 11, 2001, including the absence of information from which financial institutions can make statistically valid estimates of the probability and cost of future terrorist events, and therefore the size, funding, and allocation of the risk of loss caused by such acts of terrorism;

(5) a decision by property and casualty insurers to deal with such uncertainties, either by terminating property and casualty coverage for losses arising from terrorist events, or by radically escalating premium coverage to compensate for risks of loss that are not readily predictable, could seriously hamper ongoing and planned construction, property acquisition, and other business projects, generate a dramatic increase in rents, and otherwise suppress economic activity; and

(6) the United States Government should provide temporary financial compensation to insured parties, contributing to the stabilization of the United States economy in a time of national crisis, while the financial services industry develops the systems, mechanisms, products, and programs necessary to create a viable financial services market for private terrorism risk insurance.

(b) **PURPOSE.**—The purpose of this title is to establish a temporary Federal program that provides for a transparent system of shared public and private compensation for insured losses resulting from acts of terrorism, in order to—

(1) protect consumers by addressing market disruptions and ensure the continued widespread availability and affordability of property and casualty insurance for terrorism risk; and

(2) allow for a transitional period for the private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses, while preserving State insurance regulation and consumer protections.

SEC. 102. DEFINITIONS.

In this title, the following definitions shall apply:

(1) **ACT OF TERRORISM.**—

(A) **CERTIFICATION.**—The term “act of terrorism” means any act that is certified by the Secretary, in concurrence with the Secretary of State, and the Attorney General of the United States—

(i) to be an act of terrorism;

(ii) to be a violent act or an act that is dangerous to—

(I) human life;

(II) property; or

(III) infrastructure;

(iii) to have resulted in damage within the United States, or outside of the United States in the case of—

(I) an air carrier or vessel described in paragraph (5)(B); or

(II) the premises of a United States mission; and

(iv) to have been committed by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion.

(B) LIMITATION.—No act shall be certified by the Secretary as an act of terrorism if—

(i) the act is committed as part of the course of a war declared by the Congress, except that this clause shall not apply with respect to any coverage for workers' compensation; or

(ii) property and casualty insurance losses resulting from the act, in the aggregate, do not exceed \$5,000,000.

(C) DETERMINATIONS FINAL.—Any certification of, or determination not to certify, an act as an act of terrorism under this paragraph shall be final, and shall not be subject to judicial review.

(D) NONDELEGATION.—The Secretary may not delegate or designate to any other officer, employee, or person, any determination under this paragraph of whether, during the effective period of the Program, an act of terrorism has occurred.

(2) AFFILIATE.—The term "affiliate" means, with respect to an insurer, any entity that controls, is controlled by, or is under common control with the insurer.

(3) CONTROL.—An entity has "control" over another entity, if—

(A) the entity directly or indirectly or acting through 1 or more other persons owns, controls, or has power to vote 25 percent or more of any class of voting securities of the other entity;

(B) the entity controls in any manner the election of a majority of the directors or trustees of the other entity; or

(C) the Secretary determines, after notice and opportunity for hearing, that the entity directly or indirectly exercises a controlling influence over the management or policies of the other entity.

(4) DIRECT EARNED PREMIUM.—The term "direct earned premium" means a direct earned premium for property and casualty insurance issued by any insurer for insurance against losses occurring at the locations described in subparagraphs (A) and (B) of paragraph (5).

(5) INSURED LOSS.—The term "insured loss" means any loss resulting from an act of terrorism (including an act of war, in the case of workers' compensation) that is covered by primary or excess property and casualty insurance issued by an insurer if such loss—

(A) occurs within the United States; or

(B) occurs to an air carrier (as defined in section 40102 of title 49, United States Code), to a United States flag vessel (or a vessel based principally in the United States, on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), regardless of where the loss occurs, or at the premises of any United States mission.

(6) **INSURER.**—The term “insurer” means any entity, including any affiliate thereof—

(A) that is—

(i) licensed or admitted to engage in the business of providing primary or excess insurance in any State;

(ii) not licensed or admitted as described in clause

(i), if it is an eligible surplus line carrier listed on the Quarterly Listing of Alien Insurers of the NAIC, or any successor thereto;

(iii) approved for the purpose of offering property and casualty insurance by a Federal agency in connection with maritime, energy, or aviation activity;

(iv) a State residual market insurance entity or State workers’ compensation fund; or

(v) any other entity described in section 103(f), to the extent provided in the rules of the Secretary issued under section 103(f);

(B) that receives direct earned premiums for any type of commercial property and casualty insurance coverage, other than in the case of entities described in sections 103(d) and 103(f); and

(C) that meets any other criteria that the Secretary may reasonably prescribe.

(7) **INSURER DEDUCTIBLE.**—The term “insurer deductible” means—

(A) for the Transition Period, the value of an insurer’s direct earned premiums over the calendar year immediately preceding the date of enactment of this Act, multiplied by 1 percent;

(B) for Program Year 1, the value of an insurer’s direct earned premiums over the calendar year immediately preceding Program Year 1, multiplied by 7 percent;

(C) for Program Year 2, the value of an insurer’s direct earned premiums over the calendar year immediately preceding Program Year 2, multiplied by 10 percent;

(D) for Program Year 3, the value of an insurer’s direct earned premiums over the calendar year immediately preceding Program Year 3, multiplied by 15 percent; and

(E) notwithstanding subparagraphs (A) through (D), for the Transition Period, Program Year 1, Program Year 2, or Program Year 3, if an insurer has not had a full year of operations during the calendar year immediately preceding such Period or Program Year, such portion of the direct earned premiums of the insurer as the Secretary determines appropriate, subject to appropriate methodologies established by the Secretary for measuring such direct earned premiums.

(8) **NAIC.**—The term “NAIC” means the National Association of Insurance Commissioners.

(9) **PERSON.**—The term “person” means any individual, business or nonprofit entity (including those organized in the form of a partnership, limited liability company, corporation, or association), trust or estate, or a State or political subdivision of a State or other governmental unit.

(10) **PROGRAM.**—The term “Program” means the Terrorism Insurance Program established by this title.

(11) **PROGRAM YEARS.**—

(A) **TRANSITION PERIOD.**—The term “Transition Period” means the period beginning on the date of enactment of this Act and ending on December 31, 2002.

(B) **PROGRAM YEAR 1.**—The term “Program Year 1” means the period beginning on January 1, 2003 and ending on December 31, 2003.

(C) **PROGRAM YEAR 2.**—The term “Program Year 2” means the period beginning on January 1, 2004 and ending on December 31, 2004.

(D) **PROGRAM YEAR 3.**—The term “Program Year 3” means the period beginning on January 1, 2005 and ending on December 31, 2005.

(12) **PROPERTY AND CASUALTY INSURANCE.**—The term “property and casualty insurance”—

(A) means commercial lines of property and casualty insurance, including excess insurance, workers’ compensation insurance, and surety insurance; and

(B) does not include—

(i) Federal crop insurance issued or reinsured under the Federal Crop Insurance Act (7 U.S.C. 1501 et seq.), or any other type of crop or livestock insurance that is privately issued or reinsured;

(ii) private mortgage insurance (as that term is defined in section 2 of the Homeowners Protection Act of 1998 (12 U.S.C. 4901)) or title insurance;

(iii) financial guaranty insurance issued by monoline financial guaranty insurance corporations;

(iv) insurance for medical malpractice;

(v) health or life insurance, including group life insurance;

(vi) flood insurance provided under the National Flood Insurance Act of 1968 (42 U.S.C. 4001 et seq.); or

(vii) reinsurance or retrocessional reinsurance.

(13) **SECRETARY.**—The term “Secretary” means the Secretary of the Treasury.

(14) **STATE.**—The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, American Samoa, Guam, each of the United States Virgin Islands, and any territory or possession of the United States.

(15) **UNITED STATES.**—The term “United States” means the several States, and includes the territorial sea and the continental shelf of the United States, as those terms are defined in the Violent Crime Control and Law Enforcement Act of 1994 (18 U.S.C. 2280, 2281).

(16) **RULE OF CONSTRUCTION FOR DATES.**—With respect to any reference to a date in this title, such day shall be construed—

- (A) to begin at 12:01 a.m. on that date; and
- (B) to end at midnight on that date.

SEC. 103. TERRORISM INSURANCE PROGRAM.

(a) **ESTABLISHMENT OF PROGRAM.**—

(1) **IN GENERAL.**—There is established in the Department of the Treasury the Terrorism Insurance Program.

(2) **AUTHORITY OF THE SECRETARY.**—Notwithstanding any other provision of State or Federal law, the Secretary shall administer the Program, and shall pay the Federal share of compensation for insured losses in accordance with subsection (e).

(3) **MANDATORY PARTICIPATION.**—Each entity that meets the definition of an insurer under this title shall participate in the Program.

(b) **CONDITIONS FOR FEDERAL PAYMENTS.**—No payment may be made by the Secretary under this section with respect to an insured loss that is covered by an insurer, unless—

(1) the person that suffers the insured loss, or a person acting on behalf of that person, files a claim with the insurer;

(2) the insurer provides clear and conspicuous disclosure to the policyholder of the premium charged for insured losses covered by the Program and the Federal share of compensation for insured losses under the Program—

(A) in the case of any policy that is issued before the date of enactment of this Act, not later than 90 days after that date of enactment; Deadline.

(B) in the case of any policy that is issued within 90 days of the date of enactment of this Act, at the time of offer, purchase, and renewal of the policy; and

(C) in the case of any policy that is issued more than 90 days after the date of enactment of this Act, on a separate line item in the policy, at the time of offer, purchase, and renewal of the policy;

(3) the insurer processes the claim for the insured loss in accordance with appropriate business practices, and any reasonable procedures that the Secretary may prescribe; and

(4) the insurer submits to the Secretary, in accordance with such reasonable procedures as the Secretary may establish—

(A) a claim for payment of the Federal share of compensation for insured losses under the Program;

(B) written certification—

(i) of the underlying claim; and

(ii) of all payments made for insured losses; and

(C) certification of its compliance with the provisions of this subsection.

(c) **MANDATORY AVAILABILITY.**—

(1) **INITIAL PROGRAM PERIODS.**—During the period beginning on the first day of the Transition Period and ending on the last day of Program Year 2, each entity that meets the definition of an insurer under section 102—

- (A) shall make available, in all of its property and casualty insurance policies, coverage for insured losses; and
- (B) shall make available property and casualty insurance coverage for insured losses that does not differ materially from the terms, amounts, and other coverage limitations applicable to losses arising from events other than acts of terrorism.
- Deadline. (2) PROGRAM YEAR 3.—Not later than September 1, 2004, the Secretary shall, based on the factors referred to in section 108(d)(1), determine whether the provisions of subparagraphs (A) and (B) of paragraph (1) should be extended through Program Year 3.
- Regulations. (d) STATE RESIDUAL MARKET INSURANCE ENTITIES.—
- (1) IN GENERAL.—The Secretary shall issue regulations, as soon as practicable after the date of enactment of this Act, that apply the provisions of this title to State residual market insurance entities and State workers' compensation funds.
- (2) TREATMENT OF CERTAIN ENTITIES.—For purposes of the regulations issued pursuant to paragraph (1)—
- (A) a State residual market insurance entity that does not share its profits and losses with private sector insurers shall be treated as a separate insurer; and
- (B) a State residual market insurance entity that shares its profits and losses with private sector insurers shall not be treated as a separate insurer, and shall report to each private sector insurance participant its share of the insured losses of the entity, which shall be included in each private sector insurer's insured losses.
- (3) TREATMENT OF PARTICIPATION IN CERTAIN ENTITIES.—Any insurer that participates in sharing profits and losses of a State residual market insurance entity shall include in its calculations of premiums any premiums distributed to the insurer by the State residual market insurance entity.
- (e) INSURED LOSS SHARED COMPENSATION.—
- (1) FEDERAL SHARE.—
- (A) IN GENERAL.—The Federal share of compensation under the Program to be paid by the Secretary for insured losses of an insurer during the Transition Period and each Program Year shall be equal to 90 percent of that portion of the amount of such insured losses that exceeds the applicable insurer deductible required to be paid during such Transition Period or such Program Year.
- (B) PROHIBITION ON DUPLICATIVE COMPENSATION.—The Federal share of compensation for insured losses under the Program shall be reduced by the amount of compensation provided by the Federal Government to any person under any other Federal program for those insured losses.
- (2) CAP ON ANNUAL LIABILITY.—
- (A) IN GENERAL.—Notwithstanding paragraph (1) or any other provision of Federal or State law, if the aggregate insured losses exceed \$100,000,000,000, during the period beginning on the first day of the Transition Period and ending on the last day of Program Year 1, or during Program Year 2 or Program Year 3 (until such time as the Congress may act otherwise with respect to such losses)—

(i) the Secretary shall not make any payment under this title for any portion of the amount of such losses that exceeds \$100,000,000,000; and

(ii) no insurer that has met its insurer deductible shall be liable for the payment of any portion of that amount that exceeds \$100,000,000,000.

(B) INSURER SHARE.—For purposes of subparagraph (A), the Secretary shall determine the pro rata share of insured losses to be paid by each insurer that incurs insured losses under the Program.

(3) NOTICE TO CONGRESS.—The Secretary shall notify the Congress if estimated or actual aggregate insured losses exceed \$100,000,000,000 during the period beginning on the first day of the Transition Period and ending on the last day of Program Year 1, or during Program Year 2 or Program Year 3, and the Congress shall determine the procedures for and the source of any payments for such excess insured losses.

(4) FINAL NETTING.—The Secretary shall have sole discretion to determine the time at which claims relating to any insured loss or act of terrorism shall become final.

(5) DETERMINATIONS FINAL.—Any determination of the Secretary under this subsection shall be final, unless expressly provided, and shall not be subject to judicial review.

(6) INSURANCE MARKETPLACE AGGREGATE RETENTION AMOUNT.—For purposes of paragraph (7), the insurance marketplace aggregate retention amount shall be—

(A) for the period beginning on the first day of the Transition Period and ending on the last day of Program Year 1, the lesser of—

(i) \$10,000,000,000; and

(ii) the aggregate amount, for all insurers, of insured losses during such period;

(B) for Program Year 2, the lesser of—

(i) \$12,500,000,000; and

(ii) the aggregate amount, for all insurers, of insured losses during such Program Year; and

(C) for Program Year 3, the lesser of—

(i) \$15,000,000,000; and

(ii) the aggregate amount, for all insurers, of insured losses during such Program Year.

(7) RECOUPMENT OF FEDERAL SHARE.—

(A) MANDATORY RECOUPMENT AMOUNT.—For purposes of this paragraph, the mandatory recoupment amount for each of the periods referred to in subparagraphs (A), (B), and (C) of paragraph (6) shall be the difference between—

(i) the insurance marketplace aggregate retention amount under paragraph (6) for such period; and

(ii) the aggregate amount, for all insurers, of insured losses during such period that are not compensated by the Federal Government because such losses—

(I) are within the insurer deductible for the insurer subject to the losses; or

(II) are within the portion of losses of the insurer that exceed the insurer deductible, but are not compensated pursuant to paragraph (1).

(B) NO MANDATORY RECOUPMENT IF UNCOMPENSATED LOSSES EXCEED INSURANCE MARKETPLACE RETENTION.—Notwithstanding subparagraph (A), if the aggregate amount of uncompensated insured losses referred to in clause (ii) of such subparagraph for any period referred to in subparagraph (A), (B), or (C) of paragraph (6) is greater than the insurance marketplace aggregate retention amount under paragraph (6) for such period, the mandatory recoupment amount shall be \$0.

(C) MANDATORY ESTABLISHMENT OF SURCHARGES TO RECOUP MANDATORY RECOUPMENT AMOUNT.—The Secretary shall collect, for repayment of the Federal financial assistance provided in connection with all acts of terrorism (or acts of war, in the case of workers compensation) occurring during any of the periods referred to in subparagraph (A), (B), or (C) of paragraph (6), terrorism loss risk-spreading premiums in an amount equal to any mandatory recoupment amount for such period.

(D) DISCRETIONARY RECOUPMENT OF REMAINDER OF FINANCIAL ASSISTANCE.—To the extent that the amount of Federal financial assistance provided exceeds any mandatory recoupment amount, the Secretary may recoup, through terrorism loss risk-spreading premiums, such additional amounts that the Secretary believes can be recouped, based on—

- (i) the ultimate costs to taxpayers of no additional recoupment;
- (ii) the economic conditions in the commercial marketplace, including the capitalization, profitability, and investment returns of the insurance industry and the current cycle of the insurance markets;
- (iii) the affordability of commercial insurance for small- and medium-sized businesses; and
- (iv) such other factors as the Secretary considers appropriate.

(8) POLICY SURCHARGE FOR TERRORISM LOSS RISK-SPREADING PREMIUMS.—

(A) POLICYHOLDER PREMIUM.—Any amount established by the Secretary as a terrorism loss risk-spreading premium shall—

- (i) be imposed as a policyholder premium surcharge on property and casualty insurance policies in force after the date of such establishment;
- (ii) begin with such period of coverage during the year as the Secretary determines appropriate; and
- (iii) be based on a percentage of the premium amount charged for property and casualty insurance coverage under the policy.

(B) COLLECTION.—The Secretary shall provide for insurers to collect terrorism loss risk-spreading premiums and remit such amounts collected to the Secretary.

(C) PERCENTAGE LIMITATION.—A terrorism loss risk-spreading premium (including any additional amount included in such premium on a discretionary basis pursuant to paragraph (7)(D)) may not exceed, on an annual basis, the amount equal to 3 percent of the premium charged

for property and casualty insurance coverage under the policy.

(D) ADJUSTMENT FOR URBAN AND SMALLER COMMERCIAL AND RURAL AREAS AND DIFFERENT LINES OF INSURANCE.—

(i) ADJUSTMENTS.—In determining the method and manner of imposing terrorism loss risk-spreading premiums, including the amount of such premiums, the Secretary shall take into consideration—

(I) the economic impact on commercial centers of urban areas, including the effect on commercial rents and commercial insurance premiums, particularly rents and premiums charged to small businesses, and the availability of lease space and commercial insurance within urban areas;

(II) the risk factors related to rural areas and smaller commercial centers, including the potential exposure to loss and the likely magnitude of such loss, as well as any resulting cross-subsidization that might result; and

(III) the various exposures to terrorism risk for different lines of insurance.

(ii) RECOUPMENT OF ADJUSTMENTS.—Any mandatory recoupment amounts not collected by the Secretary because of adjustments under this subparagraph shall be recouped through additional terrorism loss risk-spreading premiums.

(E) TIMING OF PREMIUMS.—The Secretary may adjust the timing of terrorism loss risk-spreading premiums to provide for equivalent application of the provisions of this title to policies that are not based on a calendar year, or to apply such provisions on a daily, monthly, or quarterly basis, as appropriate.

(f) CAPTIVE INSURERS AND OTHER SELF-INSURANCE ARRANGEMENTS.—The Secretary may, in consultation with the NAIC or the appropriate State regulatory authority, apply the provisions of this title, as appropriate, to other classes or types of captive insurers and other self-insurance arrangements by municipalities and other entities (such as workers' compensation self-insurance programs and State workers' compensation reinsurance pools), but only if such application is determined before the occurrence of an act of terrorism in which such an entity incurs an insured loss and all of the provisions of this title are applied comparably to such entities.

(g) REINSURANCE TO COVER EXPOSURE.—

(1) OBTAINING COVERAGE.—This title may not be construed to limit or prevent insurers from obtaining reinsurance coverage for insurer deductibles or insured losses retained by insurers pursuant to this section, nor shall the obtaining of such coverage affect the calculation of such deductibles or retentions.

(2) LIMITATION ON FINANCIAL ASSISTANCE.—The amount of financial assistance provided pursuant to this section shall not be reduced by reinsurance paid or payable to an insurer from other sources, except that recoveries from such other sources, taken together with financial assistance for the Transition Period or a Program Year provided pursuant to this section, may not exceed the aggregate amount of the insurer's insured

losses for such period. If such recoveries and financial assistance for the Transition Period or a Program Year exceed such aggregate amount of insured losses for that period and there is no agreement between the insurer and any reinsurer to the contrary, an amount in excess of such aggregate insured losses shall be returned to the Secretary.

(h) GROUP LIFE INSURANCE STUDY.—

(1) STUDY.—The Secretary shall study, on an expedited basis, whether adequate and affordable catastrophe reinsurance for acts of terrorism is available to life insurers in the United States that issue group life insurance, and the extent to which the threat of terrorism is reducing the availability of group life insurance coverage for consumers in the United States.

(2) CONDITIONAL COVERAGE.—To the extent that the Secretary determines that such coverage is not or will not be reasonably available to both such insurers and consumers, the Secretary shall, in consultation with the NAIC—

(A) apply the provisions of this title, as appropriate, to providers of group life insurance; and

(B) provide such restrictions, limitations, or conditions with respect to any financial assistance provided that the Secretary deems appropriate, based on the study under paragraph (1).

(i) STUDY AND REPORT.—

(1) STUDY.—The Secretary, after consultation with the NAIC, representatives of the insurance industry, and other experts in the insurance field, shall conduct a study of the potential effects of acts of terrorism on the availability of life insurance and other lines of insurance coverage, including personal lines.

Deadline.

(2) REPORT.—Not later than 9 months after the date of enactment of this Act, the Secretary shall submit a report to the Congress on the results of the study conducted under paragraph (1).

SEC. 104. GENERAL AUTHORITY AND ADMINISTRATION OF CLAIMS.

(a) GENERAL AUTHORITY.—The Secretary shall have the powers and authorities necessary to carry out the Program, including authority—

(1) to investigate and audit all claims under the Program; and

Regulations.

(2) to prescribe regulations and procedures to effectively administer and implement the Program, and to ensure that all insurers and self-insured entities that participate in the Program are treated comparably under the Program.

(b) INTERIM RULES AND PROCEDURES.—The Secretary may issue interim final rules or procedures specifying the manner in which—

(1) insurers may file and certify claims under the Program;

(2) the Federal share of compensation for insured losses will be paid under the Program, including payments based on estimates of or actual insured losses;

(3) the Secretary may, at any time, seek repayment from or reimburse any insurer, based on estimates of insured losses under the Program, to effectuate the insured loss sharing provisions in section 103; and

(4) the Secretary will determine any final netting of payments under the Program, including payments owed to the

Federal Government from any insurer and any Federal share of compensation for insured losses owed to any insurer, to effectuate the insured loss sharing provisions in section 103.

(c) CONSULTATION.—The Secretary shall consult with the NAIC, as the Secretary determines appropriate, concerning the Program.

(d) CONTRACTS FOR SERVICES.—The Secretary may employ persons or contract for services as may be necessary to implement the Program.

(e) CIVIL PENALTIES.—

(1) IN GENERAL.—The Secretary may assess a civil monetary penalty in an amount not exceeding the amount under paragraph (2) against any insurer that the Secretary determines, on the record after opportunity for a hearing—

(A) has failed to charge, collect, or remit terrorism loss risk-spreading premiums under section 103(e) in accordance with the requirements of, or regulations issued under, this title;

(B) has intentionally provided to the Secretary erroneous information regarding premium or loss amounts;

(C) submits to the Secretary fraudulent claims under the Program for insured losses;

(D) has failed to provide the disclosures required under subsection (f); or

(E) has otherwise failed to comply with the provisions of, or the regulations issued under, this title.

(2) AMOUNT.—The amount under this paragraph is the greater of \$1,000,000 and, in the case of any failure to pay, charge, collect, or remit amounts in accordance with this title or the regulations issued under this title, such amount in dispute.

(3) RECOVERY OF AMOUNT IN DISPUTE.—A penalty under this subsection for any failure to pay, charge, collect, or remit amounts in accordance with this title or the regulations under this title shall be in addition to any such amounts recovered by the Secretary.

(f) SUBMISSION OF PREMIUM INFORMATION.—

(1) IN GENERAL.—The Secretary shall annually compile information on the terrorism risk insurance premium rates of insurers for the preceding year.

(2) ACCESS TO INFORMATION.—To the extent that such information is not otherwise available to the Secretary, the Secretary may require each insurer to submit to the NAIC terrorism risk insurance premium rates, as necessary to carry out paragraph (1), and the NAIC shall make such information available to the Secretary.

(3) AVAILABILITY TO CONGRESS.—The Secretary shall make information compiled under this subsection available to the Congress, upon request.

(g) FUNDING.—

(1) FEDERAL PAYMENTS.—There are hereby appropriated, out of funds in the Treasury not otherwise appropriated, such sums as may be necessary to pay the Federal share of compensation for insured losses under the Program.

(2) ADMINISTRATIVE EXPENSES.—There are hereby appropriated, out of funds in the Treasury not otherwise appropriated, such sums as may be necessary to pay reasonable costs of administering the Program.

SEC. 105. PREEMPTION AND NULLIFICATION OF PRE-EXISTING TERRORISM EXCLUSIONS.

(a) **GENERAL NULLIFICATION.**—Any terrorism exclusion in a contract for property and casualty insurance that is in force on the date of enactment of this Act shall be void to the extent that it excludes losses that would otherwise be insured losses.

(b) **GENERAL PREEMPTION.**—Any State approval of any terrorism exclusion from a contract for property and casualty insurance that is in force on the date of enactment of this Act, shall be void to the extent that it excludes losses that would otherwise be insured losses.

(c) **REINSTATEMENT OF TERRORISM EXCLUSIONS.**—Notwithstanding subsections (a) and (b) or any provision of State law, an insurer may reinstate a preexisting provision in a contract for property and casualty insurance that is in force on the date of enactment of this Act and that excludes coverage for an act of terrorism only—

(1) if the insurer has received a written statement from the insured that affirmatively authorizes such reinstatement; or

(2) if—

(A) the insured fails to pay any increased premium charged by the insurer for providing such terrorism coverage; and

(B) the insurer provided notice, at least 30 days before any such reinstatement, of—

(i) the increased premium for such terrorism coverage; and

(ii) the rights of the insured with respect to such coverage, including any date upon which the exclusion would be reinstated if no payment is received.

SEC. 106. PRESERVATION PROVISIONS.

(a) **STATE LAW.**—Nothing in this title shall affect the jurisdiction or regulatory authority of the insurance commissioner (or any agency or office performing like functions) of any State over any insurer or other person—

(1) except as specifically provided in this title; and

(2) except that—

(A) the definition of the term “act of terrorism” in section 102 shall be the exclusive definition of that term for purposes of compensation for insured losses under this title, and shall preempt any provision of State law that is inconsistent with that definition, to the extent that such provision of law would otherwise apply to any type of insurance covered by this title;

(B) during the period beginning on the date of enactment of this Act and ending on December 31, 2003, rates and forms for terrorism risk insurance covered by this title and filed with any State shall not be subject to prior approval or a waiting period under any law of a State that would otherwise be applicable, except that nothing in this title affects the ability of any State to invalidate a rate as excessive, inadequate, or unfairly discriminatory, and, with respect to forms, where a State has prior approval authority, it shall apply to allow subsequent review of such forms; and

(C) during the period beginning on the date of enactment of this Act and for so long as the Program is in effect, as provided in section 108, including authority in subsection 108(b), books and records of any insurer that are relevant to the Program shall be provided, or caused to be provided, to the Secretary, upon request by the Secretary, notwithstanding any provision of the laws of any State prohibiting or limiting such access.

(b) **EXISTING REINSURANCE AGREEMENTS.**—Nothing in this title shall be construed to alter, amend, or expand the terms of coverage under any reinsurance agreement in effect on the date of enactment of this Act. The terms and conditions of such an agreement shall be determined by the language of that agreement.

SEC. 107. LITIGATION MANAGEMENT.

(a) PROCEDURES AND DAMAGES.—

(1) **IN GENERAL.**—If the Secretary makes a determination pursuant to section 102 that an act of terrorism has occurred, there shall exist a Federal cause of action for property damage, personal injury, or death arising out of or resulting from such act of terrorism, which shall be the exclusive cause of action and remedy for claims for property damage, personal injury, or death arising out of or relating to such act of terrorism, except as provided in subsection (b).

(2) **PREEMPTION OF STATE ACTIONS.**—All State causes of action of any kind for property damage, personal injury, or death arising out of or resulting from an act of terrorism that are otherwise available under State law are hereby preempted, except as provided in subsection (b).

(3) **SUBSTANTIVE LAW.**—The substantive law for decision in any such action described in paragraph (1) shall be derived from the law, including choice of law principles, of the State in which such act of terrorism occurred, unless such law is otherwise inconsistent with or preempted by Federal law.

(4) **JURISDICTION.**—For each determination described in paragraph (1), not later than 90 days after the occurrence of an act of terrorism, the Judicial Panel on Multidistrict Litigation shall designate 1 district court or, if necessary, multiple district courts of the United States that shall have original and exclusive jurisdiction over all actions for any claim (including any claim for loss of property, personal injury, or death) relating to or arising out of an act of terrorism subject to this section. The Judicial Panel on Multidistrict Litigation shall select and assign the district court or courts based on the convenience of the parties and the just and efficient conduct of the proceedings. For purposes of personal jurisdiction, the district court or courts designated by the Judicial Panel on Multidistrict Litigation shall be deemed to sit in all judicial districts in the United States.

Deadline.

(5) **PUNITIVE DAMAGES.**—Any amounts awarded in an action under paragraph (1) that are attributable to punitive damages shall not count as insured losses for purposes of this title.

(b) **EXCLUSION.**—Nothing in this section shall in any way limit the liability of any government, an organization, or person who knowingly participates in, conspires to commit, aids and abets, or commits any act of terrorism with respect to which a determination described in subsection (a)(1) was made.

(c) **RIGHT OF SUBROGATION.**—The United States shall have the right of subrogation with respect to any payment or claim paid by the United States under this title.

(d) **RELATIONSHIP TO OTHER LAW.**—Nothing in this section shall be construed to affect—

(1) any party's contractual right to arbitrate a dispute;

or

(2) any provision of the Air Transportation Safety and System Stabilization Act (Public Law 107-42; 49 U.S.C. 40101 note.).

Applicability.

(e) **EFFECTIVE PERIOD.**—This section shall apply only to actions described in subsection (a)(1) that arise out of or result from acts of terrorism that occur or occurred during the effective period of the Program.

SEC. 108. TERMINATION OF PROGRAM.

(a) **TERMINATION OF PROGRAM.**—The Program shall terminate on December 31, 2005.

(b) **CONTINUING AUTHORITY TO PAY OR ADJUST COMPENSATION.**—Following the termination of the Program, the Secretary may take such actions as may be necessary to ensure payment, recoupment, reimbursement, or adjustment of compensation for insured losses arising out of any act of terrorism occurring during the period in which the Program was in effect under this title, in accordance with the provisions of section 103 and regulations promulgated thereunder.

(c) **REPEAL; SAVINGS CLAUSE.**—This title is repealed on the final termination date of the Program under subsection (a), except that such repeal shall not be construed—

(1) to prevent the Secretary from taking, or causing to be taken, such actions under subsection (b) of this section, paragraph (4), (5), (6), (7), or (8) of section 103(e), or subsection (a)(1), (c), (d), or (e) of section 104, as in effect on the day before the date of such repeal, or applicable regulations promulgated thereunder, during any period in which the authority of the Secretary under subsection (b) of this section is in effect; or

(2) to prevent the availability of funding under section 104(g) during any period in which the authority of the Secretary under subsection (b) of this section is in effect.

(d) **STUDY AND REPORT ON THE PROGRAM.**—

(1) **STUDY.**—The Secretary, in consultation with the NAIC, representatives of the insurance industry and of policy holders, other experts in the insurance field, and other experts as needed, shall assess the effectiveness of the Program and the likely capacity of the property and casualty insurance industry to offer insurance for terrorism risk after termination of the Program, and the availability and affordability of such insurance for various policyholders, including railroads, trucking, and public transit.

Deadline.

(2) **REPORT.**—The Secretary shall submit a report to the Congress on the results of the study conducted under paragraph (1) not later than June 30, 2005.

TITLE II—TREATMENT OF TERRORIST ASSETS

SEC. 201. SATISFACTION OF JUDGMENTS FROM BLOCKED ASSETS OF TERRORISTS, TERRORIST ORGANIZATIONS, AND STATE SPONSORS OF TERRORISM.

(a) IN GENERAL.—Notwithstanding any other provision of law, and except as provided in subsection (b), in every case in which a person has obtained a judgment against a terrorist party on a claim based upon an act of terrorism, or for which a terrorist party is not immune under section 1605(a)(7) of title 28, United States Code, the blocked assets of that terrorist party (including the blocked assets of any agency or instrumentality of that terrorist party) shall be subject to execution or attachment in aid of execution in order to satisfy such judgment to the extent of any compensatory damages for which such terrorist party has been adjudged liable.

28 USC 1610
note.

(b) PRESIDENTIAL WAIVER.—

(1) IN GENERAL.—Subject to paragraph (2), upon determining on an asset-by-asset basis that a waiver is necessary in the national security interest, the President may waive the requirements of subsection (a) in connection with (and prior to the enforcement of) any judicial order directing attachment in aid of execution or execution against any property subject to the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations.

28 USC 1610
note.

(2) EXCEPTION.—A waiver under this subsection shall not apply to—

(A) property subject to the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations that has been used by the United States for any nondiplomatic purpose (including use as rental property), or the proceeds of such use; or

(B) the proceeds of any sale or transfer for value to a third party of any asset subject to the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations.

(c) SPECIAL RULE FOR CASES AGAINST IRAN.—Section 2002 of the Victims of Trafficking and Violence Protection Act of 2000 (Public Law 106-386; 114 Stat. 1542), as amended by section 686 of Public Law 107-228, is further amended—

Ante, p. 1411.

(1) in subsection (a)(2)(A)(ii), by striking “July 27, 2000, or January 16, 2002” and inserting “July 27, 2000, any other date before October 28, 2000, or January 16, 2002”;

(2) in subsection (b)(2)(B), by inserting after “the date of enactment of this Act” the following: “(less amounts therein as to which the United States has an interest in subrogation pursuant to subsection (c) arising prior to the date of entry of the judgment or judgments to be satisfied in whole or in part hereunder)”;

(3) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

28 USC 1606,
1610 and note.

(4) by inserting after subsection (c) the following new subsection (d):

“(d) DISTRIBUTION OF ACCOUNT BALANCES AND PROCEEDS INADEQUATE TO SATISFY FULL AMOUNT OF COMPENSATORY AWARDS AGAINST IRAN.—

“(1) PRIOR JUDGMENTS.—

“(A) IN GENERAL.—In the event that the Secretary determines that 90 percent of the amounts available to be paid under subsection (b)(2) are inadequate to pay the total amount of compensatory damages awarded in judgments issued as of the date of the enactment of this subsection in cases identified in subsection (a)(2)(A) with respect to Iran, the Secretary shall, not later than 60 days after such date, make payment from such amounts available to be paid under subsection (b)(2) to each party to which such a judgment has been issued in an amount equal to a share, calculated under subparagraph (B), of 90 percent of the amounts available to be paid under subsection (b)(2) that have not been subrogated to the United States under this Act as of the date of enactment of this subsection.

“(B) CALCULATION OF PAYMENTS.—The share that is payable to a person under subparagraph (A), including any person issued a final judgment as of the date of enactment of this subsection in a suit filed on a date added by the amendment made by section 686 of Public Law 107-228, shall be equal to the proportion that the amount of unpaid compensatory damages awarded in a final judgment issued to that person bears to the total amount of all unpaid compensatory damages awarded to all persons to whom such judgments have been issued as of the date of enactment of this subsection in cases identified in subsection (a)(2)(A) with respect to Iran.

“(2) SUBSEQUENT JUDGMENT.—

“(A) IN GENERAL.—The Secretary shall pay to any person awarded a final judgment after the date of enactment of this subsection, in the case filed on January 16, 2002, and identified in subsection (a)(2)(A) with respect to Iran, an amount equal to a share, calculated under subparagraph (B), of the balance of the amounts available to be paid under subsection (b)(2) that remain following the disbursement of all payments as provided by paragraph (1). The Secretary shall make such payment not later than 30 days after such judgment is awarded.

“(B) CALCULATION OF PAYMENTS.—To the extent that funds are available, the amount paid under subparagraph (A) to such person shall be the amount the person would have been paid under paragraph (1) if the person had been awarded the judgment prior to the date of enactment of this subsection.

“(3) ADDITIONAL PAYMENTS.—

“(A) IN GENERAL.—Not later than 30 days after the disbursement of all payments under paragraphs (1) and (2), the Secretary shall make an additional payment to each person who received a payment under paragraph (1) or (2) in an amount equal to a share, calculated under subparagraph (B), of the balance of the amounts available to be paid under subsection (b)(2) that remain following the disbursement of all payments as provided by paragraphs (1) and (2).

“(B) CALCULATION OF PAYMENTS.—The share payable under subparagraph (A) to each such person shall be equal

Deadline.

to the proportion that the amount of compensatory damages awarded that person bears to the total amount of all compensatory damages awarded to all persons who received a payment under paragraph (1) or (2).

“(4) **STATUTORY CONSTRUCTION.**—Nothing in this subsection shall bar, or require delay in, enforcement of any judgment to which this subsection applies under any procedure or against assets otherwise available under this section or under any other provision of law.

“(5) **CERTAIN RIGHTS AND CLAIMS NOT RELINQUISHED.**—Any person receiving less than the full amount of compensatory damages awarded to that party in a judgment to which this subsection applies shall not be required to make the election set forth in subsection (a)(2)(B) or, with respect to subsection (a)(2)(D), the election relating to relinquishment of any right to execute or attach property that is subject to section 1610(f)(1)(A) of title 28, United States Code, except that such person shall be required to relinquish rights set forth—

“(A) in subsection (a)(2)(C); and

“(B) in subsection (a)(2)(D) with respect to enforcement against property that is at issue in claims against the United States before an international tribunal or that is the subject of awards by such tribunal.

“(6) **GUIDELINES FOR ESTABLISHING CLAIMS OF A RIGHT TO PAYMENT.**—The Secretary may promulgate reasonable guidelines through which any person claiming a right to payment under this section may inform the Secretary of the basis for such claim, including by submitting a certified copy of the final judgment under which such right is claimed and by providing commercially reasonable payment instructions. The Secretary shall take all reasonable steps necessary to ensure, to the maximum extent practicable, that such guidelines shall not operate to delay or interfere with payment under this section.”

(d) **DEFINITIONS.**—In this section, the following definitions shall apply:

28 USC 1610
note.

(1) **ACT OF TERRORISM.**—The term “act of terrorism” means—

(A) any act or event certified under section 102(1); or

(B) to the extent not covered by subparagraph (A), any terrorist activity (as defined in section 212(a)(3)(B)(iii) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(iii))).

(2) **BLOCKED ASSET.**—The term “blocked asset” means—
(A) any asset seized or frozen by the United States under section 5(b) of the Trading With the Enemy Act (50 U.S.C. App. 5(b)) or under sections 202 and 203 of the International Emergency Economic Powers Act (50 U.S.C. 1701; 1702); and

(B) does not include property that—

(i) is subject to a license issued by the United States Government for final payment, transfer, or disposition by or to a person subject to the jurisdiction of the United States in connection with a transaction for which the issuance of such license has been specifically required by statute other than the International

Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) or the United Nations Participation Act of 1945 (22 U.S.C. 287 et seq.); or

(ii) in the case of property subject to the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations, or that enjoys equivalent privileges and immunities under the law of the United States, is being used exclusively for diplomatic or consular purposes.

(3) **CERTAIN PROPERTY.**—The term “property subject to the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations” and the term “asset subject to the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations” mean any property or asset, respectively, the attachment in aid of execution or execution of which would result in a violation of an obligation of the United States under the Vienna Convention on Diplomatic Relations or the Vienna Convention on Consular Relations, as the case may be.

(4) **TERRORIST PARTY.**—The term “terrorist party” means a terrorist, a terrorist organization (as defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi))), or a foreign state designated as a state sponsor of terrorism under section 6(j) of the Export Administration Act of 1979 (50 U.S.C. App. 2405(j)) or section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371).

TITLE III—FEDERAL RESERVE BOARD PROVISIONS

SEC. 301. CERTAIN AUTHORITY OF THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM.

Section 11 of the Federal Reserve Act (12 U.S.C. 248) is amended by adding at the end the following new subsection:

“(r)(1) Any action that this Act provides may be taken only upon the affirmative vote of 5 members of the Board may be taken upon the unanimous vote of all members then in office if there are fewer than 5 members in office at the time of the action.

“(2)(A) Any action that the Board is otherwise authorized to take under section 13(3) may be taken upon the unanimous vote of all available members then in office, if—

“(i) at least 2 members are available and all available members participate in the action;

“(ii) the available members unanimously determine that—

“(I) unusual and exigent circumstances exist and the borrower is unable to secure adequate credit accommodations from other sources;

“(II) action on the matter is necessary to prevent, correct, or mitigate serious harm to the economy or the stability of the financial system of the United States;

“(III) despite the use of all means available (including all available telephonic, telegraphic, and other electronic means), the other members of the Board have not been able to be contacted on the matter; and

“(IV) action on the matter is required before the number of Board members otherwise required to vote on the matter can be contacted through any available means (including all available telephonic, telegraphic, and other electronic means); and

“(iii) any credit extended by a Federal reserve bank pursuant to such action is payable upon demand of the Board.

“(B) The available members of the Board shall document in writing the determinations required by subparagraph (A)(ii), and such written findings shall be included in the record of the action and in the official minutes of the Board, and copies of such record shall be provided as soon as practicable to the members of the Board who were not available to participate in the action and to the Chairman of the Committee on Banking, Housing, and Urban Affairs of the Senate and to the Chairman of the Committee on Financial Services of the House of Representatives.”. Records.

Approved November 26, 2002.

LEGISLATIVE HISTORY—H.R. 3210 (S. 2600):

HOUSE REPORTS: Nos. 107-300, Pt. 1 (Comm. on Financial Services) and Pt. 2 (Comm. on Ways and Means) and 107-779 (Comm. of Conference).

CONGRESSIONAL RECORD:

Vol. 147 (2001): Nov. 29, considered and passed House.

Vol. 148 (2002): July 25, considered and passed Senate, amended, in lieu of S. 2600.

Nov. 14, House agreed to conference report.

Nov. 19, Senate agreed to conference report.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 38 (2002):

Nov. 26, Presidential remarks.

BUILDING VULNERABILITY ASSESSMENT SCREENING **B**

The following screening tool includes questions concerning vulnerability to terrorism that need to be addressed for new or existing buildings. The questions are intended to provide the basis for a vulnerability assessment of building design and operation of various component systems. Subsets of questions in the screening tool can be used either for a rapid vulnerability estimation or for a comprehensive detailed assessment of buildings.

This screening tool includes all of the vulnerability questions from the Building Vulnerability Assessment Checklist in FEMA 426. The FEMA 426 checklist also presents extended guidance and observations regarding use of each question in assessing building vulnerability to terrorist attack. Both the FEMA 426 checklist and this screening tool are organized into 13 sections, listed below.

- A. Site
- B. Architectural
- C. Structural Systems
- D. Building Envelope
- E. Utility Systems
- F. Mechanical Systems (including Chemical, Biological, and Radiological Systems)
- G. Plumbing and Gas Systems
- H. Electrical Systems
- I. Fire Alarm Systems
- J. Communications and Information Technology Systems
- K. Equipment Operations and Maintenance
- L. Security Systems
- M. Security Master Plan

The vulnerability questions presented in this screening tool are characterized by type (vulnerability estimate or detailed assessment), how information concerning the question will likely be collected (visual inspection, design documentation, and/or review of organizational/management procedures), and common terrorist attack tactics (delivery by moving, stationary vehicles, or covert entry, disguised in the mail or in supply materials; and blast pressure, airborne, or waterborne attack mechanisms).

From the USAF *Installation Force Protection Guide*, tactics refer to the offensive strategies employed by aggressors, reflecting their capabilities and objectives. Some of the more common tactics include:

- **Moving vehicle.** The moving vehicle attack is a suicide attack where an explosive-laden vehicle is driven into a facility, and detonated.
- **Stationary vehicle.** This type of attack may be detonated by time delay or remote control.
- **Covert entry.** The aggressor attempts to enter the facility covertly using false credentials. The aggressor may attempt to carry weapons or explosives into the facility.
- **Mail attack.** Small bombs or incendiary devices are incorporated into envelopes or packages that are delivered to the targeted individual.
- **Supplies attack.** Bombs or incendiary devices, generally larger than those found in mail bombs, are incorporated into various containers and delivered to facilities or installations.
- **Airborne contamination.** The aggressor uses chemical or biological agents to contaminate the air supply of a facility or installation.
- **Waterborne contamination.** The aggressor uses chemical, biological, or radiological agents to contaminate the water supply of a facility or installation."

The table below arrays the compatibility of common tactics with a FEMA list of terrorist attack devices and methods.

FEMA Attack Devices/Modes	USAF Common Tactics/Delivery						
	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Airborne contamination	Waterborne contamination
Agri-terrorism							
Armed attack			•				
Arson/incendiary			•	•	•		
Biological agent	•	•	•	•	•	•	•
Bomb	•	•	•	•	•		
Chemical agent	•	•	•		•	•	•
Cyber-terrorism							
HAZMAT release	•	•	•	•	•	•	•
Nuclear bomb							
Radiological agent	•	•	•	•	•	•	

The following tables adapt the ‘common tactics/delivery’ described above by adding ‘blast effects’ as a category of terrorist attack ‘mechanisms.’

Table A: Site

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Site.1a	What major structures surround the facility?	●		●	●									
Site.1b	What critical infrastructure, government, military, or recreation facilities are in the local area that impact transportation, utilities, and collateral damage (attack at this facility impacting the other major structures or attack on the major structures impacting this facility)?	●		●	●	●								
Site.1c	What are the adjacent land uses immediately outside the perimeter of this facility?	●		●	●									
Site.1d	Do future development plans change these land uses outside the facility perimeter?		●	●	●									
Site.2	Does the terrain place the building in a depression or low area?		●	●										
Site.3	In dense, urban areas, does curb lane parking place uncontrolled parked vehicles unacceptably close to a facility in public rights-of-way?		●	●		●		●				●		
Site.4	Is a perimeter fence or other types of barrier controls in place?		●	●			●		●					
Site.5	What are the site access points to the facility?	●		●			●		●					
Site.6	Is vehicle traffic separated from pedestrian traffic on the site?		●	●		●	●		●					
Site.7	Is there vehicle and pedestrian access control at the perimeter of the site?		●	●		●	●		●					
Site.8a	Is there space for inspection at the curb line or outside the protected perimeter?		●	●			●							
Site.8b	What is the minimum distance from the inspection location to the building?	●		●			●		●			●		
Site.9	Is there any potential access to the site or facility through utility paths or water runoff?	●		●	●				●					
Site.10a	What are the existing types of vehicle anti-ram devices for the facility?	●		●			●							
Site.10b	Are these devices at the property boundary or at the building?		●	●			●							
Site.11	What is the anti-ram buffer zone standoff distance from the building to unscreened vehicles or parking?	●		●			●					●		

Table A: Site (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Site.12a	Are perimeter barriers capable of stopping vehicles?	●		●	●		●							
Site.12b	Will the perimeter and facility barriers for protection against vehicles maintain access for emergency responders, including large fire apparatus?		●			●								
Site.13	Does site circulation prevent high-speed approaches by vehicles?	●		●			●							
Site.14	Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?		●	●			●							
Site.15	Is there a minimum setback distance between the building and parked vehicles?	●		●				●				●		
Site.16	Does adjacent surface parking maintain a minimum standoff distance?	●		●				●				●		
Site.17	Do stand-alone, above ground parking facilities provide adequate visibility across as well as into and out of the parking facility?		●	●				●	●					
Site.18	Are garage or service area entrances for employee-permitted vehicles protected by suitable anti-ram devices?		●	●		●	●							
Site.19	Do site landscaping and street furniture provide hiding places?	●		●					●					
Site.20a	Is the site lighting adequate from a security perspective in roadway access and parking areas?		●	●					●					
Site.20b	Are line-of-sight perspectives from outside the secured boundary to the building and on the property along pedestrian and vehicle routes integrated with landscaping and green space?		●	●		●			●					
Site.21	Do signs provide control of vehicles and people?		●	●										
Site.22	Are all existing fire hydrants on the site accessible?		●	●										

Table B: Architectural

Item	Vulnerability Question	Characterization					Terrorist Tactics						
		Type		Collection			Delivery Methods					Mechanisms	
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)
Arch.1	Does the site and architectural design incorporate strategies from a Crime Prevention Through Environmental Design (CPTED) perspective?		●	●			●	●					
Arch.2	Is it a mixed-tenant facility?	●		●	●	●							
Arch.3	Are pedestrian paths planned to concentrate activity to aid in detection?		●	●				●					
Arch.4	Are there trash receptacles and mailboxes in close proximity to the facility that can be used to hide explosive devices?		●	●							●		
Arch.5	Do entrances avoid significant queuing?	●		●		●							
Arch.6a	Does security screening cover all public and private areas?		●	●		●		●					
Arch.6b	Are public and private activities separated?	●		●		●							
Arch.6c	Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?		●	●				●					
Arch.7	Is access control provided through main entrance points for employees and visitors? (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)		●	●		●		●					
Arch.8	Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?		●	●		●		●					
Arch.9	Is access to elevators distinguished as to those that are designated only for employees and visitors?		●	●		●		●					
Arch.10	Do public and employee entrances include space for possible future installation of access control and screening equipment?		●	●		●		●					
Arch.11	Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?		●	●							●		
Arch.12	Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?		●	●	●								

Table B: Architectural (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Arch.13	Do circulation routes have unobstructed views of people approaching controlled access points?	●		●					●					
Arch.14	Is roof access limited to authorized personnel by means of locking mechanisms?		●	●		●			●					
Arch.15a	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking?	●		●	●	●	●	●	●			●		
Arch.15b	Are the critical building systems and components hardened?		●	●	●							●		
Arch.16	Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	●		●	●	●						●		
Arch.17	Is high visitor activity away from critical assets?	●				●			●					
Arch.18a	Are critical assets located in spaces that are occupied 24 hours per day?	●				●								
Arch.18b	Are assets located in areas where they are visible to more than one person?	●				●								
Arch.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?		●	●							●	●	●	●
Arch.20a	Are mailrooms located away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets?		●	●						●				
Arch.20b	Is the mailroom located near the loading dock?		●	●						●	●	●	●	●
Arch.21	Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?		●	●						●		●	●	●
Arch.22	Are areas of refuge identified, with special consideration given to egress?		●	●	●	●								

Table B: Architectural (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Arch.23a	Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur?		●	●								●		
Arch.23b	Are stairways maintained with positive pressure or are there other smoke control systems?		●	●	●								●	
Arch.24	Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?		●		●							●		
Arch.25	Do interior barriers differentiate level of security within a facility?	●		●	●	●								
Arch.26	Are emergency systems located away from high-risk areas?	●		●	●	●						●		
Arch.27a	Is interior glazing near high-threat areas minimized?		●	●								●		
Arch.27b	Is interior glazing in other areas shatter resistant?		●		●							●		

Table C: Structural Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
StrucSys.1a	What type of construction?	●		●	●							●		
StrucSys.1b	What type of concrete & reinforcing steel?		●		●							●		
StrucSys.1c	What type of steel?		●		●							●		
StrucSys.1d	What type of foundation?		●		●							●		
StrucSys.2a	Do the reinforced concrete structures contain symmetric steel reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams and girders that may be subjected to rebound, uplift and suction pressures?		●		●							●		
StrucSys.2b	Do the lap splices fully develop the capacity of the reinforcement?		●		●							●		
StrucSys.2c	Are lap splices and other discontinuities staggered?		●		●							●		
StrucSys.2d	Do the connections possess ductile details?		●		●							●		
StrucSys.2e	Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?		●		●							●		
StrucSys.3a	Are the steel frame connections moment connections?		●	●	●							●		
StrucSys.3b	Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system?	●		●	●							●		
StrucSys.3c	What are the floor-to-floor heights?	●		●	●							●		
StrucSys.4	Are critical elements vulnerable to failure?		●		●							●		
StrucSys.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?		●		●							●		
StrucSys.6a	Is the structure vulnerable to progressive collapse?	●		●	●							●		
StrucSys.6b	Is the facility capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?		●		●							●		

Table C: Structural Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
StrucSys.6c	In the event of an internal explosion in an uncontrolled public ground floor area does the design prevent progressive collapse due to the loss of one primary column?		●		●							●		
StrucSys.6d	Do architectural or structural features provide a minimum 6-inch standoff to the internal columns?		●	●	●							●		
StrucSys.6e	Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?		●		●							●		
StrucSys.7	Are there adequate redundant load paths in the structure?	●			●							●		
StrucSys.8	Are there transfer girders supported by columns within unscreened public spaces or at the exterior of the building?		●	●								●		
StrucSys.9	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?		●	●	●							●		
StrucSys.10	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?		●		●	●						●		

Table D: Building Envelope

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods				Mechanisms			
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
BldgEnv.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	●			●							●		
BldgEnv.2a	Is there less than 40 % fenestration openings per structural bay?		●	●								●		
BldgEnv.2b	Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)		●	●	●							●		
BldgEnv.2c	Do the glazing systems with a ½-inch bite contain an application of structural silicone?		●	●	●							●		
BldgEnv.2d	Is the glazing laminated or is it protected with an anti-shatter film?		●	●	●							●		
BldgEnv.2e	If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?		●	●	●							●		
BldgEnv.3a	Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected?		●		●							●		
BldgEnv.3b	Are the walls capable of withstanding the dynamic reactions from the windows?		●		●							●		
BldgEnv.3c	Will the anchorage remain attached to the walls of the facility during an explosive event without failure?		●		●							●		
BldgEnv.3d	Is the façade connected to back-up block or to the structural frame?		●	●	●							●		
BldgEnv.3e	Are non-bearing masonry walls reinforced?		●	●	●							●		
BldgEnv.4a	Does the facility contain ballistic glazing?		●	●	●							●		
BldgEnv.4b	Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing?		●	●	●									
BldgEnv.4c	Does the facility contain security-glazing?		●	●	●				●					
BldgEnv.4d	Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material?		●	●	●				●					
BldgEnv.4e	Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?		●	●	●				●					
BldgEnv.5	Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?		●	●	●							●	●	

Table E: Utility Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
UtilSys.1a	What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)	●		●	●									●
UtilSys.1b	Is there a secure alternate drinking water supply?		●	●	●	●								●
UtilSys.2	Are there multiple entry points for the water supply?		●	●	●									●
UtilSys.3	Is the incoming water supply in a secure location?		●	●	●	●								●
UtilSys.4a	Does the facility have storage capacity for domestic water?		●	●	●									●
UtilSys.4b	How many gallons and how long will it allow operations to continue?	●		●	●	●								●
UtilSys.5a	What is the source of water for the fire suppression system? (local utility company lines, storage tanks with utility company backup, lake, or river)	●		●	●									
UtilSys.5b	Are there alternate water supplies for fire suppression?	●		●	●	●								
UtilSys.6	Is the fire suppression system adequate, code-compliant, and protected (secure location)?		●	●	●									
UtilSys.7a	Do the sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation?		●	●							●			
UtilSys.7b	Are the sprinkler and standpipe connections adequate and redundant?	●		●	●									
UtilSys.7c	Are there fire hydrant and water supply connections near the sprinkler/standpipe connections?		●	●										
UtilSys.8a	Are there redundant fire water pumps (e.g., one electric, one diesel)?		●	●		●								
UtilSys.8b	Are the pumps located apart from each other?		●	●										
UtilSys.9a	Are sewer systems accessible?		●	●	●	●								
UtilSys.9b	Are they protected or secured?		●	●	●									
UtilSys.10	What fuel supplies do the facility rely upon for critical operation?	●		●	●	●								
UtilSys.11a	How much fuel is stored on the site or at the facility and how long can this quantity support critical operations?		●	●		●								

Table E: Utility Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
UtilSys.11b	How is it (fuel) stored?		●	●										
UtilSys.11c	How is it (fuel) secured?		●	●		●								
UtilSys.12a	Where is the fuel supply obtained?	●				●								
UtilSys.12b	How is it (fuel) delivered?		●			●								
UtilSys.13a	Are there alternate sources of fuel?	●				●								
UtilSys.13a	Are there alternate sources of fuel?	●				●								
UtilSys.13b	Can alternate fuels be used?	●			●	●								
UtilSys.14	What is the normal source of electrical service for the facility?	●		●	●									
UtilSys.15a	Is there a redundant electrical service source?		●		●	●								
UtilSys.15b	Can the facilities be fed from more than one utility substation?		●			●								
UtilSys.16	How may service entry points does the facility have for electricity?		●	●	●									
UtilSys.17	Is the incoming electric service to the building secure?		●	●		●								
UtilSys.18a	What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested?	●		●	●	●								
UtilSys.18b	Is the emergency power co-located with the commercial electric service?		●	●										
UtilSys.18c	Is there an exterior connection for emergency power?		●	●										
UtilSys.19	By what means does the main telephone and data communications interface the facility?	●		●	●	●								
UtilSys.20	Are there multiple or redundant locations for the telephone and communication service?		●	●	●	●								
UtilSys.21a	Does the fire alarm system require communication with external sources?		●		●	●								
UtilSys.21b	By what method is the alarm signal sent to the responding agency: telephone, radio, etc?		●		●	●								
UtilSys.21c	Is there an intermediary alarm monitoring center?		●		●	●								
UtilSys.22	Are utility lifelines aboveground, underground, or direct buried?		●	●	●									

Table F: Mechanical Systems (Including Chemical, Biological, and Radiological Systems)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
MechSys.1a	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure)	●		●	●								●	
MechSys.1b	Are the intakes accessible to the public?		●	●		●							●	
MechSys.2	Are there multiple air intake locations?	●		●	●								●	
MechSys.3a	What are the types of air filtration? Include the efficiency and number of filter modules for each of the main air handling systems.		●		●								●	
MechSys.3b	Is there any collective protection for chemical, biological, and radiological contamination designed into the facility?		●	●	●	●							●	
MechSys.4	Is there space for larger filter assemblies on critical air handling systems?		●	●	●								●	
MechSys.5	Are there provisions for air monitors or sensors for chemical or biological agents?		●	●	●								●	
MechSys.6	By what method are air intakes closed when not operational?		●			●							●	
MechSys.7a	How are air handling systems zoned?	●		●	●								●	
MechSys.7b	What areas and functions do each of the primary air handling systems serve?		●		●								●	
MechSys.8	Are there large central air handling units or are there multiple units serving separate zones?	●			●								●	
MechSys.9a	Are there any redundancies in the air handling system?	●			●	●							●	
MechSys.9b	Can critical areas be served from other units if a major system is disabled?		●		●	●							●	
MechSys.10	Is the air supply to critical areas compartmentalized?		●		●	●							●	
MechSys.11	Are supply and exhaust air systems for critical areas secure?		●		●	●							●	
MechSys.12a	What is the method of temperature and humidity control?		●	●	●	●							●	
MechSys.12b	Is it (temp. control) localized or centralized?		●	●	●	●								
MechSys.13a	Where are the building automation control centers and cabinets located?		●	●	●									

Table F: Mechanical Systems (Including Chemical, Biological, and Radiological Systems) (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
MechSys.13b	Are they in secure areas?		●	●	●	●								
MechSys.13c	How is the control wiring routed?		●	●	●									
MechSys.14	Does the control of air handling systems support plans for sheltering in place?		●		●	●								
MechSys.15	Where is roof-mounted equipment located on the roof?(near perimeter, at center of roof)	●		●										
MechSys.16	Are fire dampers installed at all fire barriers?		●	●	●									
MechSys.17	Do fire walls and fire doors maintain their integrity?		●	●	●									
MechSys.18	Do elevators have recall capability and elevator emergency message capability?		●	●	●	●								

Table G: Plumbing and Gas Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
PlumbGas.1	What is the method of water distribution?	●			●									●
PlumbGas.2	What is the method of gas distribution?, (heating, cooking, medical, process)	●			●									
PlumbGas.3	Is there redundancy to the main piping distribution?		●		●									
PlumbGas.4a	What is the method of heating domestic water?	●		●	●	●								
PlumbGas.4b	What fuel(s) is used?		●	●	●	●								
PlumbGas.5a	Where are gas storage tanks located? (heating, cooking, medical, process)		●	●										
PlumbGas.5b	How are they (gas tanks) piped to the distribution system?(above or below ground)		●	●	●									
PlumbGas.6	Are there reserve supplies of critical gases?	●			●	●								

Table H: Electrical Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
ElectSys.1a	Are there any transformers or switchgears located outside the building or accessible from the building exterior?	●		●										
ElectSys.1b	Are they (transformers or switchgears) vulnerable to public access?	●		●		●								
ElectSys.1c	Are they (transformers or switchgears) secured?		●	●		●								
ElectSys.2	What is the extent of the external facility lighting in utility and service areas and at normal entryways used by the building occupants?			●	●									
ElectSys.3	How are the electrical rooms secured and where are they located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance?		●	●	●	●								
ElectSys.4a	Are critical electrical systems co-located with other building systems?		●	●										
ElectSys.4b	Are critical electrical systems located in areas outside of secured electrical areas?	●		●	●	●								
ElectSys.4c	Is security system wiring located separately from electrical and other service systems?		●	●	●									
ElectSys.5	How are electrical distribution panels serving branch circuits secured or are they in secure locations?		●	●	●	●								
ElectSys.6a	Does emergency backup power exist for all areas within the facility or for critical areas only?	●		●	●									
ElectSys.6b	How is the emergency power distributed?		●		●	●								
ElectSys.6c	Is the emergency power system independent from the normal electrical service, particularly in critical areas?		●		●									
ElectSys.7a	How is the primary electrical system wiring distributed?		●		●	●								
ElectSys.7b	Is it co-located with other major utilities?		●	●	●									
ElectSys.7c	Is there redundancy of distribution to critical areas?		●	●	●	●								

Table I: Fire Alarm Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
FireAlarm.1a	Is the facility fire alarm system centralized or localized?		●	●	●									
FireAlarm.1b	How are alarms annunciated, both locally and centrally?		●	●	●	●								
FireAlarm.1c	Are critical documents and control systems located in a secure yet accessible location?		●	●		●								
FireAlarm.2a	Where are the fire alarm panels located?		●	●										
FireAlarm.2b	Are they allow access to unauthorized personnel?		●	●		●								
FireAlarm.3a	Is the fire alarm system stand-alone or integrated with other functions such as security and environmental or building management systems?	●			●	●								
FireAlarm.3b	What is the interface?		●		●	●								
FireAlarm.4	Do key fire alarm system components have fire- and blast-resistant separation?		●	●	●						●			
FireAlarm.5	Is there redundant off-premises fire alarm reporting?	●			●	●								

Table J: Communications and IT Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
CommIT.1a	Where is the main telephone distribution room and where is it in relation to higher risk areas?	●		●	●	●								
CommIT.1b	Is the main telephone distribution room secure?		●	●		●								
CommIT.2a	Does the telephone system have an UPS (uninterruptible power supply)?		●		●	●								
CommIT.2b	What is its (ups) type, power rating, operational duration under load, and location? (battery, on-line, filtered)		●		●									
CommIT.3a	Where are communication systems wiring closets located? (voice, data, signal, alarm)	●		●	●									
CommIT.3b	Are they (communication closets) co-located with other utilities?		●	●	●									
CommIT.3c	Are they (communication closets) in secure areas?		●	●	●	●								
CommIT.4	How is communications system wiring distributed? (secure chases and risers, accessible public areas)		●	●	●									
CommIT.5	Are there redundant communications systems available?		●		●	●								
CommIT.6a	Where are the main distribution facility, data centers, routers, firewalls, and servers located?		●		●									
CommIT.6b	Where are the secondary and/or intermediate (IT) distribution facilities?		●		●									
CommIT.7	What type and where are the WAN (wide area network) connections?		●	●	●									
CommIT.8a	What type, power rating, and location of the UPS (uninterruptible power supply)? (battery, on-line, filtered)		●	●	●									
CommIT.8b	Are the UPS also connected to emergency power?		●	●	●									
CommIT.9	What type of LAN (local area network) cabling and physical topology is used? (Category(Cat) 5, Gigabit Ethernet, Ethernet, Token Ring)		●	●	●									
CommIT.10	For installed radio/wireless systems, what are their types and where are they located? (RF (radio frequency), HF (high frequency), VHF (very high frequency), MW (medium wave))		●	●	●									

Table J: Communications and IT Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
CommIT.11	Do the IT (Information Technology - computer) systems meet requirements of confidentiality, integrity, and availability?		●		●	●								
CommIT.12	Where is the disaster recovery/mirroring site?		●		●	●								
CommIT.13	Where is the back-up tape/file storage site and what is the type of safe environment? (safe, vault, underground)Is there redundant refrigeration in the (backup IT storage) site?		●		●	●								
CommIT.14	Are there any SATCOM (satellite communications) links? (location, power, UPS, emergency power, spare capacity/capability)		●	●	●									
CommIT.15a	Is there a mass notification system that reaches all building occupants? (public address, pager, cell phone, computer override, etc.)		●			●								
CommIT.15b	Will one or more of these systems be operational under hazard conditions? (UPS, emergency power)		●		●	●								
CommIT.16a	Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass notification, etc.? (emergency operations, security, fire alarms, building automation)		●		●	●								
CommIT.16b	Do the alternate locations also have access to backup systems, including emergency power?		●			●								

Table K: Equipment Operations and Maintenance

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
EquipOM.1a	Are there composite drawings indicating location and capacities of major systems and are they current? (electrical, mechanical, and fire protection; and date of last update)		●		●									
EquipOM.1b	Do updated O&M (operation and maintenance) manuals exist?		●		●									
EquipOM.2a	Have critical air systems been rebalanced?		●		●	●								
EquipOM.2b	If so, when and how often?		●			●								
EquipOM.3	Is air pressurization monitored regularly?		●			●								
EquipOM.4	Does the facility have a policy or procedure for periodic recommissioning of major Mechanical/Electrical/Plumbing systems?		●			●								
EquipOM.5	Is there an adequate operations and maintenance program including training of facilities management staff?		●			●								
EquipOM.6	What maintenance and service agreements exist for M/E/P systems?		●		●									
EquipOM.7	Are backup power systems periodically tested under load?		●			●								
EquipOM.8	Is stairway and exit sign lighting operational?		●	●										

Table L: Security Systems

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecPerim.1a	Are black/white or color CCTV (closed circuit television) cameras used?		●	●			●		●					
SecPerim.1b	Are they monitored and recorded 24 hours/7 days a week? By whom?		●			●	●		●					
SecPerim.1c	Are they analog or digital by design?		●		●		●		●					
SecPerim.1d	What are the number of fixed, wireless and pan-tilt-zoom cameras used?		●	●	●		●		●					
SecPerim.1e	Who are the manufacturers of the CCTV cameras?		●	●	●		●		●					
SecPerim.1f	What is the age of the CCTV cameras in use?		●		●	●	●		●					
SecPerim.2a	Are the cameras programmed to respond automatically to perimeter building alarm events?		●			●	●		●					
SecPerim.2b	Do they have built-in video motion capabilities?		●		●		●		●					
SecPerim.3	What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?		●	●	●		●		●					
SecPerim.4	Are panic/duress alarm buttons or sensors used, where are they located and are they hardwired or portable?		●	●			●		●					
SecPerim.5	Are intercom call boxes used in parking areas or along the building perimeter?		●	●		●	●		●					
SecPerim.6	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?		●	●	●		●		●					
SecPerim.7	Who monitors the CCTV system?		●			●	●		●					
SecPerim.8a	What is the quality of video images both during the day and hours of darkness?		●	●		●	●		●					
SecPerim.8b	Are infrared camera illuminators used?		●	●		●	●		●					
SecPerim.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?		●		●		●		●					
SecPerim.10	What type of exterior IDS sensors are used: electromagnetic, fiber optic, active infrared, bistatic microwave, seismic, photoelectric, ground, fence, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches.		●	●	●		●		●					

Table L: Security Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org./Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecPerim.11	Is a global positioning satellite system (GPS) used to monitor vehicles and asset movements?		●		●	●	●							
SecInter.12a	Are black/white or color CCTV (closed circuit television) cameras used?		●	●					●					
SecInter.12b	Are they monitored and recorded 24 hours/7 days a week? By whom?		●			●			●					
SecInter.12c	Are they analog or digital by design?		●		●				●					
SecInter.12d	What are the number of fixed, wireless and pan-tilt-zoom cameras used?		●	●	●				●					
SecInter.12e	Who are the manufacturers of the CCTV cameras?		●	●	●				●					
SecInter.12f	What is the age of the CCTV cameras in use?		●		●	●			●					
SecInter.13a	Are the cameras programmed to respond automatically to perimeter building alarm events?		●			●			●					
SecInter.13b	Do they have built-in video motion capabilities?		●		●				●					
SecInter.14	What type of camera housings are used and are they designed to protect against exposure or tampering?		●	●	●				●					
SecInter.15	Are the camera lenses used of the proper specifications, especially distance viewing and clarity?		●		●	●			●					
SecInter.16	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?		●	●	●				●					
SecInter.17	Is the quality in interior camera video images of good visual and recording quality?		●	●		●			●					
SecInter.18	Are the interior cameras supported by an uninterruptible power supply source, battery, or building emergency power?		●		●				●					
SecInter.19	What are the first costs and maintenance costs associated with the interior cameras?		●		●	●			●					
SecInter.20a	What type of security access control system is used?		●			●			●					
SecInter.20b	Are these same devices used for physical security also used (integrated) with providing access control to security computer networks (e.g. in place of or in combination with user ID and system passwords)?		●		●	●			●					

Table L: Security Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods				Mechanisms			
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecInter.23b	How old are the systems and what are the related first and maintenance service costs?		●		●	●			●					
SecInter.24	Are there panic/duress alarm sensors used, where are they located and are they hardwired or portable?		●	●	●				●					
SecInter.25	Are intercom call-boxes or building intercom system used throughout the facility?		●	●	●	●			●					
SecInter.26	Are magnetometers (metal detectors) and x-ray equipment used and at what locations within the facility?		●	●					●					
SecInter.27	What type of interior IDS sensors are used: electromagnetic, fiber optic, active infrared-motion detector, photoelectric, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches?		●	●	●				●					
SecInter.28	Are mechanical, electrical, medical gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms continuously locked, under electronic security CCTV camera and intrusion alarm systems surveillance?		●			●			●					
SecInter.29	What types of locking hardware are used throughout the facility? Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes and related hardware and software used?		●	●					●					
SecInter.30	Are any potentially hazardous chemicals, combustible or toxic materials stored on-site in non-secure and non-monitored areas?		●			●								
SecInter.31	What security controls are in place to handle the processing of mail and protect against potential biological, explosive or other threatening exposures?		●			●								
SecInter.32a	Is there a designated security control room and console in place to monitor security, fire alarm and possibly other building systems?		●	●					●					
SecInter.32b	Is there a backup control center designated and equipped?		●	●	●				●					

Table L: Security Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods				Mechanisms			
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecInter.32c	Is there off-site 24-hour monitoring of intrusion detection systems?		●			●			●					
SecInter.33	Is the security console and control room adequate in size, provide room for expansion, have adequate environment controls (e.g. a/c, lighting, heating, air circulation, backup power, etc.) and is ergonomically designed?		●	●										
SecInter.34	Is the location of the security room in a secure area with limited, controlled and restricted access controls in place?		●	●		●								
SecInter.35a	What are the means by which facility and security personnel can communicate with one another: portable radio, pager, cell phone, personal data assistants (PDA's), etc)?		●			●								
SecInter.35b	What problems have been experienced with these and other electronic security systems?		●			●								
SecInter.36	Is there a computerized security incident reporting system used to prepare reports and track security incident trends and patterns?		●			●								
SecInter.37	Does the present security force have access to use a computerized guard tour system?		●			●								
SecInter.38a	Are vaults or safes in the facility?		●	●										
SecInter.38b	Where are they located?		●	●										
SecDocs.39	Are security system as-built drawings been generated and ready for review?		●		●									
SecDocs.40	Have security system design and drawing standards been developed?		●		●									
SecDocs.41	Are security equipment selection criteria defined?		●		●									
SecDocs.42	What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?		●		●									
SecDocs.43	Have security system construction specification documents been prepared and standardized?		●		●									
SecDocs.44	Are all security system documents to include as-built drawings current?		●		●									

Table L: Security Systems (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecDocs.45	Have qualifications been determined in using security consultants, system designers and engineers, installation vendors, and contractors?		●			●								
SecDocs.46	Are security systems decentralized, centralized, integrated, and operate over existing IT network or standalone method of operation?		●		●	●								
SecDocs.47	What security systems manuals are available?		●		●									
SecDocs.48	What maintenance or service agreements exist for security systems?		●		●									

Table M: Security Master Plan

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecPlan.1a	Does a written security plan exist for this facility?		●		●									
SecPlan.1b	When was the initial security plan written and last revised?		●		●									
SecPlan.1c	Who is responsible for preparing and reviewing the security plan?		●			●								
SecPlan.2	Has the security plan been communicated and disseminated to key management personnel and departments?		●			●								
SecPlan.3	Has the security plan been benchmarked or compared against related organizations and operational entities?		●			●								
SecPlan.4	Has the security plan ever been tested and evaluated from a cost-benefit and operational efficiency and effectiveness perspective?		●			●								
SecPlan.5	Does it define mission, vision, short-long term security program goals and objectives?		●			●								
SecPlan.6	Are threats, vulnerabilities, risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?		●			●								
SecPlan.7	Has a security implementation schedule been established to address recommended security solutions?		●			●								
SecPlan.8	Have security operating and capital budgets been addressed, approved and established to support the plan?		●		●	●								
SecPlan.9	What regulatory or industry guidelines/standards were followed in the preparation of the security plan?		●		●	●								
SecPlan.10	Does the security plan address existing security conditions from an administrative, operational, managerial and technical security systems perspective?		●		●	●								
SecPlan.11	Does the security plan address the protection of people, property, assets, and information?		●		●	●								
SecPlan.12	Does the security plan address the following major components: access control, surveillance, response, building hardening and protection against biological, chemical, radiological and cyber-network attacks?		●		●	●								

Table M: Security Master Plan (continued)

Item	Vulnerability Question	Characterization					Terrorist Tactics							
		Type		Collection			Delivery Methods					Mechanisms		
		Vulnerability estimate	Detailed assessment	Visual inspection	Document review	Org//Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
SecPlan.13	Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?		●		●	●								
SecPlan.14a	When was the last security assessment performed?		●		●	●								
SecPlan.14b	Who performed the security risk assessment?		●		●	●								
SecPlan.15a	Were the following areas of security analysis addressed in the security master plan: Asset Analysis: Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current value, and replacement value?		●		●									
SecPlan.15b	Threat Analysis: Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? (possible criminal acts (documented and review of police/security incident reports) associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings)		●		●									
SecPlan.15c	Vulnerability Analysis: Does the security plan address other areas and anything else associated with a facility and it's operations that can be taken advantage of to carry out a threat? (architectural design and construction of new and existing facilities, technological support systems (e.g. heating, air conditioning, power, lighting and security systems, etc.) and operational procedures, policies and controls)		●		●									
SecPlan.15d	Risk Analysis: Does the security plan address the findings from the asset, threat, and vulnerability analyses to develop, recommend and consider implementation of appropriate security countermeasures?		●		●									

A

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

Access Control Point. A station at an entrance to a building or a portion of a building where identification is checked and people and hand-carried items are searched.

Access Controls. Procedures and controls that limit or detect access to minimum essential infrastructure resource elements (people, technology, applications, data and/or facilities), thereby protecting these resources against loss of integrity, confidentiality, accountability and/or availability.

Access Control System. Also referred to as an electronic entry control system; an electronic system that controls entry and egress from a building or area.

Access Control System Elements. Detection measures used to control vehicle or personnel entry into a protected area. Access control system elements include locks, electronic entry control systems, and guards.

Access Group. A software configuration of an access control system that group together access points or authorized users for easier arrangement and maintenance of the system.

Access Road. Any roadway such as a maintenance, delivery, service, emergency, or other special limited use road that is necessary for the operation of a building or structure.

Accountability. The explicit assignment of responsibilities for oversight of areas of control to executives, managers, staff, owners, providers, and users of minimum essential infrastructure resource elements.

Acoustic Eavesdropping. The use of listening devices to monitor voice communications or other audibly transmitted information with the objective to compromise information.

Active Vehicle Barrier. An impediment placed at an access control point which may be manually or automatically deployed in response to detection of a threat.

Aerosol. Fine liquid or solid particles suspended in a gas, for example, fog or smoke.

Aggressor. Any person seeking to compromise a function or structure.

Airborne Contamination. Chemical or biological agents introduced into and fouling the source of supply breathing or conditioning air.

Airlock. A building entry configuration with which airflow from the outside can be prevented from entering a toxic-free area. An airlock uses two doors, only one of which can be opened at a time, and a blower system to maintain positive air pressures and purge contaminated air from the airlock before the second door is opened.

Alarm Assessment. Verification and evaluation of an alarm alert through the use of closed circuit television or human observation. Systems used for alarm assessment are designed to respond rapidly, automatically, and predictably to the receipt of alarms at the security center.

Alarm Printers. Alarm printers provide a hard-copy of all alarm events and system activity, as well as limited backup in case the visual display fails.

Alarm Priority. A hierarchy of alarms by order of importance. This is often used in larger systems to give priority to alarm with greater importance.

Annunciation. A visual, audible, or other indication by a security system of a condition.

Antiterrorism. Defensive measures used to reduce the vulnerability of individuals, forces, and property to terrorist acts.

Area Commander. A military commander with authority in a specific geographical area or military installation.

Area Lighting. Lighting which illuminates a large exterior area.

Areas of Potential Compromise. Categories where losses can occur that will impact either a department or agency's minimum essential infrastructure and its ability to conduct core functions and activities.

Assessment. The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Assessment System Elements. Detection measures used to assist guards in visual verification of intrusion detection system alarms and access control system functions and to assist in visual detection by guards. Assessment system elements include closed-circuit television and protective lighting.

Asset. A resource of value requiring protection. An asset can be tangible such as people, buildings, facilities, equipment, activities, operations, and information; or intangible, such as processes or a company's information and reputation.

Asset Value. The degree of debilitating impact that would be caused by the incapacity or destruction of an asset.

Asset Protection. Security program designed to protect personnel, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

Attack. A hostile action resulting in the destruction, injury or death to the civilian population, or damage or destruction to public and private property.

Audible Alarm Devices. An alarm device which produces an audible announcement (bell, horn, siren, etc.) of an alarm condition.

B

Balanced Magnetic Switch. A door position switch utilizing a reed switch held in a balanced or center position by interacting magnetic fields when not in alarm condition.

Ballistics Attack. Attack in which small arms (such as pistols, submachine guns, shotguns, and rifles) are fired from a distance and rely on the flight of the projectile to damage the target.

Barbed Tape or Concertina. A coiled tape or coil of wires with wire barbs or blades deployed as an obstacle to human trespass or entry into an area.

Barbed Wire. A double strand of wire with four-point barbs equally spaced along the wire deployed as an obstacle to human trespass or entry into an area.

Barcode. Black bars printed on white paper or tape that can be easily read with an optical scanner.

Biological Agents. Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

Biometrics. The use of physical characteristics of the human body as a unique identification method.

Biometric Reader. A device that gathers and analyzes biometric features.

Blast Curtains. Heavy curtains made of blast resistant materials that could protect the occupants of a room from flying debris.

Blast-Resistant Glazing. Window opening glazing that is resistant to blast effects because of the interrelated function of the frame and glazing material properties frequently dependent upon tempered glass, polycarbonate, or laminated glazing.

Blast Vulnerability Envelope. The geographical area in which an explosive device will cause damage to assets.

Bollard. A vehicle barrier consisting of a cylinder, usually made of steel and sometimes filled with concrete, placed on end in the ground and spaced about 3 feet apart to prevent vehicles from passing, but allowing entrance of pedestrians and bicycles.

Boundary Penetration Sensors. Interior intrusion detection sensors which detect an attempt by individuals to penetrate or enter a building.

Building Hardening. Enhanced construction that reduces vulnerability to external blast and ballistic attack.

Building Separation. The distance between closest points on the exterior walls of adjacent buildings or structures.

Business Continuity Program. An ongoing process supported by senior management and funded to insure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity services through personnel training, plan testing and maintenance.



Cable Barrier. Cable or wire rope anchored to and suspended off the ground or attached to chain link fence to act as a barrier to moving vehicles.

Capacitance Sensor. A device that detects an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground.

Card Reader. A device that gathers or reads information when a card is presented as an identification method.

Chemical Agent. A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by severity of effect: lethal, blister, and incapacitating.

Clear Zone. An area that is clear of visual obstructions and landscape materials that could conceal a threat or perpetrator.

Closed Circuit Television (CCTV). An electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.

CCTV Pan-Tilt-Zoom Camera (PTZ). A CCTV camera that can move side to side, up and down, and zoom in or out.

CCTV Pan-Tilt-Zoom Control. The method of controlling the PTZ functions of a camera.

CCTV Pan-Tilt-Zoom Controller. The operator interface for performing PTZ control.

CCTV Switcher. A piece of equipment capable of presenting any of multiple video images to various monitors, recorders, and so forth.

Chimney Effect. Air movement in a building between floors caused by differential air temperature (differences in density), between the air inside and outside the building. It occurs in vertical shafts, such as elevator, stairwell, and conduit/wiring/piping chase. Hotter air inside the building will rise and be replaced by infiltration with colder outside air through the lower portions of the building. Conversely, reversing the temperature will reverse the flow (down the chimney). Also known as stack effect.

Collateral Damage. Injury or damage to assets that are not the primary target of an attack.

Combating Terrorism. The full range of federal programs and activities applied against terrorism, domestically and abroad, regardless of the source or motive.

Community. A political entity which has the authority to adopt and enforce laws and ordinances for the area under its jurisdiction. In most cases, the community is an incorporated town, city, township, village, or unincorporated area of a county. However, each State defines its own political subdivisions and forms of government.

Components and Cladding. Elements of the building envelope that do not qualify as part of the main wind-force resisting system.

Confidentiality. The protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.

Consequence Management. Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. state and local governments exercise primary authority to respond to the consequences of terrorism.

Contamination. The undesirable deposition of a chemical, biological, or radiological material on the surface of structures, areas, objects, or people.

Continuity of Services and Operations. Controls to ensure that, when unexpected events occur, departmental/agency minimum essential infrastructure services and operations, including computer operations, continue without interruption or are promptly resumed and critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.

Control Center. A centrally located room or facility staffed by personnel charged with the over sight of specific situations and/or equipment.

Controlled Area. An area into which access is controlled or limited. It is that portion of a restricted area usually near or surrounding a limited or exclusion area. Correlates with exclusion zone.

Controlled Lighting. Lighting illumination of specific areas or sections.

Controlled Perimeter. A physical boundary at which vehicle and personnel access is controlled at the perimeter of a site. Access control at a controlled perimeter should demonstrate the capability to search individuals and vehicles.

Conventional Construction. Building construction that is not specifically designed to resist weapons, explosives, or chemical, biological and radiological effects. Conventional construction is designed only to resist common loadings and environmental effects such as wind, seismic, and snow loads.

Coordinate. To advance systematically an exchange of information among principals who have or may have a need to know certain information in order to carry out their role in a response.

Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.

Counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism.

Covert Entry. Attempts to enter a facility by using false credentials or stealth.

Crash Bar. A mechanical egress device located on the interior side of a door that unlocks the door when pressure is applied in the direction of egress.

Crime Prevention Through Environmental Design (CPTED). A crime prevention strategy based on evidence that the design and form of the built environment can influence human behavior. CPTED usually involves the use of three principles: natural surveillance (by placing physical features, activities, and people to maximize visibility); natural access control (through the judicious placement of entrances, exits, fencing, landscaping, and lighting); and territorial reinforcement (using buildings, fences, pavement, signs, and landscaping to express ownership).

Crisis Management. The measures taken to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

Critical Assets. Those assets essential to the minimum operations of the organization, and to ensure the health and safety of the general public.

Critical Infrastructure. Primary infrastructure systems (utilities, telecommunications, transportation, etc.) whose incapacity would have a debilitating impact on the organization's ability to function.

D

Damage Assessment. The process used to appraise or determine the number of injuries and deaths, damage to public and private property, and the status of key facilities and services such as hospitals and other health care facilities, fire and police stations, communications networks, water and sanitation systems, utilities, and transportation networks resulting from a man-made or natural disaster.

Data Gathering Panel. A local processing unit that retrieves, processes, stores, and / or acts on information in the field.

Data Transmission Equipment. A path for transmitting data between two or more components (such as a sensor and alarm reporting system, a card reader and controller, a CCTV camera and monitor, or a transmitter and receiver).

Decontamination. The reduction or removal of a chemical, biological, or radiological material from the surface of a structure, area, object, or person.

Defense Layer. Building design or exterior perimeter barriers intended to delay attempted forced entry.

Defensive Measures. Protective measures which delay or prevent attack on an asset or which shield the asset from weapons, explosives, and CBR effects. Defensive measures include site work and building design.

Delay Rating. A measure of the effectiveness of penetration protection of a defense layer.

Design Basis Threat. The threat (tactics, and associated weapons, tools, or explosives) against which assets within a building must be protected and upon which the security engineering design of the building is based.

Design Constraint. Anything which restricts the design options for a protective system or which creates additional problems for which the design must compensate.

Design Opportunity. Anything which enhances protection, reduces requirements for protective measures, or solves a design problem.

Design Team. A group of individuals from various engineering and architectural disciplines responsible for the protective system design.

Detection Layer. A ring of intrusion detection sensors located on or adjacent to a defensive layer or between two defensive layers.

Detection Measures. Protective measures which detect intruders, weapons, or explosives; assist in assessing the validity of detection; control access to protected areas; and communicate the appropriate information to the response force. Detection measures include detection system, assessment system, and access control system elements.

Detection System Elements. Detection measures which detect the presence of intruders, weapons, or explosives. Detection system elements include intrusion detection systems, weapons and explosives detectors, and guards.

Disaster. An occurrence of a natural catastrophe, technological accident or human-caused event that has resulted in severe property damage, deaths, and/or multiple injuries.

Disaster Field Office (DFO). The office established in or near the designated area of a Presidentially declared major disaster to support federal and state response and recovery operations.

Disaster Recovery Center (DRC). Places established in the area of a Presidentially declared major disaster, as soon as practicable, to provide victims the opportunity to apply in person for assistance and/or obtain information relating to that assistance.

Domestic Terrorism. The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

Door Position Switch. A switch that changes state based on whether or not a door is closed. Typically, a switch mounted in a frame that is actuated by a magnet in a door.

Door Strike, Electronic. An electro-mechanical lock that releases a door plunger to unlock the door. Typically, an electronic door strike is mounted in place of or near a normal door strike plate.

Dose Rate (Radiation). A general term indicating the quantity (total or accumulated) of ionizing radiation or energy absorbed by a person or animal per unit of time.

Dosimeter. An instrument for measuring and registering total accumulated exposure to ionizing radiation.

Dual Technology Sensors. Sensors that combine two different technologies in one unit.

Duress Alarm Devices. Also known as panic buttons, these devices are designated specifically to initiate a panic alarm.



Effective Standoff Distance. A standoff distance at which the required level of protection can be shown to be achieved through analysis or can be achieved through building hardening or other mitigating construction or retrofit.

Electromagnetic Pulse (EMP). A sharp pulse of energy radiated instantaneously by a nuclear detonation which may affect or damage electronic components and equipment. EMP can also be generated in lesser intensity by non-nuclear means in specific frequency ranges to perform the same disruptive function.

Electronic Emanations. Electro-magnetic emissions from computers, communications, electronics, wiring and related equipment.

Electronic-Emanations Eavesdropping. Use of electronic-emanation surveillance equipment from outside a facility or its restricted area to monitor electronic emanations from computers, communications, and related equipment.

Electronic Entry Control Systems. Electronic devices which automatically verify authorization for a person to enter or exit a controlled area.

Electronic Security System. An integrated system which encompasses interior and exterior sensors, closed-circuit television systems for assessment of alarm conditions, electronic entry control systems, data transmission media, and alarm reporting systems for monitoring, control, and display of various alarm and system information.

Emergency. Any natural or man-caused situation that results in or may result in substantial injury or harm to the population or substantial damage to or loss of property.

Emergency Alert System. A communications system of broadcast stations and interconnecting facilities authorized by the Federal Communication Commission. The system provides the President and other national, state, and local officials the means to broadcast emergency information to the public before, during, and after disasters.

Emergency Environmental Health Services. Services required to correct or improve damaging environmental health effects on humans, including inspection for food contamination, inspection for water contamination, and vector control; providing for sewage and solid waste inspection and disposal; cleanup and disposal of hazardous materials; and sanitation inspection for emergency shelter facilities.

Emergency Medical Services. Services including personnel, facilities, and equipment required to ensure proper medical care for the sick and injured from the time of injury to the time of final disposition, including medical disposition within a hospital, temporary medical facility, or special care facility, release from site, or declared dead. Further, emergency medical services specifically include those services immediately required to ensure proper medical care and specialized treatment for patients in a hospital and coordination of related hospital services.

Emergency Mortuary Services. Services required to assure adequate death investigation, identification, and disposition of bodies; removal, temporary storage, and transportation of bodies to temporary morgue facilities; notification of next of kin; and

coordination of mortuary services and burial of unclaimed bodies.

Emergency Operations Center. The protected site from which state and local civil government officials coordinate, monitor, and direct emergency response activities during an emergency.

Emergency Operations Plan. A document that: describes how people and property will be protected in disaster and disaster threat situations; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available for use in the disaster; and outlines how all actions will be coordinated.

Emergency Planning Zones. Areas around a facility for which planning is needed to ensure prompt and effective actions are taken to protect the health and safety of the public if an accident or disaster occurs. In the Radiological Emergency Preparedness Program the two EPZ's are:

Plume Exposure Pathway (10-mile EPZ). A circular geographic zone (with a 10-mile radius centered at the nuclear power plant) for which plans are developed to protect the public against exposure to radiation emanating from a radioactive plume caused as a result of an accident at the nuclear power plant.

Ingestion Pathway (50-mile EPZ). A circular geographic zone (with a 50-mile radius centered at the nuclear power plant) for which plans are developed to protect the public from the ingestion of water or food contaminated as a result of a nuclear power plant accident.

In Chemical Stockpile Emergency Preparedness Program, the EPZ is divided into three concentric circular zones:

Immediate Response Zone (IRZ). A circular zone ranging from 10 to 15 kilometers (6 to 9 miles) from the potential chemical event source, depending on the stockpile location on-post. Emergency response plans developed for the IRZ must provide for the most rapid and effective

protective actions possible, since the IRZ will have the highest concentration of agent and the least amount of warning time.

Protective Action Zone (PAZ). An area that extends beyond the IRZ to approximately 16 to 50 kilometers (10 to 30 miles) from the stockpile location. The PAZ is that area where public protective actions may still be necessary in case of an accidental release of chemical agent, but where the available warning and response time is such that most people could evacuate. However, other responses (e.g., sheltering) may be appropriate for institutions and special populations that could not evacuate within the available time.

Precautionary Zone (PZ). The outermost portion of the EPZ for CSEPP, extending from the PAZ outer boundary to a distance where the risk of adverse impacts to humans is negligible. Because of the increased warning and response time available for implementation of response actions in the PZ, detailed local emergency planning is not required, although consequence management planning may be appropriate.

Emergency Public Information. Information which is disseminated primarily in anticipation of an emergency or at the actual time of an emergency and in addition to providing information, frequently directs actions, instructs, and transmits direct orders.

Emergency Response Team (ERT). An interagency team, consisting of the lead representative from each federal department or agency assigned primary responsibility for an ESF and key members of the FCO's staff, formed to assist the FCO in carrying out his/her coordination responsibilities.

Emergency Response Team Advance Element (ERT-A). For federal disaster response and recovery activities under the Stafford Act, the portion of the ERT that is first deployed to the field to respond to a disaster incident. The ERT-A is the nucleus of the full ERT.

Emergency Response Team National (ERT-N). An ERT that has been established and rostered for deployment to catastrophic disasters where the resources of the FEMA Region have been, or are expected to be, overwhelmed. Three ERT-Ns have been established.

Emergency Support Function (ESF). In the Federal Response Plan (FRP), a functional area of response activity established to facilitate the delivery of federal assistance required during the immediate response phase of a disaster to save lives, protect property and public health, and to maintain public safety. ESFs represent those types of federal assistance which the state will most likely need because of the impact of a catastrophic or significant disaster on its own resources and response capabilities, or because of the specialized or unique nature of the assistance required. ESF missions are designed to supplement state and local response efforts.

Emergency Support Team (EST). An interagency group operating from FEMA headquarters. The EST oversees the national-level response support effort under the FRP and coordinates activities with the ESF primary and support agencies in supporting federal requirements in the field.

Entity-Wide Security. Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.

Entry Control Point. A continuously or intermittently manned station at which entry to sensitive or restricted areas is controlled.

Entry-Control Stations. Entry-control stations should be provided at main perimeter entrances where security personnel are present. Entry-control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.

Equipment Closet. A room where field control equipment such as data gathering panels and power supplies are typically located.

Evacuation. Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.

Evacuation, Spontaneous. Residents or citizens in the threatened areas observe an emergency event or receive unofficial word of an actual or perceived threat and without receiving instructions to do so, elect to evacuate the area. Their movement, means, and direction of travel is unorganized and unsupervised.

Evacuation, Voluntary. This is a warning to persons within a designated area that a threat to life and property exists or is likely to exist in the immediate future. Individuals issued this type of warning or order are NOT required to evacuate, however it would be to their advantage to do so.

Evacuation, Mandatory or Directed. This is a warning to persons within the designated area that an imminent threat to life and property exists and individuals MUST evacuate in accordance with the instructions of local officials.

Evacuees. All persons removed or moving from areas threatened or struck by a disaster.

Exclusion Area. A restricted area containing a security interest. Uncontrolled movement permits direct access to the item. See controlled area and limited area.

Exclusive Zone. An area around an asset which has controlled entry with highly restrictive access. See controlled area.

Explosives Disposal Container. A small container into which small quantities of explosives may be placed to contain their blast pressures and fragments if the explosive detonates.



Facial Recognition. A biometric technology that is based on features of the human face.

Federal Coordinating Officer (FCO). The person appointed by the FEMA Director to coordinate federal assistance in a Presidentially declared emergency or major disaster.

Federal On-Scene Commander. The FBI official designated upon JOC activation to ensure appropriate coordination of the overall U.S. Government response with federal, state and local authorities, until such time as the Attorney General transfers the LFA role to FEMA.

Federal Response Plan (FRP). The FRP establishes a process and structure for the systematic, coordinated, and effective delivery of federal assistance to address the consequences of any major disaster or emergency.

Fence Protection. An intrusion detection technology that detects a person crossing a fence by various methods such as climbing, crawling, cutting, etc.

Fence Sensors. Exterior intrusion detection sensors which detect aggressors as they attempt to climb over, cut through, or otherwise disturb a fence.

Fiber Optics. A method of data transfer by passing bursts of light through a strand of glass or clear plastic.

Field Assessment Team (FAsT). A small team of pre-identified technical experts that conduct an assessment of response needs (not a PDA) immediately following a disaster.

Field of View. The visible area in a video picture.

First Responder. Local police, fire, and emergency medical personnel who first arrive on the scene of an incident and take

action to save lives, protect property, and meet basic human needs.

Flash Flood. Follows a situation in which rainfall is so intense and severe and runoff so rapid that it precludes recording and relating it to stream stages and other information in time to forecast a flood condition.

Flood. A general and temporary condition of partial or complete inundation of normally dry land areas from overflow of inland or tidal waters, unusual or rapid accumulation or runoff of surface waters, or mudslides/mudflows caused by accumulation of water.

Forced Entry. Entry to a denied area achieved through force to create an opening in fence, walls, doors, etc., or to overpower guards.

Fragment Retention Film. A thin, optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered.

Frame Rate. In digital video, a measurement of the rate of change in a series of pictures, often measured in frames per second (fps).

Frangible Construction. Building components which are designed to fail to vent blast pressures from an enclosure in a controlled manner and direction.



Glare Security-Lighting. Illumination projected from a secure perimeter into the surrounding area making it possible to see potential intruders at a considerable distance while making it difficult to observe activities within the secure perimeter.

Glass-Break Detector. Intrusion detection sensors that are designed to detect breaking glass either through vibration or acoustics.

Glazing. A material installed in a sash, ventilator, or panes such as glass, plastic, etc., including material such as thin granite installed in a curtain wall.

Governor's Authorized Representative. The person empowered by the Governor to execute, on behalf of the State, all necessary documents for disaster assistance.

Grid Wire Sensors. Intrusion detection sensors that use a grid of wires to cover a wall or fence. An alarm is sounded if the wires are cut.



Hand Geometry. A biometric technology that is based on characteristics of the human hand.

Hazard. A source of potential danger or adverse condition.

Hazard Mitigation. Any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster event.

Hazardous Material. Any substance or material that when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

High-Hazard Areas. Geographic locations that for planning purposes have been determined through historical experience and

vulnerability analysis to be likely to experience the effects of a specific hazard (e.g., hurricane, earthquake, hazardous materials accident, etc.) resulting in vast property damage and loss of life.

High-Risk Target. Any material resource or facility that, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive or accessible terrorist target.

Human-Caused Hazard. Human caused hazards are *technological hazards* and *terrorism*. These are distinct from natural hazards primarily in that they originate from human activity. Within the military services, the term *threat* is typically used for human-caused hazard. See definitions of *technological hazards* and *terrorism* for further information.

Hurricane. A tropical cyclone, formed in the atmosphere over warm ocean areas, in which wind speeds reach 74 miles per hour or more and blow in a large spiral around a relatively calm center or ‘eye.’ Circulation is counter-clockwise in the Northern Hemisphere and clockwise in the Southern Hemisphere.



Impact Analysis. A management level analysis which identifies the impacts of losing the entity’s resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions on hazard mitigation and continuity planning.

Incident Command System. A standardized organizational structure used to command, control, and coordinate the use of resources and personnel that have responded to the scene of an emergency. The concepts and principles for ICS include common terminology, modular organization, integrated communication, unified command structure, consolidated action plan, manageable span of control, designated incident facilities, and comprehensive resource management.

Insider Compromise. A person authorized access to a facility (an insider) compromises assets by taking advantage of that accessibility.

Intercom Door/Gate Station. Part of an intercom system where communication is typically initiated, usually located at a door or gate.

Intercom Master Station. Part of an intercom system that monitors one or more intercom door/gate stations; typically, where initial communication is received.

Intercom Switcher. Part of an intercom system that controls the flow of communications between various stations.

Intercom System. An electronic system that allows simplex, half-duplex, or full-duplex audio communications.

International Terrorism. Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Intrusion Detection Sensors. Devices that initiate alarm signals by sensing the stimulus, change, or condition for which they were designed.

Intrusion Detection System. The combination of components, including sensors, control units, transmission lines, and monitor units, integrated to operate in a specified manner.

Isolated Fenced Perimeters. Fenced perimeters with 100 feet or more of space outside the fence that is clear of obstruction making approach obvious.



Jersey Barrier. A protective concrete barrier initially and still used as a highway divider and now functions as an expedient method for traffic speed control at entrance gates and to keep vehicles away from buildings.

Joint Information Center (JIC). A central point of contact for all news media near the scene of a large-scale disaster. News media representatives are kept informed of activities and events by public information officials who represent all participating federal, state, and local agencies that are collocated at the JIC.

Joint Interagency Intelligence Support Element (JIISE). An interagency intelligence component designed to fuse intelligence information from the various agencies participating in a response to a WMD threat or incident within an FBI JOC. The JIISE is an expanded version of the investigative/intelligence component which is part of the standardized FBI command post structure. The JIISE manages five functions including: security, collections management, current intelligence, exploitation, and dissemination.

Joint Information System (JIS). Under the FRP, connection of public affairs personnel, decision-makers, and news centers by electronic mail, fax, and telephone when a single federal/state/local JIC is not a viable option.

Joint Operations Center. Established by the LFA under the operational control of the Federal OSC, as the focal point for management and direction of on-site activities, coordination/establishment of state requirements/priorities, and coordination of the overall federal response.

Jurisdiction. Typically counties and cities within a state, but states may elect to define differently in order to facilitate their assessment process.



Laminated Glass. A flat lite of uniform thickness consisting of two monolithic glass plies bonded together with an interlayer material as defined in Specification C1172. Many different interlayer materials are used in laminated glass.

Landscaping. The use of plantings (shrubs and trees), with or without landforms and/or large boulders, to act as a perimeter barrier against defined threats.

Laser Card. A card technology that use a laser reflected off of a card for uniquely identifying the card.

Layers of Protection. A traditional approach in security engineering using concentric circles extending out from an area to be protected as demarcation points for different security strategies.

Lead Agency. The federal department or agency assigned lead responsibility under U.S. law to manage and coordinate the federal response in a specific functional area.

Lead Federal Agency (LFA). The agency designated by the President to lead and coordinate the overall federal response is referred to as the LFA and is determined by the type of emergency. In general, an LFA establishes operational structures and procedures to assemble and work with agencies providing direct support to the LFA in order to provide an initial assessment of the situation, develop an action plan, monitor and update operational priorities, and ensure each agency exercises its concurrent and distinct authorities under U.S. law and supports the LFA in carrying out the President's relevant policy. Specific responsibili-

ties of an LFA vary according to the agency's unique statutory authorities.

Level of Protection. The degree to which an asset is protected against injury or damage from an attack.

Liaison. An agency official sent to another agency to facilitate interagency communications and coordination.

Limited Area. A restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access to the item. See controlled area and exclusion area.

Line of Sight. Direct observation between two points with the naked eye or hand-held optics.

Line-of-Sight Sensor. A pair of devices used as an intrusion detection sensor that monitor any movement through the field between the sensors.

Line Supervision. A data integrity strategy that monitors the communications link for connectivity and tampering. In intrusion detection system sensors, line supervision is often referred to as two-state, three-state, or four-state in respect to the number of conditions monitored. The frequency of sampling the link also plays a big part in the supervision of the line.

Local Government. Any county, city, village, town, district, or political subdivision of any state, and Indian tribe or authorized tribal organization, or Alaska Native village or organization, including any rural community or unincorporated town or village or any other public entity.



Magnetic Lock. An electro-magnetic lock that unlocks a door when power is removed.

Magnetic Stripe. A card technology that use a magnetic stripe on the card to encode data used for unique identification of the card.

Mail-Bomb Delivery. Bombs or incendiary devices delivered to the target in letters or packages.

Man-Trap. An access control strategy that use a pair of interlocking doors to prevent tailgating. Only one door can be unlocked at a time.

Mass Care. The actions that are taken to protect evacuees and other disaster victims from the effects of the disaster. Activities include providing temporary shelter, food, medical care, clothing, and other essential life support needs to those people that have been displaced from their homes because of a disaster or threatened disaster.

Mass Notification. Capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations.

Microwave Motion Sensors. Intrusion detection sensors that uses microwave energy to sense movement within the sensors field of view. These sensors work similar to radar by using the Doppler effect to measure a shift in frequency.

Military Installations. Army, Navy, Air Force, and Marine Corps bases, posts, stations, and annexes (both contractor and Government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

Minimum Essential Infrastructure Resource Elements. The broad categories of resources, all or portions of which constitute the minimal essential infrastructure necessary for a department, agency or organization to conduct its core mission(s).

Minimum Measures. Protective measures that can be applied to all buildings regardless of the identified threat. These measures offer defense or detection opportunities for minimal cost, facilitate future upgrades, and may deter acts of aggression.

Mitigation. Those actions taken to reduce the exposure to and impact of an attack or disaster.

Motion Detector. Intrusion detection sensor that changes state based on movement in the sensors field of view.

Moving Vehicle Bomb. An explosive-laden car or truck driven into or near a building and detonated.

Mutual Aid Agreement. A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

N

Natural Hazard. Naturally occurring events such as floods, earthquakes, tornadoes, tsunamis, coastal storms, landslides, and wildfires that strike populated areas. A natural event is a hazard when it has the potential to harm people or property (FEMA 386-2, *Understanding Your Risks*). The risks of natural hazards may be increased or decreased as a result of human activity. However, they are not inherently human-induced.

Protective Barriers. Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.

Non-Exclusive Zone. An area around an asset that has controlled entry but shared or less restrictive access than an exclusive zone.

Non-Persistent Agent. An agent that, upon release, loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. It is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.

Nuclear, Biological or Chemical Weapons. Also called Weapons of Mass Destruction (WMD). Weapons that are characterized by their capability to produce mass casualties.

Nuclear Detonation. An explosion resulting from fission and/or fusion reactions in nuclear material, such as that from a nuclear weapon.



On-Scene Coordinator (OSC). The federal official pre-designated by the EPA and U.S. Coast Guard to coordinate and direct response and removals under the National Oil and Hazardous Substances Pollution Contingency Plan.

Open System Architecture. A term borrowed from the IT industry to claim that systems are capable of interfacing with other systems from any vendor, which also uses open system architecture. The opposite would be a proprietary system.

Operator Interface. The part of a security management system that provides that user interface to humans.

Organizational Areas of Control. Controls consist of the policies, procedures, practices and organization structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.



Passive Infrared Motion Sensors. Devices that detect a change in the thermal energy pattern caused by a moving intruder and ini-

tiate an alarm when the change in energy satisfies the detector's alarm-criteria.

Passive Vehicle Barrier. A vehicle barrier which is permanently deployed and does not require response to be effective.

Patch Panel. A concentrated termination point that separates backbone cabling from devices cabling for easy maintenance and troubleshooting.

Perimeter Barrier. A fence, wall, vehicle barrier, landform, or line of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.

Persistent Agent. An agent that, upon release, retains its casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air; therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

Physical Security. The part of security concerned with measures/concepts designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Planter Barrier. A passive vehicle barrier, usually constructed of concrete and filled with dirt (and flowers for aesthetics). Planters, along with bollards, are the usual street furniture used to keep vehicles away from existing buildings. Overall size and the depth of installation below grade determine the vehicle stopping capability of the individual planter.

Plume. Airborne material spreading from a particular source; the dispersal of particles, gases, vapors, and aerosols into the atmosphere.

Polycarbonate Glazing. A plastic glazing material with enhanced resistance to ballistics or blast effects.

Predetonation Screen. A fence which causes an anti-tank round to detonate or prevents it from arming before it reaches its target.

Preliminary Damage Assessment. A mechanism used to determine the impact and magnitude of damage and the resulting unmet needs of individuals, businesses, the public sector, and the community as a whole. Information collected is used by the State as a basis for the Governor's request for a Presidential declaration, and by FEMA to document the recommendation made to the President in response to the Governor's request. PDAs are made by at least one state and one federal representative. A local government representative familiar with the extent and location of damage in the community often participates; other state and federal agencies and voluntary relief organizations also may be asked to participate, as needed.

Preparedness. Establishing the plans, training, exercises, and resources necessary to enhance mitigation of and achieve readiness for response to, and recovery from all hazards, disasters, and emergencies including WMD incidents.

Pressure Mat. A mat that generates an alarm when pressure is applied to any part of the mat's surface, as when someone steps on the mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors and windows to detect entry.

Primary Asset. An asset which is the ultimate target for compromise by an aggressor.

Primary Gathering Building. Inhabited buildings routinely occupied by 50 or more personnel. This designation applies to the entire portion of a building that meets the population density requirements for an inhabited building.

Probability of Detection. A measure of an intrusion detection sensor's performance in detecting an intruder within its detection zone.

Probability of Intercept. The probability that an act of aggression will be detected and that a response force will intercept the aggressor before the asset can be compromised.

Progressive Collapse. A chain reaction failure of building members to an extent disproportionate to the original localized damage. Such damage may result in upper floors of a building collapsing onto lower floors.

Protective Barriers. Define the physical limits of a site, activity, or area by restricting, channeling, or impeding access and forming a continuous obstacle around the object.

Protective Measures. Elements of a protective system which protect an asset against a threat. Protective measures are divided into defensive and detection measures.

Protective System. An integration of all of the protective measures required to protect an asset against the range of threats applicable to the asset.

Proximity Sensors. Intrusion detection sensors that change state based on the close distance or contact of a human to the sensor. These sensors often measure the change in capacitance as a human body enters the measured field.

Public Information Officer. A federal, state, or local government official responsible for preparing and coordinating the dissemination of emergency public information.

R

Radiation. High-energy particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay. Par-

icles can be either charged alpha or beta particles or neutral neutron or gamma rays.

Radiation Sickness. The symptoms characterizing the sickness known as radiation injury, resulting from excessive exposure of the whole body to ionizing radiation.

Radiological Monitoring. The process of locating and measuring radiation by means of survey instruments that can detect and measure (as exposure rates) ionizing radiation.

Recovery. The long-term activities beyond the initial crisis period and emergency response phase of disaster operations that focus on returning all systems in the community to a normal status or to reconstitute these systems to a new condition that is less vulnerable.

Regional Operating Center (ROC). The temporary operations facility for the coordination of federal response and recovery activities located at the FEMA Regional Office (or Federal Regional Center) and led by the FEMA Regional Director or Deputy Director until the DFO becomes operational. Once the ERT-A is deployed, the ROC performs a support role for federal staff at the disaster scene.

Report Printers. A separate, dedicated printer attached to the electronic security systems used for generating reports using information stored by the central computer.

Request-To-Exit Device. Passive infrared motion sensors or push buttons that are used to signal an electronic entry system that egress is imminent or to unlock a door.

Resolution. The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution.

Resource Management. Those actions taken by a government to: identify sources and obtain resources needed to support disaster response activities; coordinate the supply, allocation, distribution, and delivery of resources so that they arrive where and when most needed; and maintain accountability for the resources used.

Response. Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population.

Response Force. The people who respond to an act of aggression. Depending on the nature of the threat, the response force could consist of guards, special reaction teams, military or civilian police, an explosives ordnance disposal team, or a fire department.

Response Time. The length of time from the instant an attack is detected to the instant a security force arrives onsite.

Restricted Area. Any area with access controls that is subject to these special restrictions or controls for security reasons. See also controlled area, limited area, exclusion area, and exclusion zone.

Retinal Pattern. A biometric technology that is based on features of the human eye.

RF Data Transmission. A communication link using radio frequency to send or receive data.

Risk. The potential for loss of, or damage to, an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.

Rotating Drum or Rotating Plate Vehicle Barrier. An active vehicle barrier used at vehicle entrances to controlled areas based on a drum or plate rotating into the path of the vehicle when signaled.

Routinely Occupied. For the purposes of these standards, an established or predictable pattern of activity within a building that terrorists could recognize and exploit.

RS-232 Data. IEEE Recommended Standard 232; a point-to-point serial data protocol with a maximum effective distance of 50 feet.

RS-422 Data. IEEE Recommended Standard 422; a point-to-point serial data protocol with a maximum effective distance of 4000 feet.

RS-485 Data. IEEE Recommended Standard 485; a multi-drop serial data protocol with a maximum effective distance of 4000 feet.



Sacrificial Roof or Wall. Walls or roofs that can be lost in a blast without damage to the primary asset.

Safe Haven. Secure areas within the interior of the facility. A safe haven should be designed such that it requires more time to penetrate by aggressors than it takes for the response force to reach the protected area to rescue the occupants. It may be a haven from a physical attack or air-isolated haven from CBR contamination.

Scramble Keypad. A keypad that uses keys on which the numbers change pattern with each use to enhance security by preventing eavesdropping observation of the entered numbers.

Secondary Asset. An asset which supports a primary asset and whose compromise would indirectly affect the operation of the primary asset.

Secondary Hazard. A threat whose potential would be realized as the result of a triggering event that of itself would constitute an emergency. For example, dam failure might be a secondary hazard associated with earthquakes.

Secure/Access Mode. The state of an area monitored by an intrusion detection system in regards to how alarm conditions are reported.

Security Analysis. The method of studying the nature of and the relationship between assets, threats, and vulnerabilities.

Security Console. Specialized furniture, racking, and related apparatus used to house the security equipment required in a control center.

Security Engineering. The process of identifying practical, risk managed short and long-term solutions to reduce and/or mitigate dynamic man-made hazards by integrating multiple factors, including construction, equipment, manpower, and procedures.

Security Engineering Design Process. The process through which assets requiring protection are identified, the threat to and vulnerability of those assets is determined, and a protective system is designed to protect the assets.

Security Management System Database. In a Security Management System, a database that is transferred to various nodes or panels throughout the system for faster data processing and protection against communication link downtime.

Security Management System Distributed Processing. In a Security Management System, a method of data processing at various nodes or panels throughout the system for faster data processing and protection against communication link downtime.

Segregation of Duties. Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to minimum essential infrastructure resource elements.

Semi-Isolated Fenced Perimeters. Fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence where there is little reason for the general public or other personnel seldom have reason to be in the area.

Senior FEMA Official (SFO). The official appointed by the Director of FEMA, or his representative, that is responsible for deploying to the JOC to: (1) serve as the senior interagency consequence management representative on the Command Group; and (2) manage and coordinate activities taken by the Consequence Management Group.

Serial Interface. An integration strategy for data transfer where components are connected in series.

Shielded Wire. Wire with a conductive wrap used to mitigate electromagnetic emanations.

Situational Crime Prevention. A crime prevention strategy based on reducing the opportunities for crime by increasing the effort required to commit a crime, increasing the risks associated with committing the crime, and reducing the target appeal or vulnerability (whether property or person). This opportunity reduction is achieved by management and use policies such as procedures and training, as well as physical approaches such as alteration of the built environment.

Smart Card. A newer card technology that allows data to be written, stored, and read on a card typically used for identification and/or access.

Software Level Integration. An integration strategy that use software to interface systems. An example of this would be digital video displayed in the same computer application window and linked to events of a security management system.

Specific Threat. Known or postulated aggressor activity focused on targeting a particular asset.

Standoff Distance. A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.

Standoff Weapons. Weapons such as anti-tank weapons and mortars that are launched from a distance at a target.

State Coordinating Officer. The person appointed by the Governor to coordinate State, Commonwealth, or Territorial response and recovery activities with FRP-related activities of the Federal Government, in cooperation with the FCO.

State Liaison. A FEMA official assigned to a particular state, who handles initial coordination with the State in the early stages of an emergency.

Stationary Vehicle Bomb. An explosive-laden car or truck stopped or parked near a building.

Storm Surge. A dome of sea water created by the strong winds and low barometric pressure in a hurricane that causes severe coastal flooding as the hurricane strikes land.

Strain-Sensitive Cable. Strain-sensitive cables are transducers that are uniformly sensitive along their entire length and generate an analog voltage when subject to mechanical distortions or stress resulting from fence motion. They are typically attached to a chain-link fence about halfway between the bottom and top of the fence fabric with plastic ties.

Structural Protective Barriers. Man-made devices (such as fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.

Superstructure. The supporting elements of a building above the foundation.

Supplies-Bomb Delivery. Bombs or incendiary devices concealed and delivered to supply or material handling points such as loading docks.

System Events. Events that occur normally in the operation of a security management system. Examples include access control operations and changes of state in intrusion detection sensors.

System Software. Controls that limit and monitor access to the powerful programs and sensitive files that: (1) control the computer hardware; and (2) secure applications supported by the system.



Tactics. The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal materiel or information.

Tamper Switch. Intrusion detection sensor that monitors an equipment enclosure for breach.

Tangle-Foot Wire. Barbed wire or tape suspended on short metal or wooden pickets outside a perimeter fence to create an obstacle to approach.

Taut-Wire Sensor. An intrusion detection sensor utilizing a column of uniformly spaced horizontal wires, securely anchored at each end and stretched taut. Each wire is attached to a sensor to indicate movement of the wire.

Technical Assistance. The provisioning of direct assistance to states and local jurisdictions to improve capabilities for program development, planning, and operational performances related to responses to WMD terrorist incidents.

Technological Hazard. Incidents that can arise from human activities such as manufacture, transportation, storage, and use of hazardous materials. For the sake of simplicity, it is assumed that technological emergencies are accidental and that their consequences are unintended.

TEMPEST. An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term ‘compromising emanations;’ e.g., TEMPEST tests, TEMPEST inspections.

Terrorism. The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Thermally Tempered Glass. Glass which is heat-treated to have a higher tensile strength and resistance to blast pressures, although a greater susceptibility to airborne debris.

Threat. Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.

Threat Analysis. A continual process of compiling and examining all available information concerning potential threats and hu-

man-caused hazards. A common method to evaluate terrorist groups is to review the factors of existence, capability, intentions, history, and targeting.

Time/Date Stamp. Data inserted into a CCTV video signal with the time and date of the video as it was created.

TNT Equivalent Weight. The weight of TNT (trinitrotoluene) that has an equivalent energetic output to that of a different weight of another explosive compound.

Tornado. A local atmospheric storm, generally of short duration, formed by winds rotating at very high speeds, usually in a counter-clockwise direction. The vortex, up to several hundred yards wide, is visible to the observer as a whirlpool-like column of winds rotating about a hollow cavity or funnel. Winds may reach 300 miles per hour or higher.

Toxicity. A measure of the harmful effects produced by a given amount of a toxin on a living organism.

Toxic-Free Area. An area within a facility in which the air supply is free of toxic chemical or biological agents.

Triple-Standard Concertina (TSC) Wire. This type of fence uses three rolls of stacked concertina. One roll will be stacked on top of two rolls that run parallel to each other while resting on the ground, forming a pyramid.

Tsunami. Sea waves produced by an undersea earthquake. Such sea waves can reach a height of 80 feet and can devastate coastal cities and low-lying coastal areas.

Twisted Pair Wire. Wire that uses pairs of wires twisted together to mitigate electromagnetic interference.

Two-Person Rule. A security strategy that requires two people to be present in or gain access to a secured area to prevent unobserved access by any individual.

U

Unobstructed Space. Space around an inhabited building without obstruction large enough to conceal explosive devices 150 mm (6 inches) or greater in height.

Unshielded Wire. Wire that does not have a conductive wrap.

V

Vault. A reinforced room for securing items.

Vertical Rod. Typical door hardware often used with a crash bar to lock a door by inserting rods vertically from the door into the doorframe.

Vibration Sensors. Intrusion detection sensor that change state when vibration is present.

Video Intercom System. An intercom system that also incorporates a small CCTV system for verification.

Video Motion Detection. Motion detection technology that looks for changes in the pixels of a video image.

Video Multiplexer. A device used to connect multiple video signals to a single location for viewing and/or recording.

Visual Displays. A display or monitor used to inform the operator visually of the status of the electronic security system.

Visual Surveillance. The aggressor uses ocular and photographic devices (such as binoculars and cameras with telephoto lenses) to monitor facility or installation operations or to see assets.

Voice Recognition. A biometric technology that is based on nuances of the human voice.

Volumetric Motion Sensors. Interior intrusion detection sensors which are designed to sense aggressor motion within a protected space.

Vulnerability. Any weakness in an asset or mitigation measure than can be exploited by an aggressor (potential threat element), adversary or competitor. It refers to the organization's susceptibility to injury.

W

Warning. The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause.

Watch. Indication in a defined area, that conditions are favorable for the specified type of severe weather (e.g., flash flood watch, severe thunderstorm watch, tornado watch, tropical storm watch).

Waterborne Contamination. Chemical, biological, or radiological introduced into and fouling a water supply.

Weapons-Grade Material. Nuclear material considered most suitable for a nuclear weapon. It usually connotes uranium enriched to above 90% uranium-235 or plutonium with greater than about 90% plutonium-239.

Weapons of Mass Destruction. Any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or a missile having an explosive incendiary charge of more than 0.25 ounce, or mine or device similar to the above; poison gas; weapon involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life. Any device, material, or substance used in a manner, in a quantity or type, or under circumstances

evidencing an intent to cause death or serious injury to persons, or significant damage to property.

Weigand Protocol. A security industry standard data protocol for card readers.

Z

Zoom. The ability of a CCTV camera to close and focus or open and widen the field of view.

GLOSSARY OF CHEMICAL TERMS

A

Acetylcholinesterase. An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.

Aerosol. Fine liquid or solid particles suspended in a gas; for example, fog or smoke.

Atropine. A compound used as an antidote for nerve agents.

C

Casualty (toxic) agents. Produce incapacitation, serious injury, or death. They can be used to incapacitate or kill victims. These agents are the choking, blister, nerve, and blood agents.

Blister Agents. Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs). Examples are distilled mustard (**HD**), nitrogen mustard (**HN**), lewisite (**L**), mustard/lewisite (**HL**), and phenodichloroarsine (**PD**).

Blood Agents. Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Examples are arsine (**SA**), cyanogens chloride (**CK**), hydrogen chloride, and hydrogen cyanide (**AC**).

Choking/Lung/Pulmonary Agents. Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is “choked.” Examples are chlorine (**CL**), diphosgene (**DP**), cyanide, nitrogen oxide (**NO**), perfluroisobutylene (**PHIB**), phosgene (**CG**), red phosphorous (**RP**), sulfur trioxide-chlorosulfonic acid (**FS**), Teflon and perfluroisobutylene (**PHIB**), titanium tetrachloride (**FM**) and zinc oxide (**HC**).

Nerve Agents. Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are: pin-point pupils, an extreme headache, and severe tightness in the chest. Also see G-series and V-series nerve agents.

Chemical agent. A chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects. Excluded from consideration are riot control agents, and smoke and flame materials. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.

Cutaneous. Pertaining to the skin.

D

Decontamination. The process of making any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

G

G-series nerve agents. Chemical agents of moderate to high toxicity developed in the 1930s. Examples are tabun (**GA**), sarin (**GB**), soman (**GD**), phosphonofluoridic acid, ethyl-, 1-methylethyl ester (**GE**) and cyclohexyl sarin (**GF**).

I

Incapacitating agents. Produce temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment. However, such treatment speeds recovery.

Vomiting agents. Produce nausea and vomiting effects, can also cause coughing, sneezing, pain in the nose and throat, nasal discharge, and tears. Examples are adamsite

(**DM**), diphenylchloroarsine (**DA**), and diphenylcyanoarsine (**DC**).

Tear (riot control) agents. Produce irritating or disabling effects that rapidly disappear within minutes after exposure ceases. Examples are bromobenzylcyanide (**CA**), chloroacetophenone (**CN** or commercially as Mace), chloropicrin (**PS**), **CNB** (CN in benzene and carbon tetrachloride), **CNC** (CN in chloroform), **CNS** (CN and chloropicrin in chloroform), **CR** (dibenz-(b,f)-1,4-oxazepine, a tear gas), **CS** (tear gas), and **Capsaicin** (pepper spray).

Central nervous system depressants. Compounds that have the predominant effect of depressing or blocking the activity of the central nervous system. The primary mental effects include the disruption of the ability to think, sedation, and lack of motivation.

Central nervous system stimulants. Compounds that have the predominant effect of flooding the brain with too much information. The primary mental effect is loss of concentration, causing indecisiveness and the inability to act in a sustained, purposeful manner.

Examples of the depressants and stimulants include agent 15 (suspected Iraqi BZ), **BZ** (3-quinulidinyle benzilate), canniboids, fentanyls, **LSD** (lysergic acid diethylamide), and phenothiazines.

Industrial agents. Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. Hydrogen cyanide, cyanogen chloride, phosgene, chloropicrin and many herbicides and pesticides are industrial chemicals that also can be chemical agents.

L

Liquid agent. A chemical agent that appears to be an oily film or droplets. The color ranges from clear to brownish amber.

N

Nonpersistent agent. An agent that upon release loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate and is lighter than air and will disperse rapidly. It is considered to be a short-term hazard. However, in small unventilated areas, the agent will be more persistent.

O

Organophosphorous compound. A compound, containing the elements phosphorus and carbon, whose physiological effects include inhibition of acetylcholinesterase. Many pesticides (malathione and parathion) and virtually all nerve agents are organophosphorous compounds.

P

Percutaneous agent. Able to be absorbed by the body through the skin.

Persistent agent. An agent that upon release retains its casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air. Therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

Protection. Any means by which an individual protects his body. Measures include masks, self-contained breathing apparatuses, clothing, structures such as buildings, and vehicles.

V









V-series nerve agents. Chemical agents of moderate to high toxicity developed in the 1950s. They are generally persistent.

Examples are **VE** (phosphonothioic acid, ethyl-, S-[2-(diethylamino)ethyl] O-ethyl ester), **VG** (phosphorothioic acid, S-[2-(diethylamino)ethyl] O,O-diethyl ester), **VM** (phosphonothioic acid, methyl-, S-[2-(diethylamino)ethyl] O-ethyl ester), **VS** (phosphonothioic acid, ethyl-, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl ester), and **VX** (phosphonothioic acid, methyl-, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl ester).

Vapor agent. A gaseous form of a chemical agent. If heavier than air, the cloud will be close to the ground. If lighter than air, the cloud will rise and disperse more quickly.

Volatility. A measure of how readily a substance will vaporize.

Placards Associated With Chemical Incidents

Gases – Toxic and/or Corrosive		Substances – Toxic (Combustible)
	Substances – Toxic (Non-Combustible)	
		
		

GLOSSARY OF BIOLOGICAL TERMS

A

Aerosol. Fine liquid or solid particles suspended in a gas; for example, fog or smoke.

Antibiotic. A substance that inhibits the growth of or kills microorganisms.

Antisera. The liquid part of blood containing antibodies, that react against disease causing agents such as those used in biological warfare.

B

Bacteria. Single-celled organisms that multiply by cell division and that can cause disease in humans, plants, or animals.

Biochemicals. The chemicals that make up or are produced by living things.

Biological warfare agents. Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants, or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

Biological warfare. The intentional use of biological agents as weapons to kill or injure humans, animals, or plants, or to damage equipment.

Bioregulators. Biochemicals that regulate bodily functions. Bioregulators that are produced by the body are termed “endogenous.” Some of these same bioregulators can be chemically synthesized.

C

Causative agent. The organism or toxin that is responsible for causing a specific disease or harmful effect.

Contagious. Capable of being transmitted from one person to another.

Culture. A population of micro-organisms grown in a medium.

D

Decontamination. The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

F

Fungi. Any of a group of plants mainly characterized by the absence of chlorophyll, the green colored compound found in other plants. Fungi range from microscopic single-celled plants (such as molds and mildews) to large plants (such as mushrooms).

H

Host. An animal or plant that harbors or nourishes another organism.

I

Incapacitating agent. Agents that produce physical or psychological effects, or both, that may persist for hours or days after exposure, rendering victims incapable of performing normal physical and mental tasks.

Infectious agents. Biological agents capable of causing disease in a susceptible host.

Infectivity. (1) The ability of an organism to spread. (2) The number of organisms required to cause an infection to secondary hosts. (3) The capability of an organism to spread out from the site of infection and cause disease in the host organism. Infectivity also can be viewed as the number of organisms required to cause an infection.

L

Line-source delivery system. A delivery system in which the biological agent is dispersed from a moving ground or air vehicle in a line perpendicular to the direction of the prevailing wind. (See also “point-source delivery system.”)

M

Mycotoxin. A toxin produced by fungi.

Microorganism. Any organism, such as bacteria, viruses, and some fungi, that can be seen only with a microscope.

N

Nebulizer. A device for producing a fine spray or aerosol.

O

Organism. Any individual living thing, whether animal or plant.

P

Parasite. Any organism that lives in or on another organism without providing benefit in return.

Pathogen. Any organism (usually living) capable of producing serious disease or death, such as bacteria, fungi, and viruses.

Pathogenic agents. Biological agents capable of causing serious disease.

Point-source delivery system. A delivery system in which the biological agent is dispersed from a stationary position. This delivery method results in coverage over a smaller area than with the line-source system. (See also “line-source delivery system.”)

R

Route of exposure (entry). The path by which a person comes into contact with an agent or organism; for example, through breathing, digestion, or skin contact.

Single-cell protein. Protein-rich material obtained from cultured algae, fungi, protein and bacteria, and often used as food or animal feed.

Placard Associated with Biological Incidents



GLOSSARY OF RADIOLOGICAL TERMS

A

Acute radiation Syndrome. Consists of three levels of effects: hematopoietic (blood cells, most sensitive); gastrointestinal (GI cells, very sensitive); and central nervous system (brain/muscle cells, insensitive). The initial signs and symptoms are nausea, vomiting, fatigue, and loss of appetite. Below about 200 rems, these symptoms may be the only indication of radiation exposure.

Alpha particle (•). The alpha particle has a very short range in air and a very low ability to penetrate other materials, but it has a strong ability to ionize materials. Alpha particles are unable to penetrate even the thin layer of dead cells of human skin and consequently are not an external radiation hazard. Alpha-emit-

ting nuclides inside the body as a result of inhalation or ingestion are a considerable internal radiation hazard.

B

Beta particles (β). High-energy electrons emitted from the nucleus of an atom during radioactive decay. They normally can be stopped by the skin or a very thin sheet of metal.

C

Cesium-137 (Cs-137). A strong gamma ray source and can contaminate property, entailing extensive clean-up. It is commonly used in industrial measurement gauges and for irradiation of material. Half-life is 30.2 years.

Cobalt-60 (Co-60). A strong gamma ray source, and is extensively used as a radiotherapeutic for treating cancer, food and material irradiation, gamma radiography, and industrial measurement gauges. Half-life is 5.27 years.

Curie (Ci). A unit of radioactive decay rate defined as 3.7×10^{10} disintegrations per second.

D

Decay. The process by which an unstable element is changed to another isotope or another element by the spontaneous emission of radiation from its nucleus. This process can be measured by using radiation detectors such as Geiger counters.

Decontamination. The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

Dose. A general term for the amount of radiation absorbed over a period of time.

Dosimeter. A portable instrument for measuring and registering the total accumulated dose to ionizing radiation.

G

Gamma rays (•). High-energy photons emitted from the nucleus of atoms; similar to x rays. They can penetrate deeply into body tissue and many materials. Cobalt-60 and Cesium-137 are both strong gamma-emitters. Shielding against gamma radiation requires thick layers of dense materials, such as lead. Gamma rays are potentially lethal to humans.

H

Half-life. The amount of time needed for half of the atoms of a radioactive material to decay.

Highly enriched uranium (HEU). Uranium that is enriched to above 20% Uranium-235 (U-235). Weapons-grade HEU is enriched to above 90% in U-235.

I

Ionize. To split off one or more electrons from an atom, thus leaving it with a positive electric charge. The electrons usually attach to one of the atoms or molecules, giving them a negative charge.

Iridium-192. A gamma-ray emitting radioisotope used for gamma- radiography. The half-life is 73.83 days.

Isotope. A specific element always has the same number of protons in the nucleus. That same element may, however, appear in forms that have different numbers of neutrons in the nucleus. These different forms are referred to as “isotopes” of the element. For example, deuterium (2H) and tritium (3H) are isotopes of ordinary hydrogen (H).

L

Lethal dose (50/30). The dose of radiation expected to cause death within 30 days to 50% of those exposed without medical treatment. The generally accepted range from 400-500 rem received over a short period of time.

N

Nuclear reactor. A device in which a controlled, self-sustaining nuclear chain reaction can be maintained with the use of cooling to remove generated heat.

P

Plutonium-239 (Pu-239). A metallic element used for nuclear weapons. The half-life is 24,110 years.

R

Rad. A unit of absorbed dose of radiation defined as deposition of 100 ergs of energy per gram of tissue. A rad amounts to approximately one ionization per cubic micron.

Radiation. High energy alpha or beta particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay.

Radiation sickness. Symptoms resulting from excessive exposure to radiation of the body.

Radioactive waste. Disposable, radioactive materials resulting from nuclear operations. Wastes are generally classified into two categories, high-level and low-level waste.

Radiological Dispersal Device (RDD). A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.

Radioluminescence. The luminescence produced by particles emitted during radioactive decay.

REM or rem. A Roentgen Man Equivalent is a unit of absorbed dose that takes into account the relative effectiveness of radiation that harms human health.

S

Spore. A reproductive form some micro-organisms can take to become resistant to environmental conditions, such as extreme heat or cold, while in a “resting stage.”

T

Toxicity. A measure of the harmful effect produced by a given amount of a toxin on a living organism. The relative toxicity of an agent can be expressed in milligrams of toxin needed per kilogram of body weight to kill experimental animals.

Toxins. Poisonous substances produced by living organisms.

V

Vaccine. A preparation of killed or weakened microorganism products used to artificially induce immunity against a disease.

Vector. An agent, such as an insect or rat, capable of transferring a pathogen from one organism to another.

Venom. A poison produced in the glands of some animals; for example, snakes, scorpions, or bees.

Virus. An infectious micro-organism that exists as a particle rather than as a complete cell. Particle sizes range from 20 to 400 nanometers (one-billionth of a meter). Viruses are not capable of reproducing outside of a host cell.

Placards Associated with Radiological Incidents



A

AA&E Arms, Ammunition, and Explosives

AAR After Action Report

ACL Access Control Lists

ACP access control point

AECS Automated Entry Control System

AFMAN Air Force Manual

AFJMAN Air Force Joint Manual, also may be known as AFMAN (I) for Air Force Manual

ALERT Automated Local Evaluation in Real Time

AMS Aerial Measuring System

ANS alert and notification system

ANSI American National Standards Institute

ANSIR Awareness of National Security Issues and Response Program

AOR Area of Responsibility

AP Armor Piercing

APHL Agency for Public Health Laboratories

ARAC Atmospheric Release Advisory Capability

ARC American Red Cross

ARG Accident Response Group

ARS Agriculture/Research Service

ASTHO Association for State and Territorial Health Officials

AT Antiterrorism

ATC Air Traffic Control

ATSD(CS) Assistant to the Secretary of Defense for Civil Support

ATSDR Agency for Toxic Substances and Disease Registry

B

BCA Benefit-Cost Analysis

BCP Business Continuity Plan

BDC Bomb Data Center

C

CAMEO Computer-Aided Management of Emergency Operations

CB Citizens Band

CBIAC Chemical and Biological Defense Information and Analysis Center

CBR Chemical, Biological, or Radiological

CBRNE Chemical, Biological, Radiological, Nuclear Material, or High-Yield Explosive

CCTV Closed-Circuit Television

CDC Centers for Disease Control and Prevention

CDR Call Detail Report

CDRG Catastrophic Disaster Response Group

CEO Chief Executive Officer

CEPPO Chemical Emergency Preparedness and Prevention Office

CERCLA Comprehensive Environmental Response, Compensation, and Liability Act

CERT Community Emergency Response Team

CFO Chief Financial Officer

CFR Code of Federal Regulations

CHEMTREC Chemical Manufacturers' Association Chemical Transportation Emergency Center

CHPPM Center for Health Promotion and Preventive Medicine

CIAO Chief Infrastructure Assurance Officer, also, Critical Infrastructure Assurance Officer

CICG Critical Infrastructure Coordination Group

CIO Chief Information Officer

CIP Critical Infrastructure Protection

CIRG Crisis Incident Response Group

CJCS Chairman of the Joint Chiefs of Staff

CM Consequence Management

CMS Call Management System

CMU Crisis Management Unit (CIRG)

CO/DO Central Office/Direct Outdial

COB Continuity of Business

COBIT™ Control Objectives for Information Technology

CONEX Container Express

CONOPS Concept of Operations

COO Chief Operations Officer

COOP Continuity of Operations

COR Class of Restriction

COS Class of Service

CPG Civil Preparedness Guide

CPTED Crime Prevention Through Environmental Design

CPX Command Post Exercise

CRU Crisis Response Unit
CSEPP Chemical Stockpile Emergency Preparedness Program
CSREES Cooperative State Research, Education and Extension Service
CST Civil Support Teams
CSTE Council of State and Territorial Epidemiologists
CT Counterterrorism
CW/CBD Chemical Warfare/Contraband Detection

D

DBMS Database Management System
DBT Design Basis Threat
DBU Dial Backup
DD Data Dictionary
DES Data Encryption Standard
DEST Domestic Emergency Support Team
DFO Disaster Field Office
DISA Direct Inward System Access
DMA Disaster Mitigation Act of 2000
DMAT Disaster Medical Assistance Team
DMCR Disaster Management Central Resource
DMORT Disaster Mortuary Operational Response Team
DoD Department of Defense
DOE Department of Energy
DOJ Department of Justice
DOS Department of State

DOT U.S. Department of Transportation
DPP Domestic Preparedness Program
DRC Disaster Recovery Center
DTCTPS Domestic Terrorism/Counter Terrorism Planning
Section (FBI HQ)
DTIC Defense Technical Information Center
DWI Disaster Welfare Information

E

EAS Emergency Alert System
ECL Emergency Classification Level
EECS Electronic Entry Control System
EFR Emergency First Responder
EM Emergency Management
EMAC Emergency Medical Assistance Compact
EMI Emergency Management Institute
EMP Electromagnetic Pulse
EMS Emergency Medical Services
EOC Emergency Operating Center
EOD Explosive Ordnance Disposal
EOP Emergency Operating Plan or Emergency Operations Plan
EPA Environmental Protection Agency
EPCRA Emergency Planning and Community Right-to-Know Act
EPG Emergency Planning Guide
EPI Emergency Public Information
EPZ Emergency Planning Zone

ERT Emergency Response Team
ERT-A Emergency Response Team Advance Element
ERT-N Emergency Response Team National
ERTU Evidence Response Team Unit
ESC Expandable Shelter Container
ESF Emergency Support Function
ESS Electronic Security System
EST Emergency Support Team
EU Explosives Unit

F

FAsT Field Assessment Team
FBI Federal Bureau of Investigation
FCO Federal Coordinating Officer
FEMA Federal Emergency Management Agency
FEST Foreign Emergency Support Team
FHBM Flood Hazard Boundary Map
FIA Federal Insurance Administration
FIPS Federal Information Processing Standard
FIRM Flood Insurance Rate Map
FIS Flood Insurance Study
FISCAM Federal Information Systems Control Audit Manual
FMFIA Federal Manager's Financial Integrity Act
FNS Food and Nutrition Service
FOIA Freedom of Information Act

FOUO For Official Use Only

FPEIS Final Programmatic Environmental Impact Statement

FRERP Federal Radiological Emergency Response Plan

FRF Fragment-retention film

FRMAC Federal Radiological Monitoring and Assessment Center

FRP Federal Response Plan

FRL Facility Restriction Level

FS Forest Service

FSTFS Frame-Supported Tensioned Fabric Structure

FTP File Transfer Protocol

FTX Functional Training Exercise



GAO General Accounting Office

GAR Governor's Authorized Representative

GP General Purpose

GIS Geographic Information System

GSA General Services Administration



HAZMAT Hazardous materials

HAZUS Hazards US

HEPA High Efficiency Particulate Air

HHS Department of Health and Human Services

HIRA Hazard Identification and Risk Assessment

HMRU Hazardous Materials Response Unit

HQ Headquarters

HRCQ Highway Route Controlled Quantity

HRT Hostage Rescue Team (CIRG)

HTIS Hazardous Technical Information Services (DoD)

HVAC Heating, Ventilation, and Air Conditioning



IC Incident Commander

ICDDC Interstate Civil Defense and Disaster Compact

ICP Incident Command Post

ICS Incident Command System

IDS Intrusion Detection System

IED Improvised Explosive Device

IEMS Integrated Emergency Management System

IID Improvised Incendiary Device

IND Improvised Nuclear Device

IPL Initial Program Load

IRZ Immediate Response Zone

IS Information System

ISACF Information Systems Audit and Control Foundation

ISO International Organization for Standardization

ISP Internet Service Provider

IT Information Technology



JIC Joint Information Center

JIS Joint Information System

JNACC Joint Nuclear Accident Coordinating Center

JOC Joint Operations Center

JTF-CS Joint Task Force for Civil Support

JTTF Joint Terrorism Task Force

JTWG Joint Terrorism Working Group

L

LAN Local Area Network

LAW Light Antitank Weapon

LCM Life Cycle Management

LEPC Local Emergency Planning Committee

LFA Lead Federal Agency

LLNL Lawrence Livermore National Laboratory

LOP Level of Protection

LOS Line of Sight

LPHA Local Public Health Agency

LPHS Local Public Health System

M

MAC Moves Adds Changes

MEDCOM Medical Command

MEI Minimum Essential Infrastructure

MEP Mission Essential Process

MMRS Metropolitan Medical Response System

MOU/A Memorandum of Understanding/Agreement

mph miles per hour

MSCA Military Support to Civil Authorities

MSDS material safety data sheet

MSS Medium Shelter System

N

NACCHO National Association for County and City Health Officials

NAP Nuclear Assessment Program

NBC Nuclear, Biological, and Chemical

NCP National Oil and Hazardous Substances Pollution Contingency Plan

NDA National Defense Area

NDMS National Disaster Medical System

NDPO National Domestic Preparedness Office

NEST Nuclear Emergency Search Team

NETC National Emergency Training Center

NFA National Fire Academy

NFIP National Flood Insurance Program

NIOSH National Institute for Occupational Safety and Health

NMRT National Medical Response Team

NMS Network Management Systems

NOAA National Oceanic and Atmospheric Administration

NRC Nuclear Regulatory Commission; National Response Center

NRT National Response Team

NSC National Security Council

NTIS National Technical Information Service

NUREG Nuclear Regulation

NWS National Weather Service



ODP Office of Disaster Preparedness

OEP Office of Emergency Preparedness

OES Office of Emergency Services

OFCM Office of the Federal Coordinator for Meteorology

OHS Office of Homeland Security

OJP Office of Justice Programs

OMB Office of Management and Budget

OPA Oil Pollution Act

OSC On-Scene Coordinator

OSD Office of Secretary of Defense

OSHA Occupational Safety and Health Administration

OSLDPS Office for State and Local Domestic Preparedness
Support



PA public address

PAZ Protective Action Zone

PBX Public Branch Exchange

PCC Policy Coordinating Committee

PCCIP President's Commission on Critical Infrastructure
Protection

PCM Procedures Control Manual

PDA Preliminary Damage Assessment
PDD Presidential Decision Directive
PHS Public Health Service
PIN Personal Identification Number
PIO Public Information Officer
PL Public Law
POC Point of Contact
POL Petroleum, Oils, and Lubricants
PPA Performance Partnership Agreement
PT Preparedness, Training, and Exercises Directorate (FEMA)
PTE Potential Threat Element
PZ Precautionary Zone

R

RACES Radio Amateur Civil Emergency Service
RAP Radiological Assistance Program
RCRA Research Conservation and Recovery Act
RDD Radiological Dispersal Device
RDT&E Research, Development, Test and Evaluation
REACT Radio Emergency Associated Communications Teams
REAC/TS Radiation Emergency Assistance Center/Training Site
REP Radiological Emergency Preparedness Program
ROC Regional Operating Center
ROD Record of Decision
RPG Rocket Propelled Grenade
RRIS Rapid Response Information System (FEMA)

RRP Regional Response Plan

RRT Regional Response Team

S

SAA State Administrative Agency

SAC Special Agent in Charge (FBI)

SAME Specific Area Message Encoder

SARA Superfund Amendments and Reauthorization Act

SBCCOM Soldier and Biological Chemical Command (U.S. Army)

SCADA Supervisory, Control, and Data Acquisition

SCBA Self-Contained Breathing Apparatus

SCO State Coordinating Officer

SEA Southeast Asia

SEB State Emergency Board

SEL Standardized Equipment List

SEMA State Emergency Management Agency

SERC State Emergency Response Commission

SIOC Strategic Information and Operations Center (FBI HQ)

SLA Service Level Agreement

SLG State and Local Guide

SOP standard operating procedure

SPCA Society for the Prevention of Cruelty to Animals

SPSA Super Power Small Arms

SSS Small Shelter System

STC Sound Transmission Class

SWAT Special Weapons and Tactics

T

TAC Trunk Access Codes

TEA Threat Environment Assessment

TEMPER Tent, Extendable, Modular, Personnel

TERC Tribal Emergency Response Commission

TIA Terrorist Incident Appendix

TM Technical Manual

TNT Trinitrotoluene

TRIS Toxic Release Inventory System

TSO Time Share Option

U

UC Unified Command

UCS Unified Command System

UL Underwriters Laboratories

UPS Uninterrupted Power Supply

USC U.S. Code

USDA U.S. Department of Agriculture

USFA U.S. Fire Administration

USGS U.S. Geological Survey

US&R Urban Search and Rescue

V

VA Department of Veterans Affairs

VAV Variable Air Volume

VAP Vulnerability Assessment Plan

VDN Vector Directory Number

VRU Voice Response Unit



WAN Wide Area Network

WMD Weapons of Mass Destruction

WMD-CST WMD Civil Support Team

American Lifelines Alliance

<http://www.americanlifelinesalliance.org>

Applied Technology Council <http://www.atcouncil.org>

Battelle Memorial Institute, National Security Program

<http://www.battelle.org/natsecurity/default.stm>

Center for Strategic and International Studies (CSIS)

<http://www.csis.org>

Centers for Disease Control and Prevention (CDC) / National
Institute for Occupational Safety and Health (NIOSH)

<http://www.cdc.gov/niosh>

Central Intelligence Agency (CIA) <http://www.cia.gov>

Council on Tall Buildings and Urban Habitat (CTBUH)

<http://www.ctbuh.org>

Federal Aviation Administration (FAA) <http://www.faa.gov>

Healthy Buildings International, Inc.

<http://www.healthybuildings.com>

Institute of Transportation Engineers <http://www.ite.org>

Interagency Security Committee (ISC) led by U.S. General
Services Administration

International CPTED [Crime Prevention Through
Environmental Design] Association (ICA)

<http://new.cpted.net/home.amt>

Lawrence Berkeley National Laboratory (LBNL)

<http://securebuildings.lbl.gov>

National Academy of Sciences

<http://www4.nationalacademies.org/nas/nashome.nsf>

- Federal Facilities Council (FFC) Standing Committee on
Physical Security and Hazard Mitigation
[http://www7.nationalacademies.org/ffc/
Physical_Security_Hazard_Mitigation.html](http://www7.nationalacademies.org/ffc/Physical_Security_Hazard_Mitigation.html)

○ National Research Council

<http://www.nationalacademies.org/nrc>

National Defense Industrial Association (NDIA)

<http://www.ndia.org>

Public Entity Risk Institute <http://www.riskinstitute.org>

Security Design Coalition <http://www.designingforsecurity.org>

Security Industry Association (SIA) <http://www.siaonline.org/>

Technical Support Working Group (Departments of Defense and State) <http://www.tswg.gov>

U.S. Air Force Electronic System Center (ESC), Hanscom Air Force Base <http://eschq.hanscom.af.mil/>

U.S. Army Soldiers and Biological Chemical Command (SBCCOM): Basic Information on Building Protection
<http://buildingprotection.sbccom.army.mil>

U.S. Department of Justice <http://www.usdoj.gov>

○ Federal Bureau of Investigation: Terrorism in the United States reports

<http://www.fbi.gov/publications/terror/terroris.htm>

○ Office of Domestic Preparedness (ODP)

<http://www.ojp.usdoj.gov/odp>

○ National Institute of Justice (NIJ)

<http://www.ojp.usdoj.gov/nij>

○ U.S. Marshals Service (USMS)

<http://www.usdoj.gov/marshals>

The Infrastructure Security Partnership (TISP)

<http://www.tisp.org>

Founding Organizations:

American Council of Engineering Companies (ACEC)

<http://www.acec.org>

The American Institute of Architects (AIA), Security Resource Center <http://www.aia.org/security>

American Society of Civil Engineers (ASCE) <http://www.asce.org>

○ Architectural Engineering Institute (AEI) of ASCE

<http://www.asce.org/instfound/aei.cfm>

○ Civil Engineering Research Foundation (CERF) of ASCE

<http://www.cerf.org>

○ Structural Engineering Institute (SEI) of ASCE

<http://www.seinstitute.org>

Associated General Contractors of America <http://www.agc.org>

Construction Industry Institute <http://construction-institute.org>

Federal Facilities Council – See National Academy of Sciences above.

Federal Emergency Management Agency (FEMA)

<http://www.fema.gov>

○ Building Performance Assessment Team

<http://www.fema.gov/mit/bpat>

○ Mitigation Planning

<http://www.fema.gov/fima/planning.shtm>

○ Human Caused Hazards <http://www.fema.gov/hazards>

National Institute of Standards and Technology (NIST), Building and Fire Research Laboratory <http://www.bfrl.nist.gov>

Naval Facilities Engineering Command

<http://www.navfac.navy.mil>

- Naval Facilities Engineering Service Center (NFESC),
Security Engineering Center of Expertise ESC66
<http://atfp.nfesc.navy.mil>

Society of American Military Engineers (SAME)
<http://www.same.org>

U.S. Army Corps of Engineers <http://www.usace.army.mil>

- Blast Mitigation Action Group, U.S. Army Corps of Engineers
Center of Expertise for Protective Design
<http://bmag.nwo.usace.army.mil>

- U.S. Army Corps of Engineers, Electronic Security Center
<http://www.hnd.usace.army.mil/esc>

- U.S. Army Corps of Engineers, Protective Design Center
<http://pdc.nwo.usace.army.mil>

Selected Member Organizations:

Air Conditioning Contractors of America <http://www.acca.org>

Air-Conditioning and Refrigeration Institute, Inc
<http://www.ari.org>

Airport Consultants Council <http://www.acconline.org>

Alliance for Fire & Smoke Containment & Control
<http://www.afsconline.org>

American Association of State Highway and Transportation
Officials (AASHTO) <http://www.transportation.org>

American Institute of Chemical Engineers, Center for Chemical
Process Safety <http://www.aiche.org/ccps>

American Planning Association <http://www.planning.org>

American Portland Cement Alliance
<http://www.portcement.org/apca>

American Public Works Association <http://www.apwa.net>

American Railway Engineering & Maintenance of Way
Association <http://www.arema.org>

American Society for Industrial Security International (ASIS)
<http://www.asisonline.org>

American Society of Heating, Refrigerating, and Air
Conditioning Engineers (ASHRAE) <http://www.ashrae.org>

American Society of Interior Designers <http://www.asid.org>

American Society of Landscape Architects (ASLA)
<http://www.asla.org>

American Society of Mechanical Engineers (ASME)
<http://www.asme.org>

American Underground Construction Association (AUA)
<http://www.auca.org> or <http://www.auaonline.org>

American Water Resources Association (AWRA)
<http://www.awra.org>

Associated Locksmiths of America <http://www.aloa.org>

Association of Metropolitan Water Agencies
<http://www.amwa.net>

Association of State Dam Safety Officials
<http://www.damsafety.org>

Building Futures Council <http://www.thebfc.com>

Building Owners and Managers Association International
(BOMA), Emergency Resource Center
<http://www.boma.org/emergency>

California Department of Health Services, Division of Drinking
Water & Environmental Management
<http://www.dhs.cahwnet.gov/ps/ddwem>

Construction Industry Roundtable <http://www.cirt.org>

Construction Innovation Forum <http://www.cif.org>

Construction Specifications Institute <http://www.csinet.org>

Construction Users Roundtable <http://www.curt.org>

Defense Threat Reduction Agency (DTRA) <http://www.dtra.mil>

Design-Build Institute of America <http://www.dbia.org>

Drexel (University) Intelligent Infrastructure & Transportation
Safety Institute <http://www.di3.drexel.edu>

Federal Highway Administration <http://www.fhwa.dot.gov>

Florida Department of Transportation, Emergency Management
Office <http://www11.myflorida.com/safety/Emp/emp.htm> or

Florida Department of Community Affairs, Division of
Emergency Management <http://www.floridadisaster.org/bpr/EMTOOLS/Severe/terrorism.htm> or
http://www.dca.state.fl.us/bpr/EMTOOLS/CIP/critical_infrastructure_protecti.htm

George Washington University, Institute for Crisis, Disaster, and
Risk Management <http://www.cee.seas.gwu.edu> or
<http://www.seas.gwu.edu/~icdm>

Homeland Protection Institute, Ltd. <http://www.hpi-tech.org>

Inland Rivers Ports and Terminals <http://www.irpt.net>

Institute of Electrical and Electronics Engineers, Inc. – USA
<http://www.ieeeusa.org> or
<http://www.ieee.org/portal/index.jsp>

International Association of Foundation Drilling
<http://www.adsc-iafd.com>

International Code Council (ICC) <http://www.intlcode.org>
Consolidates services – products and operations of BOCA
(Building Officials and Code Administrators), ICBO
(International Conference of Building Officials), and SBCCI
(Southern Building Code Congress International) into one
member service organization – the International Code
Council (ICC) in January 2003.

International Facility Management Association (IFMA)
<http://www.ifma.org>

Market Development Alliance of the FRP Composites Industry
<http://www.mdacomposites.org>

Multidisciplinary Center for Earthquake Engineering Research
<http://mceer.buffalo.edu>

National Aeronautics and Space Administration
<http://www.nasa.gov>

National Capital Planning Commission (NCPC)
<http://www.ncpc.gov>

○ Security and Urban Design
http://www.ncpc.gov/planning_init/security.html

National Center for Manufacturing Sciences
<http://www.ncms.org>

National Concrete Masonry Association <http://www.ncma.org>

National Conference of States on Building Codes and Standards
<http://www.ncsbc.org>

National Council of Structural Engineers Associations (NCSEA)
<http://www.ncsea.com> or
<http://dwp.bigplanet.com/engineers/homepage>

National Crime Prevention Institute
<http://www.louisville.edu/a-s/ja/ncpi/courses.htm>

National Fire Protection Association <http://www.nfpa.org>

National Institute of Building Sciences (NIBS)
<http://www.nibs.org> and <http://www.wbdg.org>

National Park Service, Denver Service Center
<http://www.nps.gov/dsc>

National Precast Concrete Association <http://www.precast.org>

National Wilderness Training Center, Inc.
<http://www.wildernesstraining.net>

New York City Office of Emergency Preparedness
<http://www.nyc.gov/html/oem>

Ohio State University <http://www.osu.edu/homelandsecurity>

Pentagon Renovation Program <http://renovation.pentagon.mil>

Portland Cement Association (PCA) <http://www.portcement.org>

Primary Glass Manufacturers Council
<http://www.primaryglass.org>

Protective Glazing Council <http://www.protectiveglazing.org>

Protective Technology Center at Penn State University
<http://www.ptc.psu.edu>

SAVE International <http://www.value-eng.org>

Society of Fire Protection Engineers <http://www.sfpe.org>

Southern Building Code Congress, International
<http://www.sbcci.org>

Sustainable Buildings Industry Council
<http://www.sbicouncil.org>

The Security and Hazards Mitigation Alliance, Contact Susan Ballard Hirsch at Email Address: sballard@g-and-o.com

Transit Standards Consortium <http://www.tsconsortium.org>

Transportation Research Board/Marine Board
<http://www.trb.org>

Transportation Security Administration - Maritime and Land
<http://www.tsa.dot.gov>

U.S. Air Force Civil Engineer Support Agency
<http://www.afcesa.af.mil>

U.S. Coast Guard <http://www.uscg.mil>

U.S. Department of Energy <http://www.energy.gov>

○ Sandia National Laboratories (SNL) <http://www.sandia.gov>

- Architectural Surety Program
<http://www.sandia.gov/archsur>

- Critical Infrastructure Protection initiative
http://www.sandia.gov/LabNews/LN02-11-00/steam_story.html
- U.S. Department of Health and Human Services
<http://www.hhs.gov>
- U.S. Department of Veterans Affairs (VA)
<http://www.va.gov/facmgt>
- U.S. Environmental Protection Agency (EPA), Chemical Emergency Preparedness and Prevention Office (CEPPO) - Counter-terrorism <http://www.epa.gov/swercepp/cntr-ter.html>
- U.S. General Services Administration (GSA) <http://www.gsa.gov>
 - Office of Federal Protective Service (FPS) of GSA
http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=117945&contentType=1005&P=1&S=1
 - Office of Public Building Service (PBS) of GSA
http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=22883&contentType=1005&PPzz=1&S=1
 - Office of the Chief Architect of GSA http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=22899&contentType=1005 and <http://www.oca.gsa.gov>
- U.S. Green Building Council <http://www.usgbc.org>
- U.S. Marine Corps Headquarters <http://www.usmc.mil>
- U.S. Society on Dams <http://www.ussdams.org>
- University of Missouri, Department of Civil & Environmental Engineering, National Center for Explosion Resistant Design
<http://www.engineering.missouri.edu/explosion.htm>
- Virginia Polytechnic Institute and State University
<http://www.ce.vt.edu>
- Water and Wastewater Equipment Manufacturers Association
<http://www.wwema.org>

The Partnership for Critical Infrastructure (PCIS)

<http://www.pcis.org> (Note: Involved mainly with information systems and not building real property.)

Government:

Department of Commerce Critical Infrastructure Assurance Office (CIAO) <http://www.ciao.gov>

Department of Energy (DOE) <http://www.energy.gov>

Department of Homeland Security
<http://www.whitehouse.gov/deptofhomeland>

National Infrastructure Protection Center (NIPC)
<http://www.nipc.gov>

Private Sector:

Anser Institute for Homeland Security (ANSER)
<http://www.homelandsecurity.org>

The Financial Services Roundtable Technology Group (BITS)
<http://www.bitsinfo.org>

CERT® Coordination Center (CERT/CC) <http://www.cert.org>

Electronic Warfare Associates (EWA) <http://www.ewa.com>

Information Technology Association of America (ITAA)
<http://www.itaa.org>

The Institute for Internal Auditors (IIA) <http://www.theiia.org>

National Cyber Security Alliance (Alliance)
<http://www.staysafeonline.info>

North American Electric Reliability Council (NERC)
<http://www.nerc.com>

SANS Institute (SANS – SysAdmin, Audit, Network, Security)
<http://www.sans.org>

The U.S. Chamber of Commerce, Center for Corporate Citizenship (CCC) <http://www.uschamber.com/cc>

Selected States and Local Organizations:

Association of Metropolitan Water Agencies

<http://www.amwa.net>

The Council of State Governments (CSG) <http://www.csg.org>

International Association of Emergency Managers (IAEM)

<http://www.iaem.com>

National Association of State CIOs (NASCIO)

<http://www.nascio.org>

National Emergency Managers Association (NEMA)

<http://www.nemaweb.org>

National Governor's Association (NGA) <http://www.nga.org>

The National League of Cities (NLC) <http://www.nlc.org>

American Association of State Highway and Transportation Officials

A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection, May 2002 , The American Association of State Highway and Transportation Officials' Security Task Force, Washington, D.C. <http://security.transportation.org/community/security/guides.html>

The American Institute of Architects

Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients, November 2001, The American Institute of Architects (book) <http://www.aia.org/security>

American Institute of Chemical Engineers

Pub No: G-79, *Guidelines for Analyzing and Managing the Security Vulnerabilities at Fixed Chemical Sites*, 2002, **Center for Chemical Process Safety**, ISBN No: 0-8169-0877-X <http://www.aiche.org/ccpssecurity>

American Medical Association

Physical injuries and fatalities resulting from the Oklahoma City bombing, August 7, 1996, Mallonee, S., Shariat, S., Stennies, G., Waxweiler, R., Hogan, D., and Jordan, F., The Journal of the American Medical Association, Vol. 276 No. 5., pp 382-387
Abstract at URL: <http://jama.ama-assn.org/cgi/content/abstract/276/5/382>

American Society of Civil Engineers

Blast Effects on Buildings: Design of Buildings to Optimize Resistance to Blast Loading, 1995, G.C. Mays and P.D. Smith, London: Thomas Telford, Ltd., American Society of Civil Engineers, ISBN: 0-7277-2030-9 <http://www.pubs.asce.org/BOOKdisplay.cgi?9990338>

Blast Resistant Design of Commercial Buildings, 1996, M. Ettouney, R. Smilowitz, and T. Rittenhouse, Practice Periodical on Structural

Design and Construction, Vol. 1, No. 1, February 1996, American Society of Civil Engineers <http://ojps.aip.org/dbt/dbt.jsp?KEY=PPSCFX&Volume=1&Issue=1> A preprint of the final article is available at <http://www.wai.com/AppliedScience/Blast/blast-struct-design.html>

Design of Blast Resistant Buildings in Petrochemical Facilities, 1997, American Society of Civil Engineers, ISBN: 0-7844-0265-5
<http://www.pubs.asce.org/BOOKdisplay.cgi?9704510>

Glass-Related Injuries in Oklahoma City Bombing, Journal of Performance of Constructed Facilities, May 1999, 13, No. 2, H Scott Norville, Natalie Harville, Edward J. Conrath, Sheryll Shariat, and Sue Mallonee <http://www.pubs.asce.org/WWWdisplay.cgi?9902006>

Lessons from the Oklahoma City Bombing: Defensive Design Techniques, January 1997, Eve E. Hinman and David J. Hammond, January 1997, American Society of Civil Engineers (ASCE Press), Reston, VA, ISBN: 0784402175 <http://www.asce.org/publications/booksdisplay.cfm?type=9702295>

Minimum Design Loads for Buildings and Other Structures, ASCE 7-02, 2002, American Society of Civil Engineers, ISBN: 0-7844-0624-3, [note revision of 7-98, does not include building security or antiterrorism but covers all natural hazards]
http://www.asce.org/publications/dsp_pubdetails.cfm?puburl=http://www.pubs.asce.org/ASCE7.html?9991330

Vulnerability and Protection of Infrastructure Systems: The State of the Art, An ASCE Journals Special Publication compiling articles from 2002 and earlier available online http://ascestore.aip.org/OA_HTML/aipCCtpSctDspRte.jsp?section=10123

Architectural Engineering Institute of American Society of Civil Engineers AEI Newsletter, *The Team, Special Terrorism Issue*, Fall 2001, Volume 4, Issue 3 http://www.asce.org/pdf/aei_11_1.pdf

Structural Engineering Institute of American Society of Civil Engineers *Structural Design for Physical Security: State of the Practice*, 1999, Edward Conrath, et al., Reston, Virginia, Structural

Engineering Institute of American Society of Civil Engineers
<http://www.pubs.asce.org/BOOKdisplay.cgi?9990571>

American Society of Heating, Refrigerating, and Air-Conditioning Engineers

Defensive Filtration, ASHRAE Journal, December 2002, James D. Miller <http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=9346&view=item&categoryid=409&page=1&loginid=29483>

Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents on Risk Management Guidance for Health, Safety and Environmental Security under Extraordinary Incidents, Washington, D.C., January 26, 2003
<http://xp20.ashrae.org/about/extraordinary.pdf>

Risk Management Guidance for Health and Safety under Extraordinary Incidents, ASHRAE 2002 Winter Meeting Report, January 12, 2002 <http://atfp.nfesc.navy.mil/pdf/ASHRAE%20CBR%20Guidance.pdf> or http://engineering.tamu.edu/safety/guidelines/faclab/ASHRAE_Security_Rpt_12Jan02.pdf

Standard 62-2001, *Ventilation for Acceptable Indoor Air Quality* (ANSI Approved), ISSN 1041-2336, addenda to basic ANSI/ASHRAE Standard 62 basic (1989) <http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=6852&view=item&categoryid=311&page=1&loginid=29483>

Building Owners and Managers Association International

How to Design and Manage Your Preventive Maintenance Program, 1996 <http://www.boma.org/pubs/bomampm.htm>

Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health

Publication No. 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological*

Attacks, May 2002, Cincinnati, Ohio www.cdc.gov/niosh/bldvent/2002-139.html

Publication No. 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, May 2002, Cincinnati, Ohio < Publication No. 2003-136, *Guidance for Filtration and Air Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, April 2003, Cincinnati, Ohio <http://www.cdc.gov/niosh/docs/2003-136/2003-136.html>

Central Intelligence Agency

Chemical, Biological, Radiological Incident Handbook, October 1998
http://www.cia.gov/cia/publications/cbr_handbook/cbrbook.htm

Council on Tall Buildings and Urban Habitat

Building Safety Enhancement Guidebook, 2002 <http://www.ctbuh.org>

Task Force on Tall Buildings: "The Future," October 15, 2001
http://www.lehigh.edu/ctbuh/htmlfiles/hot_links/report.pdf or
http://www.ctbuh.org/htmlfiles/hot_links/report.pdf

Federal Aviation Administration

DOT/FAA/AR-00/52, *Recommended Security Guidelines for Airport Planning, Design and Construction*, Revised June 2001, Associate Administrator for Civil Aviation Security Office of Civil Aviation Security, Policy and Planning, Federal Aviation Administration, Washington, DC 20591 (not available on Internet)

FAA Order 1600.69A, *FAA Facility Security Management Program*, updated FAA Order 1600.69B to be published shortly – The Federal Aviation Administration's criteria for the protection of its facilities. [*For Official Use Only*] (not available on Internet)

Federal Emergency Management Agency

FEMA 152, *Seismic Considerations: Apartment Buildings, Earthquake Hazards Reduction Series 37*, November 1988, Washington, D.C. (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480- 2520, Fax: 301-362-5335

FEMA 153, *Seismic Considerations: Office Buildings, Earthquake Hazards Reduction Series 38*, November 1988, Washington, D.C. (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480- 2520, Fax: 301-362-5335

FEMA 154, *Rapid Visual Screening of Buildings for Seismic Hazards: A Handbook (2nd Edition)*, 2002, 1988, Washington, D.C. (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480- 2520, Fax: 301-362-5335

FEMA 277, *The Oklahoma City Bombing: Improving Building Performance through Multi-Hazard Mitigation*, August 1, 1996, Washington, D.C. <http://www.fema.gov/mit/bpat/bpat009.htm>

FEMA 372, *Mitigation Resources for Success (CD-ROM)*, October 2001, Washington, D.C. http://www.fema.gov/pdf/library/poster_fnl2.pdf

FEMA 386-2, *Understanding Your Risks, Identifying Hazards and Estimating Losses*, August 2001. http://www.fema.gov/fima/planning_toc3.shtm

FEMA 386-7, *Integrating Human-Caused Hazards Into Mitigation*, September 2002, *Planning* <http://www.fema.gov/fima/antiterrorism/resources.shtm>

FEMA 403, *World Trade Center Building Performance Study: Data Collection, May 2002, Preliminary Observations, and Recommendations*, Washington, D.C. <http://www.fema.gov/library/wtcstudy.shtm>

State and Local Guide 101, *Guide for All-Hazard Emergency Operations Planning, Chapter 6, Attachment G, Terrorism*, April 2001

General Services Administration

Balancing Security and Openness: A Thematic Summary of a Symposium on Security and the Design of Public Buildings, November 30, 1999
http://hydra.gsa.gov/pbs/pc/gd_files/SecurityOpenness.pdf

Cost Impact of ISC Security Criteria, GSA & Applied Research Associates, Inc., Bryant L. and Smith J., Vicksburg, Mississippi
<http://www.oca.gsa.gov/specialphp/References.php>

Facility Standards for the Public Building Service (PBS-P100); Chapter 8, Security Design, Revised November 2000
<http://hydra.gsa.gov/pbs/pc/facilitiesstandards/>

Mail Center Manager's Security Guide – Second Edition, October 22, 2002 http://www.gsa.gov//attachments/GSA_PUBLICATIONS/extpub/MailCenterManagersSecurityGuideV2.pdf

Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects, November 2000 http://www.oca.gsa.gov/about_progressive_collapse/progcollapse.php

Security Reference Manual, Part 3: Blast Design and Assessment Guidelines, July 31, 2001 [*For Official Use Only*]
http://www.oca.gsa.gov/specialphp/restrictedblast_effects.php

Healthy Building International, Inc.

Vulnerability Assessments and Counter Terrorist Protocols
<http://www.healthybuildings.com/s2/vacbt.pdf>

Interagency Security Committee (executive agent – GSA)

ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects, May 28, 2001, [For Official Use Only]
<http://www.oca.gsa.gov/restricted/protectedfiles/ISCCriteriaMay282001.PDF>

Institute of Transportation Engineers

The Influence of Traffic Calming Devices upon Fire Vehicle Travel Times, Coleman, Michael A., 1997, ITE Annual Meeting Compendium, 1997 pp. 838-845 <http://webservices.camsys.com/fhwa/cmn/cmn33.htm>

Split Speed Bump, 1998, Mulder, Kathy, Washington, D.C., TE International Conference, 1998 <http://www.ite.org/traffic/documents/CCA98A33.pdf>

Lawrence Berkeley National Lab

Protecting Buildings From a Biological or Chemical Attack: actions to take before or during a release. LBNL/PUB-51959, January 10, 2003 <http://securebuildings.lbl.gov/images/bldgadvice.pdf>

National Academy of Sciences

Combating Terrorism: Prioritizing Vulnerabilities and Developing Mitigation Strategies, Project Identification Number: NAEP-R-02-01-A, National Academy of Engineering, soon to be published <http://www4.nationalacademies.org/webcr.nsf/ProjectScopeDisplay/NAEP-R-02-01-A?OpenDocument>

National Capital Planning Commission

Designing for Security in the Nation's Capital, October 2001 http://www.ncpc.gov/whats_new/ITFreport.pdf

The National Capital Planning Urban Design and Security Plan, October 2002 <http://www.ncpc.gov/publications/udsp/Final%20UDSP.pdf>

National Institute of Building Sciences

Whole Building Design Guide: Provide Security for Building Occupants and Assets, <http://www.wbdg.org/design/index.php?cn=2.7.4&cx=0>

National Research Council

Protecting Buildings and People from Terrorism: Technology Transfer for Blast-effects Mitigation, 2001, National Academy Press, Washington, D.C., ISBN 0-309-08286-2 <http://books.nap.edu/books/0309082862/html/index.html>

Protecting Buildings From Bomb Blast, Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications, 1995, National Academy Press, Washington, D.C., ISBN 0-309-05375-7 <http://books.nap.edu/books/0309053757/html/index.html>

Protection of Federal Office Buildings Against Terrorism, 1988, Committee on the *Protection of Federal Facilities Against Terrorism*, Building Research Board, National Academy Press, Washington, D.C., ISBN 0-309-07691-9 <http://books.nap.edu/books/0309076463/html/index.html>

Society of American Military Engineers

National Symposium of Comprehensive Force Protection, October 2001, Charleston, South Carolina, Lindbergh & Associates For list of participants access <http://www.same.org/forceprot/force.htm>

The House National Security Committee

Statement of Chairman Floyd D. Spence on the Report of the Bombing of Khobar Towers, August 1996, Washington, D.C. <http://www.house.gov/hasc/Publications/104thCongress/Reports/saudi.pdf>

Technical Support Working Group (TSWG)

Terrorist Bomb Threat Stand-Off Card with Explanation of Use, http://www.tswg.gov/tswg/prods_pubs/newBTSCPress.htm

U.S. Air Force

ESL-TR-87-57, *Protective Construction Design Manual*, November 1989; Contact Airbase Technologies Division (AFRL/MLQ) at Tyndall Air Force Base, Florida, via e-mail to techinfo@afrl.af.mil. [Superceded by Army Technical Manual TM 5-855-1 (Air Force Pamphlet AFPAM 32-1147(I), Navy Manual NAVFAC P-1080, DSWA Manual DAHSCWEMAN-97), December 1997]

Expedient Hardening Methods for Structures Subjected to the Effect of Nonnuclear Munitions, October 1990, Wright Laboratory Report (not available on Internet)

Installation Entry Control Facilities Design Guide, October 2002, Air Force Center for Environmental Excellence

<http://www.afcee.brooks.af.mil/dc/dcd/gate/index.html>

Installation Force Protection Guide, 1997, Air Force Center for Environmental Excellence <http://www.afcee.brooks.af.mil/dc/dcd/arch/force.pdf>

Vehicle Bomb Mitigation Guide, July 1, 1999, Force Protection Battlelab [**For Official Use Only**] Contact the USAF Force Protection Battlelab, Lackland Air Force Base, Texas, phone: (210) 671-0058

U.S. Army

Field Manual (FM) 3-19.30, *Physical Security*, January 8, 2001, Washington, D.C. <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/fm3-19.30.pdf> or http://www.wood.army.mil/mpdoctrines/PDF_Files/FM_3-19.30.pdf

Field Manual (FM) 5-114, *Engineer Operations Short of War*, July 13, 1992 <http://155.217.58.58/cgi-bin/atdl.dll/fm/5-114/toc.htm>

Technical Instruction 853-01 (Draft), *Protecting Buildings and Their Occupants from Airborne Hazards*, October 2001 http://buildingprotection.sbcom.army.mil/basic/airborne_hazards

U.S. Army Corps of Engineers

Engineer Technical Letters (ETL)

ETL 1110-3-494, *Airblast Protection Retrofit for Unreinforced Concrete Masonry Walls*, July 14, 1999 [**Restricted Access**] <http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-495, *Estimating Damage to Structures from Terrorist Bombs Field Operations Guide*, July 14, 1999 [**Restricted Access**] <http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-498, *Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents*, February 24, 1999 <http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-501, *Window Retrofit Using Fragment Retention Film with Catcher Bar System*, July 14, 1999 [**Restricted Access**] <http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

Protective Design – Mandatory Center of Expertise – Technical Reports

PDC-TR-91-6, *Blast Analysis Manual, Part 1 – Level of Protection Assessment Guide*, July 1991 [**For Official Use Only**] Contact U.S. Army Corps of Engineers Protective Design Center, ATTN: CENWO-ED-ST, 215 N. 17th Street, Omaha, Nebraska, 68102-4978, phone: (402) 221-4918

Technical Manuals (TM)

TM 5-853-1, *Security Engineering Project Development*, May 12, 1994, also Air Force Manual 32-1071, Volume 1 [**For Official Use Only**] <http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-2, *Security Engineering Concept Design*, May 12, 1994, also Air Force Manual 32-1071, Volume 2 [**For Official Use Only**] <http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-3, *Security Engineering Final Design*, May 12, 1994, also Air Force Manual 32-1071, Volume 3 [*For Official Use Only*] <http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-4, *Security Engineering Electronic Security Systems*, May 12, 1994 <http://www.military-info.com/mphoto/newlj98.htm#engineer>

TM 5-855-4, *Heating, Ventilation, and Air Conditioning of Hardened Installations*, November 28, 1986 <http://www.usace.army.mil/inet/usace-docs/armytm/tm5-855-4/toc.htm>

TM 5-1300, *Structures to Resist Accidental Explosions*, November 19, 1990, (also Navy NAVFAC (Naval Facilities) P-397, Air Force Regulation 88-2); Contact David Hyde, U.S. Army Engineer Research and Development Center, 3909 Halls Ferry Road, Vicksburg, Mississippi 39180 or via e-mail to hyded@ex1.wes.army.mil

U.S. Department of Commerce

Administrative Orders (DAO)

DAO 206-5, *Occasional Use of Public Areas in Public Buildings*, December 9, 1986 <http://www.osec.doc.gov/bmi/daos/206-5.htm>

DAO 207-1, *Security Programs*, June 24, 1991, Amended September 6, 1991 <http://www.osec.doc.gov/bmi/daos/207-1.htm>

Critical Infrastructure Assurance Office

Vulnerability Assessment Framework 1.1, October 1998
<http://www.ciao.gov/resource/vullassessframework.pdf>

Practices For Securing Critical Information Assets, January 2000 http://www.ciao.gov/resource/Practices_For_Securing_Critical_Information_Assets.pdf

U.S. Department of Defense

DoD Security Engineering Manual [Expected to have a major portion for public distribution once published as Unified Facilities Criteria and a smaller portion For Official Use Only similar to the UFC for AT Standards for Buildings listed below. This publication will replace Army Technical Manual 5-853 (Air Force Joint Manual 32-1071) volumes 1, 2, and 3 and Navy Military Handbook 1013/1A]

DoD O-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence: Mandatory Standards and Implementing Guidance, with Changes 1 and 2*, February 1993, Change 1 — May 21, 1993, Change 2 – October 3, 1997 [**For Official Use Only**] <http://www.dtic.mil/whs/directives/corres/publ.html>

Force Protection Equipment Demonstration IV, 6-8 May 2003
<http://www.fped4.org>

Interim Antiterrorism/Force Protection Construction Standards, December 16, 1999 [**For Official Use Only**] Contact U.S. Army Engineer District, Omaha, ATTN: CENWO-ED-ST, 215 North 17th Street, Omaha, NE 68102-4978, phone: (402) 221-4918.

Interim Antiterrorism/Force Protection Construction Standards – Progressive Collapse Guidance, April 4, 2000 (not available on Internet) Contact U.S. Army Corps of Engineers Protective Design Center, ATTN: CENWO-ED-ST, 215 N. 17th Street, Omaha, Nebraska, 68102-4978, phone: (402) 221-4918

Unified Facilities Criteria (UFC)

UFC 3-340-01, Design and Analysis of Hardened Structures to Conventional Weapons Effects, June 30, 2002 [**For Official Use Only**] [Formerly Army TM 5-855-1] <http://www.hnd.usace.army.mil/techinfo/ufc/UFC3-340-01WEB.PDF>

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, July 31, 2002 <http://www.wbdg.org/ccbref/ccbdoc.php?category=ufc&docid=106&ref=1>

Unified Facilities Guide Specifications (UFGS)

UFGS-02821A, *Fencing*, February 2002

<http://www.ccb.org/ufigs/pdf/02821A.pdf>

UFGS-02840A, *Active Vehicle Barriers*, February 2002

<http://www.ccb.org/ufigs/pdf/02840A.pdf>

UFGS-02841N, *Traffic Barriers*, August 2001

<http://www.ccb.org/ufigs/pdf/02841N.pdf>

UFGS-08390A, *Blast Resistant Doors*, April 2001

<http://www.ccb.org/ufigs/pdf/08390.pdf>

UFGS-08581, *Blast Resistant Tempered Glass Windows*,

August 2001 <http://www.ccb.org/ufigs/pdf/08581.pdf>

UFGS-08840A, *Plastic Glazing*, July 1995

<http://www.ccb.org/ufigs/pdf/08840A.pdf>

UFGS-08850, *Fragment Retention Film for Glass*, July 1992

<http://www.ccb.org/ufigs/pdf/08850.pdf>

UFGS-11020, *Security Vault Door*, August 2002

<http://www.ccb.org/ufigs/pdf/11020.pdf>

UFGS-11025, *Forced Entry Resistant Components*, August

2001 <http://www.ccb.org/ufigs/pdf/11025.pdf>

UFGS-11035, *Bullet-Resistant Components*, April 2000

<http://www.ccb.org/ufigs/pdf/11035.pdf>

UFGS-13095A, *Electromagnetic (EM) Shielding*, July 2001

<http://www.ccb.org/ufigs/pdf/13095A.pdf>

UFGS-13420A, *Self-Acting Blast Valves*, November 1997

<http://www.ccb.org/ufigs/pdf/13420A.pdf>

U.S. Department of Energy

DOE/TIC 11268, *A Manual for the Prediction of Blast and Fragment Loadings on Structures*, February 1992, Albuquerque, NM, Southwest Research Institute [not available on Internet]

U.S. Department of Homeland Security

National Strategy for Homeland Security, July 2002

http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf

The National Strategy for the Physical Protection of Critical

Infrastructures and Key Assets, February 2003 http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

National Strategy to Secure Cyberspace, February 2003

http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

U.S. Department of Housing and Urban Development

The Avoidance of Progressive Collapse, Regulatory approaches to the problem, PB-248 781, October 1975, Division of Energy, Building Technology and Standards, Office of Policy Development and Research, Washington, D.C. 20410 (not available on Internet)

Creating Defensible Space, April 1996, Oscar Newman, Washington, D.C. <http://www.huduser.org/publications/pdf/def.pdf>

U.S. Department of Justice

Federal Bureau of Investigation (FBI)

Terrorism in the United States, 1999, Washington, D.C., Counterterrorism Division <http://www.fbi.gov/publications/terror/terror99.pdf>

Office of Domestic Preparedness (ODP)

Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit, NCJ181200, May 15, 2000, *[For Official Use Only]* <http://www.ojp.usdoj.gov/odp/docs/assessment.txt>

National Institute of Justice (NIJ)

The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies, September 1999, with U.S. Department of

Education, Safe and Drug-Free Schools Program; and
U.S. Department of Energy, Sandia National Laboratories
<http://www.ncjrs.org/school/home.html>

NIJ Guide 100-00, *Guide for the Selection of Chemical Agent
and Toxic Industrial Material Detection Equipment for
Emergency First Responders*, June 2000
<http://www.ncjrs.org/pdffiles1/nij/184449.pdf>

NIJ Guide 101-00, *An Introduction to Biological Agent
Detection Equipment for Emergency First Responders*, December
2001 <http://www.ncjrs.org/pdffiles1/nij/190747.pdf>

NIJ Guide 102-00, *Guide for the Selection of Personal Protective
Equipment for Emergency First Responders*, Volumes I-IV,
November 2002 <http://www.ncjrs.org/pdffiles1/nij/191518.pdf>

NIJ Guide 602-00, *Guide to the Technologies of Concealed
Weapon and Contraband Imaging and Detection*, February
2001 <http://www.ncjrs.org/pdffiles1/nij/184432.pdf>

NIJ Standard 0108.01, *Blast Resistant Protective Materials*,
September 1985 www.ccb.org under Standards,
Government Standards

*Crime Prevention Through Environmental Design and
Community Policing*, August 1996, Dan Fleissner and Fred
Heinzelmann, Washington, D. C. <http://www.ncjrs.org/pdffiles/crimepre.pdf>

*Crime Prevention Through Environmental Design in Parking
Facilities*, April 1996, Mary S. Smith, Washington, D. C.
<http://www.ncjrs.org/pdffiles/cptedpkg.pdf>

“Designing Out” Gang Homicides and Street Assaults,
November 1998, James Lasley, Washington, D. C. <http://www.ncjrs.org/pdffiles/173398.pdf>

*The Expanding Role of Crime Prevention Through
Environmental Design in Premises Liability*, April 1996, Corey

L. Gordon and William Brill Washington, D. C.
<http://www.ncjrs.org/pdffiles/cptedlia.pdf>

Physical Environment and Crime, January 1996, Ralph B. Taylor and Adele V. Harrell, Washington, D. C.
<http://www.ncjrs.org/pdffiles/physenv.pdf>

Visibility and Vigilance: Metro's Situational Approach to Preventing Subway Crime, November 1997, Nancy G La Vigne, Washington, D.C. <http://www.ncjrs.org/pdffiles/166372.pdf>

U.S. Marshals Service

Vulnerability Assessment of Federal Facilities, June 28, 1995
<http://www.oca.gsa.gov>

U.S. Department of State, Bureau of Diplomatic Security

Architectural Engineering Design Guidelines (5 Volumes), March 1998 [**For Official Use Only**] (not available on Internet)

Certification Standard SD-STD-01.01, Revision G (Amended), *Forced Entry and Ballistic Resistance of Structural Systems*, Amended April 30, 1993 www.ccb.org under Standards, Government Standards

Patterns of Global Terrorism, 2001, May 2002, Washington, D.C.
<http://www.state.gov/s/ct/rls/pgtrpt/2001/pdf>

Physical Security Standards Handbook, January 7, 1998 [**For Official Use Only**] (not available on Internet)

Structural Engineering Guidelines for New Embassy Office Buildings, August 1995 [**For Official Use Only**] (not available on Internet)

The Report of the Accountability Review Board on the Embassy Bombings in Nairobi and Dar es Salaam on August 7, 1998, January 1999, Washington, D.C. http://www.state.gov/www/regions/africa/accountability_report.html

U.S. Department of the Treasury/Bureau of Alcohol, Tobacco and Firearms

Vehicle Bomb Explosion Hazard And Evacuation Distance Tables, 1999, request in writing, address information available at http://www.atf.treas.gov/pub/fire-explo_pub/i54001.htm

U.S. Department of Veterans Affairs

Physical Security Assessment of Veterans Affairs Facilities, Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs, 6 September 2002 <http://www.va.gov/facmgt/standard/etc/vaphysicalsecurityreport.pdf>

U.S. Fire Administration (USFA of FEMA)

The Critical Infrastructure Protection Process Job Aid, May 1, 2002 <http://www.usfa.fema.gov/dhtml/fire-service/cipc-jobaid.cfm>

U.S. Navy

Design Manual (DM) NAVFAC (Naval Facilities Command)

NAVFAC DM 2.08, *Blast Resistant Structures*, December 1986 <http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=46&ref=1>

NAVFAC DM 13.02, *Commercial Intrusion Detection Systems (IDS)*, September 1986 <http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=47&ref=1>

Military Handbooks (MIL-HDBK)

MIL-HDBK-1002/1, *Structural Engineering General Requirements*, November 30, 1987 <http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=48&ref=1>

MIL-HDBK-1004/4, *Electrical Utilization Systems*, October 13, 1987 <http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=49&ref=1>

MIL-HDBK-1012/3, *Telecommunications Premises Distribution Planning, Design, and Estimating*, May 31, 1996

<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=50&ref=1>

MIL-HDBK-1013/1A, *Design Guidelines for Physical Security of Fixed Land-Based Facilities*, December 15, 1993 For copies contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, (215) 697-2179, FAX (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities*, May 14, 1993 For copies contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, (215) 697-2179, FAX (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/12, *Evaluation of Security Glazing for Ballistic, Bomb, and Forced Entry Tactics*, March 10, 1997 For copies contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, (215) 697-2179, FAX (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK- 1013/14, *Selection and Application of Vehicle Barriers*, February 1, 1999 For copies contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, (215) 697-2179, FAX (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

TechData Sheets – Naval Facilities Engineering Service Center (NFESC)

TDS-2062-SHR, *Estimating Damage to Structures from Terrorist Bombs*, September 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division

(ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370, (805) 982-1582 (Primary), (805) 982-4817 (Alternate), (805) 982-1253 (Fax)

TDS-2063-SHR, *Blast Shielding Walls*, September 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370, (805) 982-1582 (Primary), (805) 982-4817 (Alternate), (805) 982-1253 (Fax)

TDS-2079-SHR, *Planning and Design Considerations for Incorporating Blast Mitigation in Mailrooms*, May 2000 For copies contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, (215) 697-2179, FAX (215) 697-1462

TDS-2090-SHR, *Design Parameters for a Controlled Entry Point* For copies contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, (215) 697-2179, FAX (215) 697-1462

User Guides – Naval Facilities Engineering Service Center (NFESC)

UG-2030-SHR, *Security Glazing Applications*, May 1998, distributed June 25, 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370, (805) 982-1582 (Primary), (805) 982-4817 (Alternate), (805) 982-1253 (Fax)

UG-2031-SHR, *Protection Against Terrorist Vehicle Bombs*, May 1998, distributed June 25, 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370, (805) 982-1582 (Primary), (805) 982-4817 (Alternate), (805) 982-1253 (Fax)

Other Books, Magazines, Magazine Articles, and Newspaper Articles

Atlas, Randall I., June 1998, *Designing for Crime and Terrorism, Security and Technology Design* (not found on Internet – suspect this may be a magazine article in Security and Technology Design magazine) Security Technology and Design Magazine Reprint Services, Jim Benesh, Phone: (800) 547-7377 x324, FAX: (920) 568-2244, E-MAIL: jim.benesh@cygnuspub.com

Archibald, Rae W., et al., 2002, *Security and Safety in Los Angeles High-Rise Buildings after 9/11*. RAND, Santa Monica, California, ISBN: 0-8330-3184-8 <http://www.rand.org/publications/DB/DB381>

Broder, James F., December 15, 1999, *Risk Analysis and the Security Survey, 2nd Edition*, Butterworth-Heinemann, Stoneham, Massachusetts, ISBN 0750670894 http://www.amazon.com/exec/obidos/ASIN/0750670894/ref=pd_sxp_elt_11/103-7416668-4182264#product-details

Craighead, Geoff, December 2002, *High-Rise Security and Fire Life Safety, 2nd Edition*, Academic Press, ISBN 0750674555 http://www.amazon.com/exec/obidos/tg/detail/-/0750674555/qid=/br=1-/ref=br_lf_b_/t/103-7416668-4182264?v=glance&s=books&n=173507#product-details

Crowe, Timothy D., 2000, *Crime Prevention Through Environmental Design: Applications Of Architectural Design And Space Management Concepts (2nd Edition)*, Stoneham, Massachusetts, Butterworth-Heinemann, ISBN: 075067198X <http://www.amazon.com/exec/obidos/ASIN/075067198X/103-7416668-4182264#product-details>

Fehr, Stephen C., July 1996, Parking Under Siege in D.C.: U.S. Anti-Terrorism Plan Threatens 360 Spaces, *The Washington Post*, July 13, 1996 <http://www.washingtonpost.com/wp-adv/archives/advanced.htm>

Fenelly, Lawrence J., June 1997, *Effective Physical Security, 2nd Edition*, Stoneham, Massachusetts, Butterworth-Heinemann,

ISBN 0-75-069873-X http://www.amazon.com/exec/obidos/ASIN/075069873X/ref=ase_lksmsubsite-dfl-2-20/103-7416668-4182264#product-details

Garcia, Mary Lynn, February 23, 2001, *The Design and Evaluation of Physical Protection Systems*, Stoneham, Massachusetts, Butterworth-Heinemann, ISBN: 0750673672 <http://www.amazon.com/exec/obidos/tg/detail/-/0750673672//103-7416668-4182264?v=glance&s=books>

Gonchar, Joann, March 2002, Building for a Secure Future: Government Facilities under way incorporate already tough standards, *Engineering News-Record*, March 25, 2002 <http://www.construction.com/NewsCenter/Headlines/ENR/20020325e.asp>

Greene, R.W., October 2002, *Confronting Catastrophe: A GIS Handbook*, ESRI Press, ISBN: 1589480406 http://www.amazon.com/exec/obidos/ASIN/1589480406/ref=ase_inktomi-bkasin-20/103-7416668-4182264

Hart, Sara, March 2002, In the aftermath of September 11, the urban landscape appears vulnerable and random: Architects and consultants focus on risk assessment and security through design, *Architectural Record*, March 2002 http://archrecord.construction.com/CONTEduc/ARTICLES/03_02_1.asp

Kowalski, Wladyslaw Jan, P.E., Ph.D., September 26, 2002, *Immune Building Systems Technology*, McGraw-Hill Professional, ISBN: 0-07-140246-2 <http://www.amazon.com/exec/obidos/tg/stores/detail/-/books/0071402462/002-5179887-1245633#product-details>

Nadel, Barbara A, March 1998, Designing for Security, *Architectural Record*, March 1998 http://www.archrecord.com/CONTEduc/ARTICLES/3_98_1.asp

Owen, David D. and R.S.Means Engineering Staff, *Building Security: Strategies and Costs*, Construction Publishers & Consultants, ISBN: 0-87629-698-3, 2003.

Pearson, Robert, September 1997, *Security through Environmental Design, Security and Technology Design*, Security Technology and Design Magazine Reprint Services, Jim Benesh, Phone: (800) 547-7377 x324, FAX: (920) 568-2244, E-MAIL: jim.benesh@cygnuspub.com

Rochon, Donald M., June 1998, *Architectural Design for Security, Security and Technology Design*, Security Technology and Design Magazine Reprint Services, Jim Benesh, Phone: (800) 547-7377 x324, FAX: (920) 568-2244, E-MAIL: jim.benesh@cygnuspub.com

Security Magazine [on-line magazine]
<http://www.securitymagazine.com>

Security Solutions Online: Access Control and Security Systems
[on-line magazine] <http://industryclick.com/magazine.asp?magazineid=119&siteid=24>

Security Technology and Design [on-line and print magazine]
<http://www.st-and-d.com>

Sidell, Frederick R., et al, 1998, *Jane's Chem-Bio Handbook*, Jane's Information Group, Alexandria, Virginia, ISBN 0-7106 2568-5
http://www.janes.com/company/catalog/chem_bio_hand.shtml

Smith, Keith, November 2000, *Environmental Hazards: Assessing Risk and Reducing Disaster*, Routledge, New York, New York, ISBN 0415224632
<http://www.routledge-ny.com/books.cfm?isbn=0415224632>