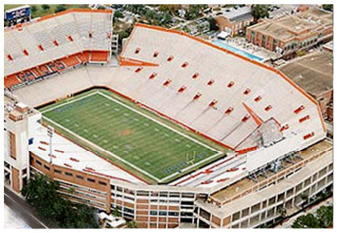
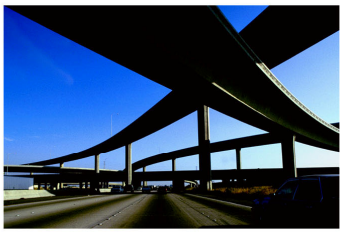
Terrorism Protection Manual

Florida Department of Law Enforcement

FDLE
Florida Department of Law Enforcement
SAIC Team



SAIC
An Employee-Owned Company

The views expressed or facts presented are not necessarily endorsed by FDLE and SAIC. They accept no responsibility for any error or omissions contained in any of the information provided. Nor are they liable for any loss or damage arising from or in connection with the information contained in this manual. It is the responsibility of the user to evaluate the content and usefulness of the information. Reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism.

Acknowledgements

Science Applications International Corporation (SAIC), Integrated Security Strategies Division, in collaboration with the Florida Department of Law Enforcement (FDLE), Office of Domestic Security, developed this Manual to improve the safety and security of the citizens and visitors of Florida. A team of security, law enforcement, and engineering experts with over 300 years of experience researched, designed, and developed this document and a Protective Measures Database towards that end. Key contributors from FDLE were Steve Lauer, Steve Williams, and Stacy Lehman. Key project managers and developers from SAIC were Joseph Hebert, Timothy West, Phil Henning, and Anna Langen.

Contact Information

Florida Department of Law Enforcement Office of Domestic Security

Call Us: 1-850-410-7000
E-mail Us: info@fdle.state.fl.us
Write Us: FDLE
P.O. Box 1489
Tallahassee, FL 32302-1489
Visit Us: FDLE
2331 Phillips Road
Tallahassee, FL 32308
Our Web Site: http://www.fdle.state.fl.us/

Publishing Information

SAIC, Strategies Group, Integrated Security Strategies Division, researched, designed, developed, and published this Manual and the accompanying Protective Measures Database for the FDLE. Questions regarding methodologies or technical information can be referred to:

Integrated Security Strategies Division
SAIC
1710 SAIC Drive, MS: 3-3-8
McLean, VA 22102
(703) 676-5553
www.saic.com

February 28, 2003

Table of Contents

INTRODUCTION

Foreword

On September 11, 2001, the United States was the victim of a horrific series of attacks in New York, Pennsylvania, and Virginia and reached a turning point in its history. Though the enemy assaults on our country occurred a thousand miles from Florida, we would soon learn that this state was not unaffected by the terrorists. Floridians were stunned to learn that 13 of the 19 attackers had lived in, transited through, or trained for their deadly missions in Florida in the months and years prior to the attacks. Floridians would quickly experience terror of a different kind in their state—bioterrorism in the form of anthrax.

In the early fall of 2001, government leaders at every level in the state of Florida had to reevaluate their priorities and plans. The most fundamental and crucial responsibility of elected and appointed leaders—protecting the lives of our people from a ruthless enemy—had been brought out in stark, graphic detail.

Florida's response was swift and certain. Immediately following the attacks, Governor Jeb Bush issued Executive Order #01-262, declaring a state of emergency. The state's Emergency Operations Center was activated, security was heightened at key public and private facilities, and 24-hour intelligence and investigative efforts began.

Days later a second order was issued, this one directing the Florida Department of Law Enforcement (FDLE) and the Division of Emergency Management to jointly conduct a comprehensive assessment of Florida's capability to prevent, mitigate, and respond to a terrorist attack. Within the week, several hundred subject matter experts converged in Tallahassee to work around the clock in four workgroups based on the state's existing emergency support functions: Emergency Services, Human Services, Critical Infrastructure, and Public Information and Awareness. The assessment, which was submitted to the governor within the prescribed 10-day turnaround, resulted in 26 key recommendations and would serve as the foundation for the state's original domestic security strategy.

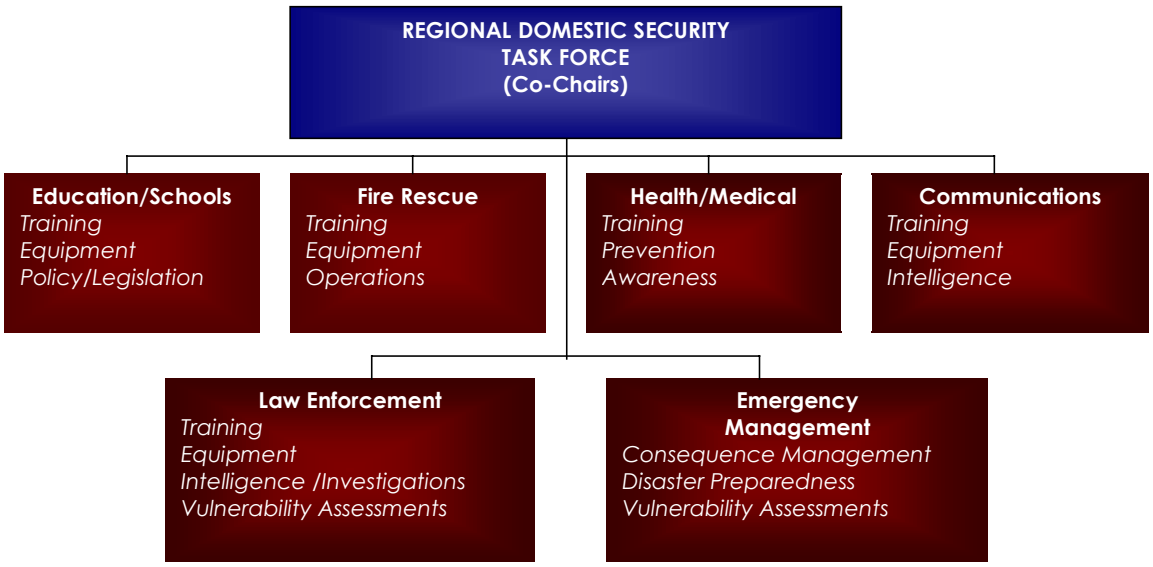
Creation of the RDSTFs

On October 11, 2001, the governor issued Executive Order #01-300, directing specific preparedness actions by state agencies, including the creation of seven Regional Domestic Security Task Forces (RDSTF). Chaired by a local sheriff and FDLE Regional Director, and including more than 100 full-time members statewide, these task forces represent the foundation of the state's ability to prevent, and, if necessary, respond to acts of terrorism.

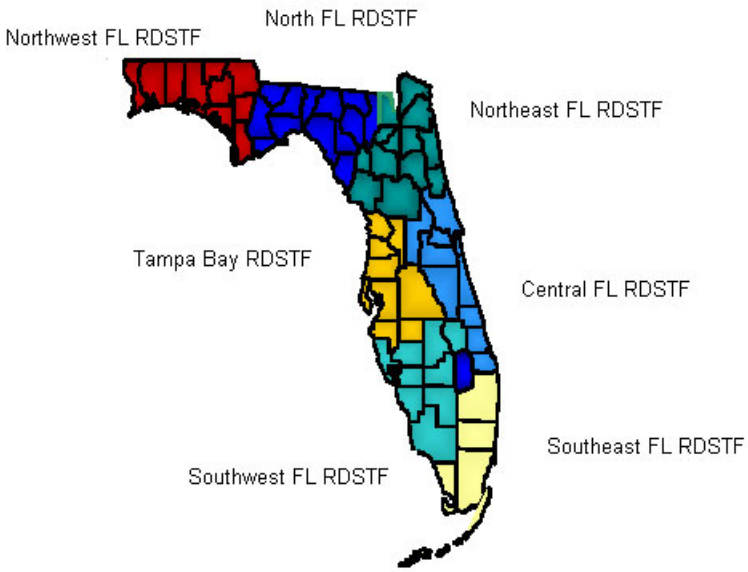
Task force membership includes first responders from the disciplines of fire and rescue, emergency management, and public health and hospitals, as well as law enforcement. In addition, the task forces include partnerships with education/schools and business and private industry, with an additional focus on the requirements for interoperable communications across all disciplines and agencies in the event of an incident. County, state, federal, and local agencies are represented, and committees fulfill the functions of a regional oversight body.

Based on a standard organization template in each region, the RDSTFs serve as the model for delivery of Florida's Domestic Security Strategy. They are unique in that they integrate all of the state's public safety fields; this is the first time these disciplines have gathered in one dedicated, long-term group or on such a massive scale. Furthermore, the RDSTFs are designed to support the locally impacted community; they are a force multiplier for local agencies and work in conjunction with emergency management professionals. One of the benefits of this multidisciplinary approach is that task force members from different fields and agencies have an opportunity to understand one another's capabilities, procedures, and requirements—an invaluable learning tool that becomes crucial when decisions must be made in an emergency. In November 2001, a Domestic Security Oversight Board was created to ensure statewide operational consistency among the RDSTFs.

During the November 2001 Special Session, the legislature established the task forces in law and formally designated FDLE, in conjunction with the Division of Emergency Management, to coordinate statewide domestic security preparedness and response efforts. Legislation also provided for the appointment of a Chief of Domestic Security Initiatives within FDLE. The Chief of Florida Domestic Security Initiatives is charged with coordinating the efforts in the ongoing assessment of Florida's vulnerability to, and ability to detect, prevent, and respond to acts of terrorism, and to prepare recommendations for the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.



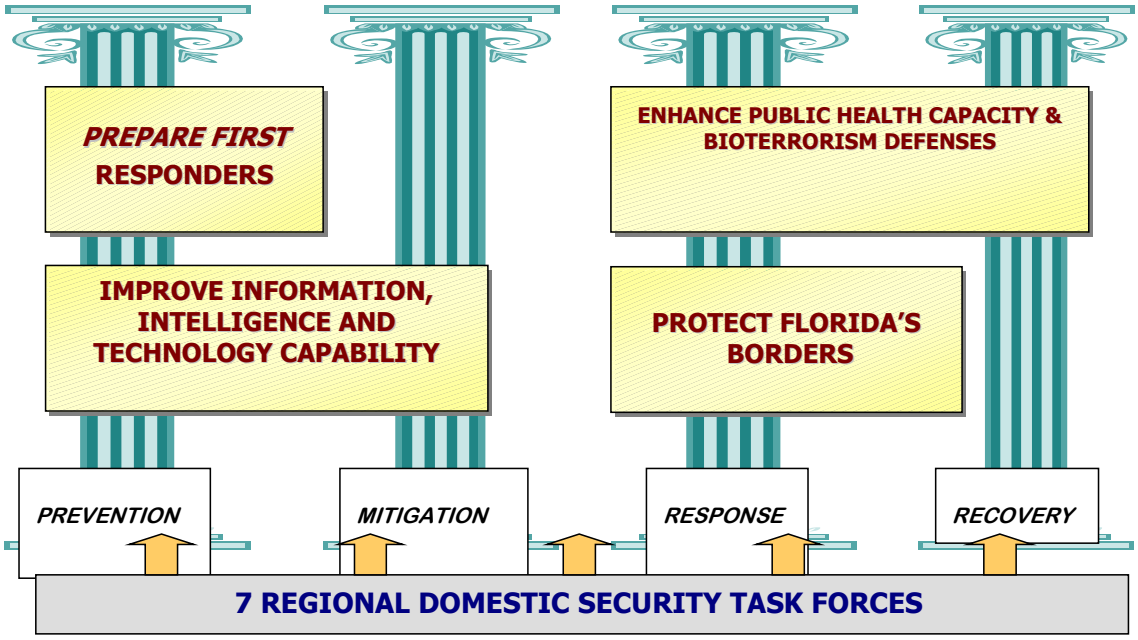
The state map shows the seven RDSTFs.



Florida's Comprehensive Counterterrorism Strategy

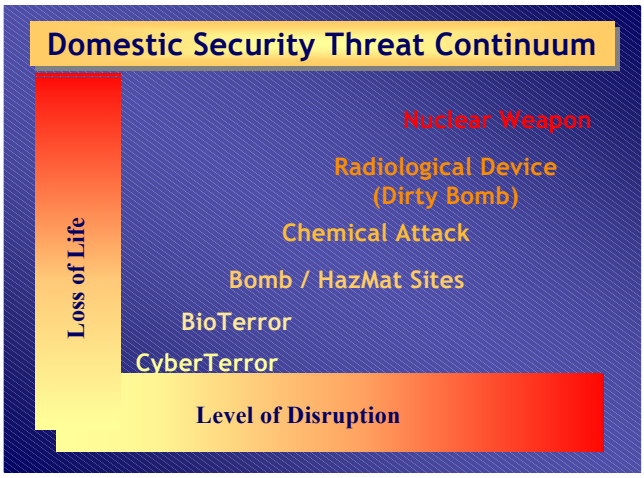
Formally released in October 2001, Florida's strategy was the first comprehensive counterterrorism strategy to be published and the first submitted to Governor Tom Ridge upon his appointment as the Homeland Security Advisor to President Bush. Based on recommendations from the statewide assessment, the Florida strategy defines the requirements needed to bring Florida into a greater state of readiness in the post-September 11, 2001, world.

The strategy is organized around four objectives that serve as the framework for the state's plans and goals, and its efforts at prevention of, response to, mitigation of, and recovery from terrorism aimed at the people of Florida.



During each phase of planning and implementation of this comprehensive strategy, Florida has adhered to seven guiding principles:

- Develop and provide for a uniform level of capability statewide
- Use a Regional Delivery Model
- Maximize the integration of the effort locally
- Recognize unique concerns and identify unique solutions
- Maximize the use of federal funds
- Avoid duplication of federal efforts
- Maximize public awareness



Now and the Future

After development of the strategy, many of the most urgent initial strategy recommendations were quickly implemented. Progress can be attributed to several factors, including the collaboration and cooperation of the individuals and agencies involved; the continued commitment to translate ideas into action; and the support, in terms of resources and the passage of key substantive legislation, of Florida's governor and legislature. One of the many objectives of Florida's strategy was to conduct vulnerability assessments of publicly owned and leased buildings, as well as critical infrastructure, with recommendations for security "best practices." The term **critical** in this context refers to **the likelihood that our enemies may target a facility and that a successful attack will have a significant effect in either loss or disruption of life.**

Because of the large number of sites defined by the term *buildings and facilities owned or leased by state agencies or local governments*, and the relatively short time frame in which to accomplish the assessments, a means to identify and prioritize the most critical sites was developed and implemented.

Scope of Project

FDLE developed this Terrorism Protection Manual (TPM) and the accompanying database to accomplish the following tasks:

- Review the nature and types of public buildings in Florida and the current security best practices for these sites by category (e.g., stadium, courthouse, water treatment facility, administrative building, and others). From this review, develop security best practices of publicly owned and/or leased buildings and make recommendations to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House for the application by site category of recommended security best practices for buildings, sites, and facilities owned or leased by state agencies or local governments.
- Provide a list of best practices for security measures of public and private entities for infrastructure categories identified by a combination of federal directives, such as Presidential Decision Directive 63 (PDD-63), the new National Homeland Security Strategy, and, using the newly created Counter-Terrorism Intelligence Center, Florida's own analysis of additional infrastructure categories, such as schools and entertainment venues.

Intent

It is the intent of this Manual to provide a basis for decisions by local governments, state agencies, and private entities to conduct, at minimum, a self-assessment of risk, and, given a known national threat level, to determine measures recommended for the protection of facilities.

Further, it is recommended that any agency, when needed, be able to call upon the RDSTF for advice and assistance in matters of prevention and response to a terrorist attack. To that end, the following Web site is provided: http://www.fdle.state.fl.us/

This Manual provides a basis for the assessment of risk and provides guidance but not mandates. Each agency or entity using this Manual does so on its own initiative, accepting the risks associated with decisions made or not made on the basis of any recommended measure. There are no absolutes and no guarantees regarding the possible effects of a terrorist attack. While this Manual is comprehensive across a broad range of conditions, it is not intended to be exhaustive or to provide final recommendations that will absolutely prevent or deter a terrorist attack on any individual site. The intent and scope of the effort are part of a unified Florida Domestic Security Strategy—a strategy that is broad in scope and the most comprehensive in the nation. This Manual is a valuable addition to that strategy and one that will be uniquely useful.

TPM Overview

The Manual is divided into five parts, which are explained briefly below.

- The ***Introduction*** provides information on the three facility types (public, private, and special venues) as well as an explanation of the Protective Measures Database, which is on the accompanying CD.
- ***Part I: Basics*** presents key security issues and principles and information on terrorism and security training concepts. Part I provides the foundation and necessary information for the design, development, and implementation of security programs. It offers information and materials that can be used for security training. A sample lesson plan is included to aid in the development of an awareness and education program on antiterrorism for employees.
  - *Chapter 1, Principles* explains security principles for facility managers and those new to the security field. This chapter explains differences in security disciplines, "layered security," and the difference between security policies and security procedures. Additionally, the chapter provides brief overviews of access control, surveillance, and intrusion detection systems, and engineering solutions. An exhibit provides a list of general security measures for managers to consider for facility protection. An additional exhibit is provided to enable managers to better understand how to apply security technologies and engineering.
  - *Chapter 2, Terrorism* presents a brief historical evolution of terrorism and explains the organizational structure and types of groups threatening the United States. It explains the methods and tactics commonly used and provides a recommendation to promote citizen awareness and involvement to counter future attacks.
  - *Chapter 3, Training* gives users a succinct explanation of why training "buy in" is important and explains the necessity of analyzing, designing, developing, implementing, and evaluating training programs. The chapter also provides a list of solutions to training problems, a sample antiterrorism lesson plan (with a student handout), and a sample security education and security adviser program.

- ***Part II: Management*** helps users understand roles and responsibilities and policies. It provides information on the diverse nature of terrorist threats and overarching management tools to mitigate those threats.
  - *Chapter 1, Roles and Responsibilities* provides recommended lists of actions that managers, supervisors, employees, building managers, and even visitors can take to enhance facility security.
  - *Chapter 2, Security Policies* explains why security policies are important, recommends a security hierarchy to manage security programs, and explains the charter of security councils and threat working groups.
  - *Chapter 3, Risk Management* defines terms and provides a six-step process for risk management. This chapter highlights the need for managers to weigh the application of security measures against risk levels.
  - *Chapter 4, Threat Levels* briefly explains the Homeland Security Advisory System and how it relates to Florida.
  - *Chapter 5, Threat Planning* provides several hypothetical scenarios, explains anti-terrorism planning, and provides a planning guide.

- ***Part III: Assessments*** is a core component of this Manual. Before beginning an assessment, an inventory of current facilities and resources must be completed. Those responsible for security must understand and be able to apply one of the three assessment tools presented. Once a tool is chosen and the assessment completed, the resulting information is used to populate the database (the facility protective measures matrices). When the matrices are completed, the user will have a list of protective measures for his or her facility type.
  - *Chapter 1, Methodology* defines and explains the vulnerability assessment process, implementation, and team composition.
  - *Chapter 2, FDLE Assessment Tool* gives users a facility security checklist to assess and highlight security features in place. This document should be completed to note security gaps and assist FDLE in better assessing the "health" of the state security program.
  - *Chapter 3, DOJ Assessment Model* offers users a simple vulnerability assessment option. This tool provides a mildly objective rapid assessment of the facility risk level in order to move on to protective measures implementation.
  - *Chapter 4, DoD Assessment Model* provides a fairly objective, more quantifiable facility review and assessment tool. This middle-of-the-road option was derived from the DoD and modified to assist the state of Florida in conducting vulnerability assessments.
  - *Chapter 5, AASHTO Assessment Model* is a comprehensive, empirical vulnerability assessment tool that was developed for the U.S. Department of Transportation and modified to suit the needs of public and private facility managers.

- ***Part IV: Encyclopedia*** explains the best security practices. It also explains items used in the Protective Measures Database matrices. This part is designed for facility managers, the team charged with implementation (security, engineering, maintenance, and human resources, for example), corporate and government policy makers and leaders, and public and private sector financial advisors. The eight chapters in this part contain detailed security information on policies, procedures, technology, and engineering features. This comprehensive encyclopedia also explains the characteristics and applications of numerous security tools.

- ***Part V: Appendix*** provides a glossary and lists of acronyms, references, and Web sites. It contains the protective measures matrices and the Protective Measures Database (on a CD-ROM as an attachment to the Manual).

INTRODUCTION

Chapter 1: How to Use the Manual

The TPM was created to provide state and local governments and the private sector with a method to determine their vulnerabilities and risks on the basis of today's national terrorist threat, and then implement recommended security best practices. This Manual is designed for facility managers, security directors, and others responsible for the security of a facility. The Manual has been organized to allow users to decide which portions are applicable to them.

This Manual was designed for use as part of an integrated system; it is not a stand-alone tool. However, not all sections are dependent on one another. For example, some users may have the core knowledge presented in **Part I: Basics**, and may be able to skip that portion. Or security professionals could use it as an educational tool to gain support from senior management. The following steps will assist in determining which portions are necessary.

Step 1

Determine if the TPM is applicable to the facility. The Manual addresses the following types of facilities:

- **Publicly owned or leased** sites, facilities, structures, and resources such as government office buildings, schools, and courthouses. Information on public facility categories can be found in Chapter 2 of this Introduction.
- **Privately owned or leased** critical infrastructure such as oil refineries or transportation and agricultural facilities. Refer to Chapter 3 of this Introduction for detailed information on the critical infrastructure protection (CIP) initiative and a list of the CIP sectors and functional categories of facilities.
- **Private and publicly owned special venues** such as football stadiums, concert halls, convention centers, and festivals. These special venues are explained in Chapter 4 of this Introduction.

Step 2

Identify the current threat level using the Department of Homeland Security Threat Advisory System. The TPM allows for the use of threat levels higher than the current level to anticipate increased security measures.

Step 3

Determine facility risk using one of the three assessment tools located in **Part III: Assessments**. Users who have already determined a risk level can proceed directly to Step 5.

Step 4

An individual with little or no experience in facility security may wish to read other portions of the TPM prior to conducting a risk assessment. To determine your level of expertise and identify additional Manual resources, see Exhibit 1 to this chapter.

Step 5

Now that you have established the applicability of the Manual to your facility, and identified the appropriate national threat level and risk level, you should proceed to Chapter 5, Protective Measures Database, to review the recommended security best practices. For detailed explanations of these best practices refer to **Part IV: Encyclopedia**.

If you need additional assistance in using the TPM, contact your RDSTF or visit www.fdle.state.fl.us.

Exhibit 1 to Chapter 1

Levels of Expertise and Manual Resources

One of the most important initial steps in using the TPM is determining what level of security expertise is organic to your agency or department. This depends on whether your organization has a professional, highly trained and certified security director or whether your security programs are managed by a self-taught facility manager. Perhaps you are a small organization or are simply under-staffed and rely on a relatively inexperienced person whose security role is an additional duty. Many agencies will not have a full-time or experienced security manager or director; however, someone in the organization may be assigned security responsibilities on a full- or part-time basis. These personnel will likely be:

Security Director. For the purpose of our recommendation, we recognize a security director as being a full-time agency, department, or company official who is charged with at least one of the following responsibilities:

- Conducts loss prevention or asset protection program reviews
- Manages a security officer force
- Manages a visitor and employee identification system
- Maintains in-depth knowledge of the physical security protection system of the facility, site, or building
- Assists in conceptualizing, designing, and using a security protection system when gaps have been identified or there is a need for upgrade or improvement.

Full-time facility, site, or building manager (especially in the mechanical or craft trades). Although primarily concerned with the mechanical operation of the building (maintenance, utilities, office relocation, and heating, ventilation, and air conditioning [HVAC]), the facility or building manager will also have knowledge of and responsibility for the general security of the building, site, or facility.

Part-time facility, site, or building manager or additional duty person. This category may include a non-facility manager. Although they may be familiar with the general operation of the building, they rely mostly on contract (outside) support or call on your agency, department, or company's maintenance section for repairs and upgrades. They know of the presence of security systems, but do not have detailed knowledge of or maintain such systems. An example would be a person who is assigned to human resources or administrative support services who may not be familiar with or has no responsibility for managing security systems or upgrades. The non-facility manager may be someone with a general responsibility for a site, building, or facility who relies totally on outside or external assistance in all areas of maintenance or upgrades to the facilities. The non-facility manager might even be the owner or manager of a business (hospitality, retail, or private education facility, for example). Finally, the non-facility manager may have a custodial staff that is responsible only for facility cleanliness and appearance and minor maintenance (public schools and general administrative offices).

Matching Your Level of Security Expertise to the Manual

Security Director or Manager. If you are a full-time security director or manager and you fall into one of the experience level categories listed above, we have designed this manual to allow you to select portions of the TPM based on your qualifications and experience. You will not need to review the basic concepts of security, determining the threat, and reviewing the purpose of a perimeter security system or closed circuit television (CCTV) installation.

You may have already completed a vulnerability assessment, with the results accepted by your agency, department, or company management. You have the **discretion** to decide, based on your level of experience and using our general guidelines, what sections of the TPM you will need to carefully review and use. Obviously you are welcome to review the entire TPM, but to save you time and effort, as a minimum **we recommend that you review and use the following chapters**.

Security Director Steps for Using the TPM

- If you have in-depth security knowledge and know the risk level for your facility, site, or building, go directly to the Protective Measures Database, explained in Chapter 5 (Introduction). Then enter your data and receive suggested methods for high-, medium-, and low-risk facilities in threat levels Yellow, Orange, and Red. The remaining steps (below) are considered optional for the fully qualified security director or manager.
- *Part II, Management, Chapter 5 (Threat Planning)*—Review, **unless** you already have a threat planning document.
- *Part III, Assessments*—Review **if you have not** conducted a facility assessment or want to reconfirm your risk category as low, medium, or high.
  - *Chapters 3, 4, and 5*. Use this section to select the assessment methodology that best suits your needs. You can also use this section if you require background data to develop and submit a capital improvement budget request for security upgrades. For the highest level of empirical data, see Chapter 5, American Association of State Highway and Transportation Officials (AASHTO) Assessment Model. This is an in-depth vulnerability assessment tool that gives you quantifiable data to present to your managers for implementing security measures and programs.
- *Part IV, Encyclopedia*—Review if you would like a refresher on all aspects of security.

Full-time facility, site, or building manager classification. Because you may also function as the security manager, you may need to review more portions of the TPM than a full-time or assigned security official. Based on your qualifications and experience, you will probably not need to review the basic concepts of security, determining the threat, and reviewing the purpose of a perimeter security system or CCTV installation. You have the discretion to decide, based on your level of experience and using our general guidelines, what sections of the TPM you will need to review and use. Obviously you are welcome to review the entire TPM, but to save you time and effort, as a minimum **we recommend that you review and use the following chapters**.

Full-Time Facility, Site, or Building Manager Steps for Using the TPM

- *Part I Basics*
  - *Chapter 1, Security Principles*
  - *Chapter 2, Terrorism*
- *Part II Management*
  - *Chapter 1, Roles and Responsibilities*
  - *Chapter 2, Security Policies*
  - *Chapter 3, Risk Management*
  - *Chapter 4, Threat Levels*
  - *Chapter 5, Threat Planning*
- *Part III Assessments*
  - *Chapter 1, Introduction.* To determine the risk level of your facility (high, medium, or low), select one of the three assessment tools (Department of Defense [DoD], Department of Justice [DOJ], or AASHTO). The general guidelines for selecting an assessment tool are as follows:
    - If you are in a low-risk facility, use the DOJ assessment tool
    - For medium- to high-risk facilities, use the more comprehensive DoD assessment tool
    - For obvious high-risk facilities or if you need extensive empirical data, use the AASHTO assessment tool
- *Part IV Encyclopedia.* Based on your "comfort level" you should review all chapters of Part IV, but skip those that obviously do not apply to your facility. If you manage a general administrative building, you can skip Chapter 8, Special Venues.
- Once you know the risk level for your facility, site, or building, go to the Protective Measures Database, which is explained in Chapter 5 (Introduction). Gather and then enter your data and obtain suggested methods for high-, medium-, and low-risk facilities in threat levels Yellow, Orange, and Red.
- Additional information and explanations can be found in the Appendix section of this Manual, including a glossary and Web sites.

Part-time facility, site, or building manager or additional duty person or non-facility manager. You will likely require the assistance of the entire TPM to conduct your facility risk assessment if you do not have daily responsibility for, or knowledge of, the "mechanical" operation and maintenance of the building, site, or facility. Although you have the discretion to decide, based on your level of experience and using our general guidelines, what sections of the TPM you will need to carefully review and use, you should read Chapter 1 (Introduction) to determine if the TPM is applicable to your situation. **We recommend that you review and use the following chapters**.

Part-Time Manager, Additional Duty Person, or Non-Facility Manager Steps for Using the TPM

- Introduction. Read all chapters to determine if the TPM applies to your agency, department, or company.
- *Part I Basics*
  - *Chapter 1, Security Principles*
  - *Chapter 2, Terrorism*
- *Part II Management*
  - *Chapter 1, Roles and Responsibilities*
  - *Chapter 2, Security Policies*
  - *Chapter 3, Risk Management*
  - *Chapter 4, Threat Levels*
  - *Chapter 5, Threat Planning*
- *Part III Assessments*
  - *Chapter 1, Introduction.* To determine the risk level of your facility, select one of the three assessment tools. The general guidelines for selecting an assessment tool are:
    - For a low-risk facility, use the DOJ assessment tool
    - For medium- to high-risk facilities, use the more comprehensive DoD assessment tool
    - For obvious high-risk facilities or if you will need an extensive empirical scoring process, use the AASHTO assessment tool
- *Part IV Encyclopedia.* Because you have responsibility as either an additional or secondary duty, or you own the facility, you will probably need to review all sections of Part IV to obtain a basic understanding of all areas of security. If you manage a general administrative building, you can skip Chapter 8, Special Venues.
- Once you know the risk level for your facility, site, or building, go to the Protective Measures Database, which is fully explained in Chapter 5 (Introduction). Gather and then enter your data and obtain suggested methods for high-, medium-, and low-risk facilities in threat levels Yellow, Orange, and Red.
- Additional information and explanations can be found in the Appendix section of this Manual, including a glossary and Web sites.

Additional Recommendations

Whether you are a security director or manager, a full-time facility manager in the trades industry, a full-time non-trades-industry facility manager, a part-time (additional duty) manager, or a facility owner, once you have determined your security requirements, go back to the TPM and review the following:

- Part I, Basics, Chapter 3, Training. This section is valuable if you have determined that your work force needs special training in antiterrorism or your agency, department, or company needs an antiterrorism training program.
- Part II, Management, Chapter 5, Exhibit 1. We recommend that you develop an anti-terrorism plan once you have completed your vulnerability assessment and obtained a list of security measures that will be required.
- Part V, Appendix. For additional information and other sources, you are encouraged to review all parts of the Appendix.

INTRODUCTION

Chapter 2: Public Facilities

Facility managers, security directors, and those responsible for the security of Florida's **publicly owned or leased** sites, facilities, structures, and resources should determine which category of the following public facilities most closely represents their facility type. Use this category when conducting the vulnerability self-assessment and when using the protective measures database.

State, City, County, Municipal Buildings, Sites, and Facilities	
Government Administration	
✹ Administration (with public access) ✹ Administration (without general public access) ✹ IT facilities (does not include an examination of cyber security) ✹ State capitol complex	✹ State agency administration buildings (outside Tallahassee) ✹ Revenue collection facilities ✹ Human services facilities
Government Public Safety	
✹ Fire and rescue stations and training facilities ✹ Police/sheriff/state law enforcement agency stations and training facilities	✹ Combined public safety buildings ✹ Forensic and criminology laboratories
Government Justice Facilities	
✹ Courtrooms and courthouses ✹ Probation/parole offices	✹ Juvenile justice facilities
Government Public Works Facilities	
✹ Shops ✹ Corporation yards ✹ Bulk and HAZMAT storage ✹ Sanitation lift stations	✹ Sanitation processing (solid and water waste stations) ✹ Drinking water treatment and reservoir sites ✹ Wastewater treatment sites/landfills
Government Energy Facilities	
✹ Power production and transmission	
Government Education Facilities	
✹ Elementary ✹ Middle/junior ✹ High schools ✹ Universities, community colleges, vo-techs — Annexes — Research facilities ➤ Cyclotron ➤ Nuclear reactor ➤ Nuclear medicine ➤ Biological and genetic ➤ Agricultural/animal	— Dormitories/housing facilities — Auditoriums and mixed-use performance centers — Gymnasiums/other sports facilities — Classrooms/libraries/administration facilities
Government Transportation Facilities	
✹ Bus transit stations and storage areas ✹ Light rail transit stations and storage areas ✹ Heavy rail transit stations (Amtrak) ✹ Repair facilities and shops	✹ State/municipal motor pools/vehicle storage and staging areas ✹ Student bus transportation stations and storage areas ✹ General aviation airfields ✹ Ferries

State, City, County, Municipal Buildings, Sites, and Facilities	
✹ Transfer points	✹ State aviation facilities
Government Recreational Facilities	
✹ Parks — Campgrounds/day-only facilities — Historical sites ➤ Homes ➤ Forts ➤ Monuments	
Government Health Facilities	
✹ Hospitals ✹ Trauma centers ✹ Mental health centers ✹ Community health centers ✹ Research centers	✹ Laboratories — Health — Agriculture/animal/food safety — Environmental protection
Government Public Gathering Venues	
✹ Interstate welcome centers ✹ Official tourism offices	✹ Convention centers
Government Emergency Management Facilities	
✹ Emergency operations centers	✹ Microwave/communications nodes

Chapter 2 provided the official list of public facilities that support the citizens of and visitors to Florida. Select your type of facility from this list before proceeding to the self-assessment.

INTRODUCTION

Chapter 3: Critical Infrastructure Protection (Private Facilities)

The following statement comes from the White House Office of Critical Information Assurance: "The United States' critical infrastructures are truly the foundation of our economy, national security and certainly essential to our way of life as Americans. Our economy, government, and security, at home and abroad, now depend mainly upon technology systems. As a result of this reliance, our critical infrastructures become more and more reliant on a vast array of interconnected information systems. Consequently, America faces ever-changing challenges in terms of protecting these vital national resources."

The government has made the fight against terrorism a top national security objective. It has deepened its cooperation with friends and allies abroad, strengthened law enforcement's counterterrorism tools, and improved security on airplanes and at airports. These efforts have paid off—terrorist attacks have been foiled and terrorists apprehended.

Yet America's military superiority means that potential enemies—whether nations or terrorist groups—are more likely to resort to terrorist attacks than conventional military assault. Moreover, easier access to sophisticated technology means that the destructive power of terrorists is greater than ever. Adversaries may use unconventional tools, such as weapons of mass destruction, to target our cities and disrupt government operations. They may try to attack the economy and critical infrastructure using advanced technologies.

Federal Directives

To meet these challenges, Presidential Decision Directive 62 (PDD-62) created a new, more systematic approach to fighting the terrorist threat in the 21st century. It reinforced the mission of the many U.S. agencies charged with defeating terrorism. It also codified and clarified their activities in the wide range of U.S. counterterrorism programs, from apprehension and prosecution of terrorists to increasing transportation security, enhancing response capabilities, and protecting the computer-based systems that are at the heart of America's economy. PDD-62 was designed to ensure that the threat of terrorism in the 21st century is addressed as rigorously as other military threats in the 20th century.

To achieve this new level of integration in the fight against terror, PDD-62 established the Office of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. The National Coordinator oversees a wide variety of polices and programs, in such areas as counterterrorism, protection of critical infrastructure, and preparedness and consequence management for weapons of mass destruction. The National Coordinator works within the National Security Council, reports to the President through the assistant to the President for National Security Affairs, and produces an annual Security Preparedness Report for the President. The National Coordinator also provides advice regarding budgets for counterterror programs and leads the development of guidelines for crisis management.

Presidential Decision Directive 63 (PDD-63), Executive Order on Critical Infrastructure Protection (CIP), was established to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

PDD-63 Policy:

"The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of

continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.

It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations."

PDD-63 was issued to achieve and maintain the capability to protect the nation's critical infrastructure from intentional acts that would significantly diminish the abilities of:

- The federal government to perform essential national security missions and to ensure the health and safety of the general public
- State and local governments to maintain order and deliver minimum essential public services
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

To achieve these ends, PDD-63 articulates a strategy of:

- Creating a public-private partnership to address information technology security
- Raising awareness of the importance of cyber security in the government and in the private sector
- Stimulating market forces to increase the demand for cyber security and to create standards or best practices
- Funding or facilitating research into new information technology systems with improved security inherent in their design
- Working with higher educational facilities to increase the number of students specializing in cyber security
- Helping to prevent, mitigate, or respond to major cyber attacks by building an information-sharing system among government agencies, among corporations, and between government and industry.

The federal government established PDD-63 as a national program, but the policy architects realized that the program required a collaborative effort by public and private entities in order to succeed. When the President's Commission on Critical Infrastructure Protection conducted its research in 1997, most of the critical infrastructures were found to be privately owned and operated and many owners and operators were business competitors. Protecting CIP is essential to the continued success of this business group and requires shared responsibility and partnership between private owners/operators and government entities.

The CIP Commission stated that failures of infrastructure can harm business operations by affecting their bottom lines, eroding consumer confidence, and disrupting operations. Some CIP nodes, if not secured properly, can cause serious problems and lead to major disruptions throughout the economy.

Infrastructure protection cannot be static. In today's high-speed business world, core business processes and technologies are constantly changing in order to create competitive

advantages and efficiency. Consequently, ensuring the safety of our infrastructure requires ongoing concern, recognition, and application of security protective measures in the business decisions of managers, starting with the highest levels of management.

The PDD-63 mandate leaned heavily towards hardening the accessibility to computer networks and enhancing cyber security. This FDLE TPM project, however, addresses the physical protection of Florida's CIP facilities rather than cyber security.

The critical infrastructure sectors as reported in the National Strategy for Homeland Security, the President's approved strategy for homeland security (published in July 2002 by the Office of Homeland Security) are:

- Agriculture
- Food and water
- Public health
- Emergency services
- Government
- Defense industrial base
- Information and telecommunications
- Energy
- Transportation
- Banking and finance
- Postal and shipping

Florida Criteria for Designating a Critical Asset

The FDLE Office of Statewide Intelligence in its document *Intelligence Assessment: Critical Infrastructure* issued its definition of the critical infrastructure for the state of Florida.

For the purposes of this Manual, critical infrastructure is defined as *"all systems and assets, whether physical or virtual so vital, to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national health or safety, or any combination of those matters. Critical infrastructure includes telecommunications, financial, transportation, energy, public utilities services (i.e., water and wastewater), commerce, and education services."*

The federal criterion for designating an asset as critical was modified to create lists significant to operations and functions applicable to Florida. The following lists consist of entities unique but not exclusive to Florida.

1. ***Telecommunications***. The networks and systems that support the transmission and exchange of electronic communications among and between end users. A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support: the processing, storage, and transmission of data into information and information into knowledge; and the data and the information itself.
   - FCIC/Tallahassee FDLE building
   - Critical infrastructure plan
   - Phone relay system servicing 10,000 plus
   - Cable television servicing 10,000 plus
   - Commercial television/radio broadcasting facilities
   - Cell phone relay towers
2. ***Electrical Power Systems***. The generation stations and transmission and distribution networks that create and supply electricity to end users so they achieve and maintain nominal functionality, including the transportation and storage of fuel essential to these systems.

- Systems supplying power to 10,000 plus
- Power grid sites
- Systems supplying power to large metropolitan areas
- Power systems supplying power to food storage facilities
- Electrical power for nuclear plants

3. ***Gas and Oil Production, Storage, and Transportation***. The holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels; the refining and processing facilities for those fuels; and the pipelines, ships, trucks, and rail systems that transport these commodities from their sources to systems that are dependent on gas and oil in one of their useful forms.

- Gas facilities servicing 10,000 plus
- Oil tanks, that, if exposed, will cause environmental disaster
- Pipelines/natural gas transmission lines
- Crude oil refineries

4. ***Banking/Finance***. The retail and commercial operations, investment institutions, exchange boards, trading houses and reserve systems, and associated operational organizations, government operations, and support entities that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.

- Banks housing mainframes for outlying branches

5. ***Transportation***. The aviation, rail, highway, and aquatic vehicles, conduits, and support systems by which people and goods are moved from a port of origin to a destination point in order to support and complete matters of commerce, government operations, and personal affairs.

- International airports
- Regional airports
- Ports providing for both tourism and commerce
- Critical railroad junctions (content of trains, if exposed, would cause loss of life and/or environmental damage)
- Major loading areas for Florida's agricultural industry

6. ***Water Supply Systems***. The sources of water, reservoirs, and holding facilities, aqueducts and other water transport systems, filtration and cleaning systems, pipelines, cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with wastewater and firefighting.

- Water supplies servicing major metropolitan areas (more than 10,000)
- Water supplies servicing key agricultural sites
- Main aquifers
- Water holding tanks

7. ***Emergency Services***. The medical, police, and fire and rescue systems and personnel that are called upon when an individual or community is involved in a public health or safety incident where speed and efficiency are necessary. *(Note: Medical facilities and private ambulance services and some privately formed EMS and fire departments will qualify as private infrastructure.)*

- Major metropolitan:
  - Hospitals
  - Police departments
  - Fire departments
  - Other rescue services/systems

- State law enforcement agencies serving as headquarters
- Law enforcement agencies serving large metropolitan areas
- Emergency operations centers (state, county, city)

8. ***Continuity of Government Services***. Those operations and services of governments at federal, state and local levels critical to the functioning of the nation's systems, i.e. public health, safety and welfare. *(Note: These are generally government owned facilities and will not be part of the private infrastructure unless leased by a state or local government.)*

- Capitol building
- Governor's mansion
- Headquarters for state agencies whose disruption would cripple the entire agency's operations
- State law enforcement (see Emergency Services)
- Correctional facilities (federal, state, local)

9. ***Commerce***. Those operations, industries and assets that directly impact the state of Florida economy. These include, but are not limited to, assets in the tourism, agriculture, and commerce transportation industries. A failure in one or more of these assets will result in a grave loss of revenue to Florida and impair the ability of government to function properly.

- Tourist attractions
- Agriculture
- Recreational transportation

10. ***Educational Facilities***. Facilities that house and educate children and adults. These institutions provide a gathering point for large numbers of people, making them desirable targets for terrorist attacks. *(Note: Publicly owned schools will be the responsibility of the owning state or local government agency that is responsible for the operation of the academic facility.)*

- Major universities and community colleges
- High schools
- Middle schools
- Elementary schools

Florida's 12 CIP Sectors

As a result of reviewing these lists, the Florida legislature decided that the following 12 CIP sectors best represent and capture the essence of Florida's critical infrastructure:

- Agriculture
- Food and water
- Emergency medicine and hospitals
- Defense industrial base
- Information and communications
- Energy
- Transportation
- Banking and finance
- Postal and shipping
- Education
- Insurance
- Entertainment venues

Within each Florida CIP sector, a number of functional operations were identified which represent the diverse makeup of these vital organizations. These functional operations may

not apply to all CIP sectors. However, for a particular private industry segment there may be an intersecting functional operation somewhere in the industry. However, within the CIP realm, some functional operations were not rated as critical. For example, from a critical infrastructure perspective, a CIP operational sector of production and manufacturing was not identified within the Education CIP sector.

Listed below are the officially designated functional areas from which to select for use by each CIP sector:

- Administration
- Operations
- Communications
- Information/financial
- Production/manufacturing
- Distribution
- Storage/warehousing
- Research/labs
- Retail/operations
- Utilities

The 12 CIP sectors were grouped and scored within the Protective Measures Database, using the CIP functional areas.

Agriculture Sector	
✸ Administration	✸ Distribution
✸ Operations	✸ Storage/Warehousing
✸ Communications	✸ Research
✸ Information/Financial	✸ Utilities
✸ Production/Manufacturing	
Food and Water Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	
Emergency Medicine and Hospitals Sector	
✸ Administration	✸ Information/Financial
✸ Operations	✸ Utilities
✸ Communications	✸ Research
Defense Industrial Base Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	
Information and Communications Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	

Energy Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	
Transportation Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	
Banking and Finance Sector	
✸ Administration	✸ Information/Financial
✸ Operations	✸ Utilities
✸ Communications	
Postal and Shipping Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	
Education Sector	
✸ Administration	✸ Production
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	
Insurance Sector	
✸ Administration	✸ Information/Financial
✸ Operations	✸ Utilities
✸ Communications	
Entertainment Venues Sector	
✸ Administration	✸ Production/Manufacturing
✸ Operations	✸ Distribution
✸ Communications	✸ Storage/Warehousing
✸ Information/Financial	✸ Research
✸ Utilities	

This chapter provides a detailed explanation of every component of the critical infrastructure for the private sector and a list of sites, facilities, and buildings that are recognized by the state as critical facilities. This information will enable companies, agency and department chiefs, and managers to determine if their facility is a critical infrastructure or facility that may require a vulnerability assessment.

INTRODUCTION

Chapter 4: Special Venues

At present threat levels, large gatherings of Americans may be a tempting and potentially "productive" target for terrorists. For the purposes of this Manual, special venues are defined as "events of a specific duration involving a large gathering of people in either a private or public area that may or may not combine public and private security operations." There are three major categories of venues:

- Indoor: Facilities such as civic centers, conference centers, performing arts centers and auditoriums.
- Open: Includes street festivals, fairs, and other activities not confined to a building or stadium/arena type facility.
- Stadium or Arena: Includes facilities such as football stadiums, baseball stadiums, and racetracks.

People assemble every day to view sporting events, art, and music or attend a variety of festivals or political rallies, and it is not likely that this will change. Accordingly, assembly managers and those charged with public safety face significant challenges in protecting citizens from terrorists carrying out attacks against these "soft" targets.

To aid **venue managers** in protecting these public and private events, use the Manual as indicated in the ***Introduction: How to Use the Manual*** section, and refer to ***Part IV, Encyclopedia, Chapter 8, Special Venues.***

INTRODUCTION

Chapter 5: Protective Measures Database

In conjunction with the TPM, a scoring checklist (matrix) was designed that assigns protective measures on a graduated basis from low to medium to high risk. These risks correspond to the Department of Homeland Security Threat Levels of elevated, high, and severe. The state of Florida considers elevated to be the "baseline" threat level.

The database matrix combines three factors—facility category area; risk level (determined by the vulnerability assessment process); and threat level (determined through current intelligence and threat warnings)—with a list of over 300 terrorism protective measures (recommended best practices).

The security best practices were compiled and loaded as protective measures into a Microsoft Access database file. Two versions of the database are provided: one in Access 2000 and one in Access 97. For users who do not have Microsoft Access, the database is also available in a Microsoft Excel spreadsheet. This database is the main terrorism protection implementation tool for facility managers and security directors. It is designed to provide a graduated approach to protecting facilities. This instrument is also useful to managers in designing a financial strategy to correct security deficiencies.

Database Overview

The first factor to be determined is the facility category. The protective measures in the database are organized into three categories of facilities:

- Public facilities
- Private facilities (critical infrastructure)
- Special venues

When all types of facilities are combined, there are 96 categories: 62 public facility categories, 31 private categories, and 3 special venues. Each of the 96 facility categories is contained within the database and falls within one of the three main categories.

The second factor to be determined is risk level. There are three risk levels (high, medium, and low), which will be outlined in **Part III: Assessments.** From the assessment, a risk level will be established. The resulting risk level for the facility is based on a set of objective measurements found in the selected assessment tool.

The third factor is the level of threat: elevated, high, or severe. These three threat levels are contained within the database.

The database contains over 300 protective measures. Each measure describes actions or tools that can be used to mitigate terrorist attacks and contains a recommended action, followed by immediate and long-term measures that managers can take to reduce the effects of or to deter attacks. The protective measures are organized into eight categories and these categories are divided into 45 subcategories. The eight categories are:

1. External Security
2. Internal Building Controls
3. Emergency Services
4. Communications
5. Security Systems
6. Security Design
7. Security Resources
8. Special Venues

These eight categories (and a narrative of each) are also contained in **Part IV: Encyclopedia** and organized as chapters with detailed explanations. In the database, each measure is organized under the applicable subheading in the order in which the activity must take place. For example, within the Building Security Checks subcategory of Chapter 2, Internal Building Controls, managers should write procedures for conducting building checks before implementing random checks.

Matrix Explanations

The protective measures are merely recommendations; they are not to be considered mandates. Variables and site constraints will affect the implementation of these recommended measures. Consequently, users must remain flexible and open-minded and realize that these measures may not apply to their specific facility. For example, a rural water treatment plant will not generally implement the same types of protective measures as a metropolitan area facility.

A "one size fits all" matrix recognizes that there are many unique environments and situations. The matrices attempt to offer as many recommendations as possible and expect users to tailor these recommendations to their situations.

After populating the matrix with the facility type, risk, and threat levels, a document will be produced that contains "X's" in columns on the right side that indicate what protective measures are recommended. On the left side, a "P" or "P/T" indicates whether the measure is considered a "permanent" or "permanent/temporary" recommendation.

Before beginning this implementation phase of terrorism protection measures, it is imperative that the information within the TPM be reviewed and understood. Especially important are the Part I: Basics chapters, as they provide necessary conceptual information to build a meaningful security program. Before initiating the steps in these chapters, it is important to review the Assessment chapters, as they provide the requisite tools and a road map to proceed.

If there are "Security Design" recommendations that are not already in place, please contact the FDLE, Office of Domestic Security, before implementation.

Preparing to Use the Database

Before you begin using the database, read the information in this chapter thoroughly.

Hardware Requirements

Verify that the computer system you will use to view the database meets the hardware requirements listed below:

- IBM PC (or 100% PC-compatible) computer
- Color or monochrome monitor
- CD-ROM disk drive or Internet access
- 10 MB memory
- Windows 3.1 (or higher)
- Microsoft Access or Microsoft Excel (if Access is not available)
- Printer (optional)
- Mouse (optional)

Care and Handling of the CD-ROM

The Protective Measures Database is provided on a single CD-ROM.

- Handle the disk with care
- Never touch the bottom surface of the disk
- Carefully load the disk in the CD drive with the label facing up
- Do not remove the CD while the database program is open (running)
- Data changes cannot be made to the CD; however, data (and the entire database) may be exported and saved to the computer hard drive and then modified
- Store the CD-ROM at room temperature out of direct sunlight

Start-Up

The Protective Measures Database does not currently contain an installation file—that is, you can access the CD-ROM via a file search or by opening Microsoft Access or Excel and then opening the file from the CD-ROM.

Database Details

The Protective Measures Database is the integration of 96 facility categories with risk and threat levels into a relational database. The database includes a query tool that processes a series of user-defined point-and-click queries to establish a range of protective measures options. Prior to using the database tool, the user should review the core elements of the TPM and determine what risk level they are and the range of threats they face.

Main Menu Screen

The chief output from the Protective Measures Database tool is a user-driven list or range of options in response to facility protection recommendations. At the beginning and end of each database session, users encounter a screen identical to the one shown in **figure 1**. This screen launches users into the Protective Measures Database and is used at the end of the session to properly close the database session. For administrators, this screen allows access to manipulate data and tailor measures as necessary.

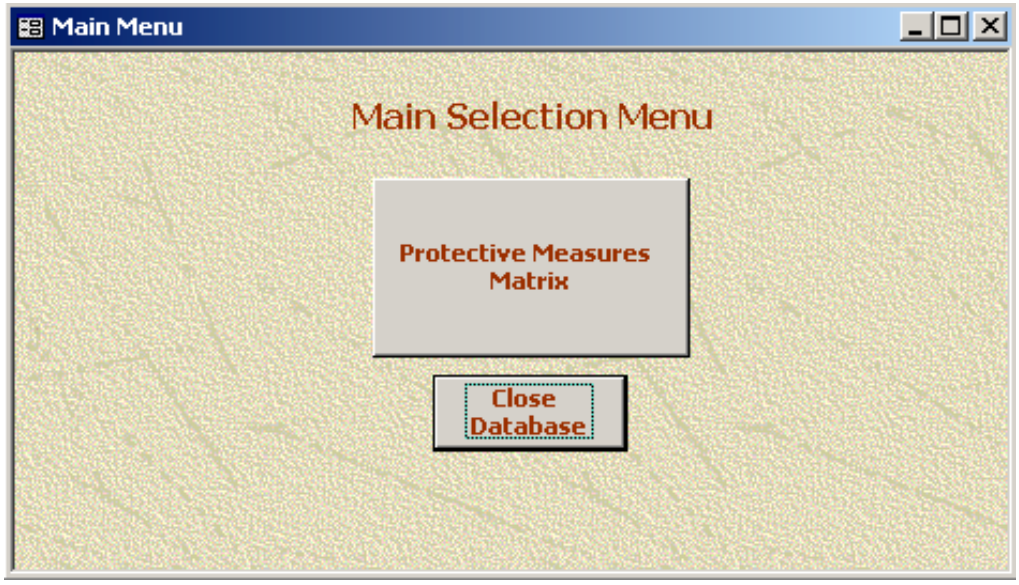


Figure 1. Protective Measures Database Main Menu

Start Point

After selecting the *Protective Measures Matrix* button on the Main Menu, users are launched into a subordinate screen and face a number of decisions, as shown in **figure 2**.

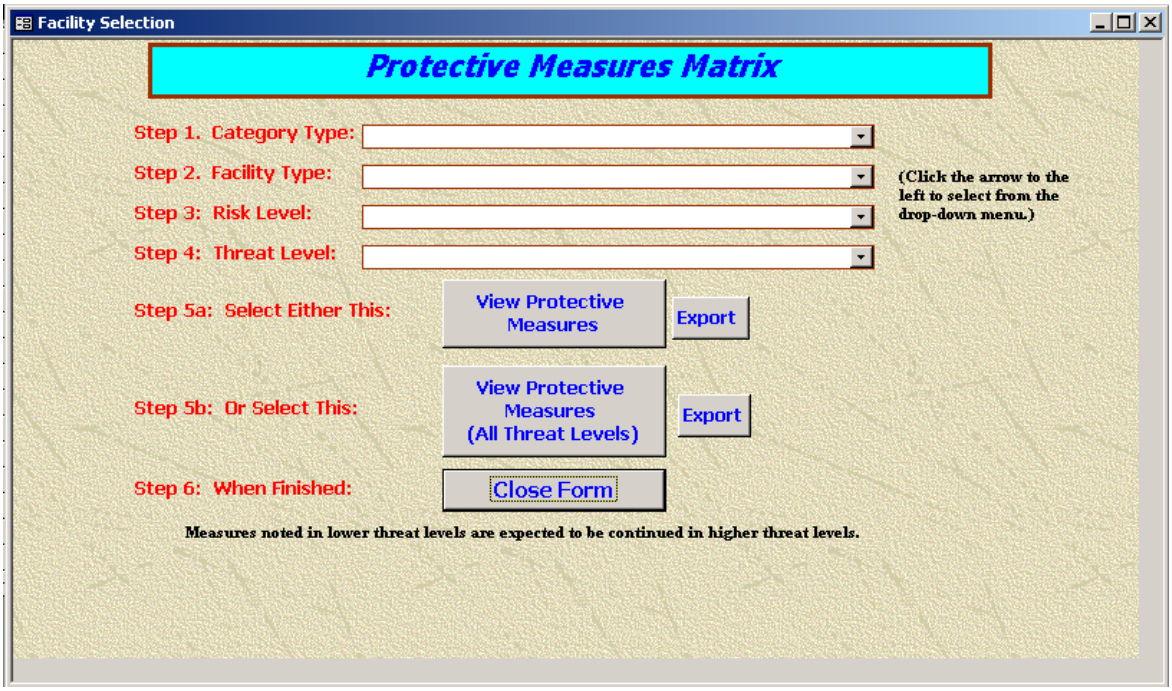


Figure 2. Protective Measures Matrix Screen

The **figure 2** screen shows the six steps used to select, review, and exit this screen. Each step is fairly simple and is completed using a drop-down menu or button. A drop-down menu is represented by a small triangle appearing at the right side of a field. By clicking on the triangle, a list of items for possible selection will appear. An example of the drop-down menu for Step 1 is shown in **figure 3**.

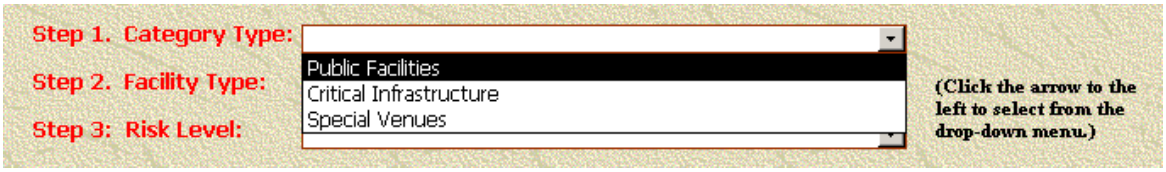


Figure 3. Step 1 Drop-Down List

There are also notes built into the various sections or buttons appearing on the screen. By placing the cursor over a particular button or field a small yellow box will appear. The box will contain a brief description of the contents or functionality of the selected item. If the user were to place his or her cursor over the *View Protective Measures (All Threat Levels)* button he or she would see a box identical to the one in **figure 4**.

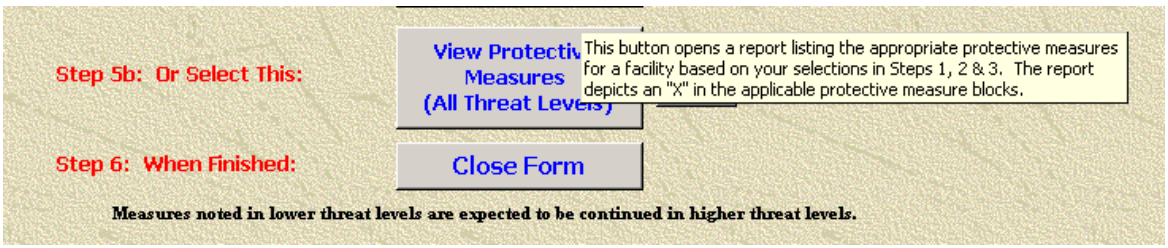


Figure 4. Help Box Example

If the user selects a combination that does not have protective measures associated with it or fails to make a selection in each of the four drop-down boxes, the message in **figure 5** will appear.

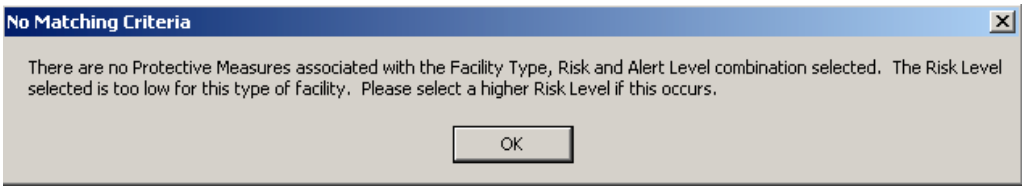


Figure 5. No Matching Criteria Error Message

Clicking the "OK" button will close the message box and return the user to the protective measures matrix screen.

Users must be prepared to make three decisions before launching the screen steps:

1. Type of **Facility.** This decision is based on the main category in which the facility falls in terms of public, private (critical infrastructure), or special venues.
2. **Risk Level.** This decision is based on the assessment results of **Part III, Assessments**.
3. **Threat Level.** Users review the current threat level as indicated by the Homeland Security Advisory System (explained in **Part II, Management**).

Once the three questions are answered, users toggle the drop-down arrows in Steps 1, 2, 3, and 4 of the **figure 2** menu and make the appropriate selection. Next, users decide which report output they desire from the following options:

- Selecting Step 5a, View Protective Measures, launches an output as shown in **figure 6**:

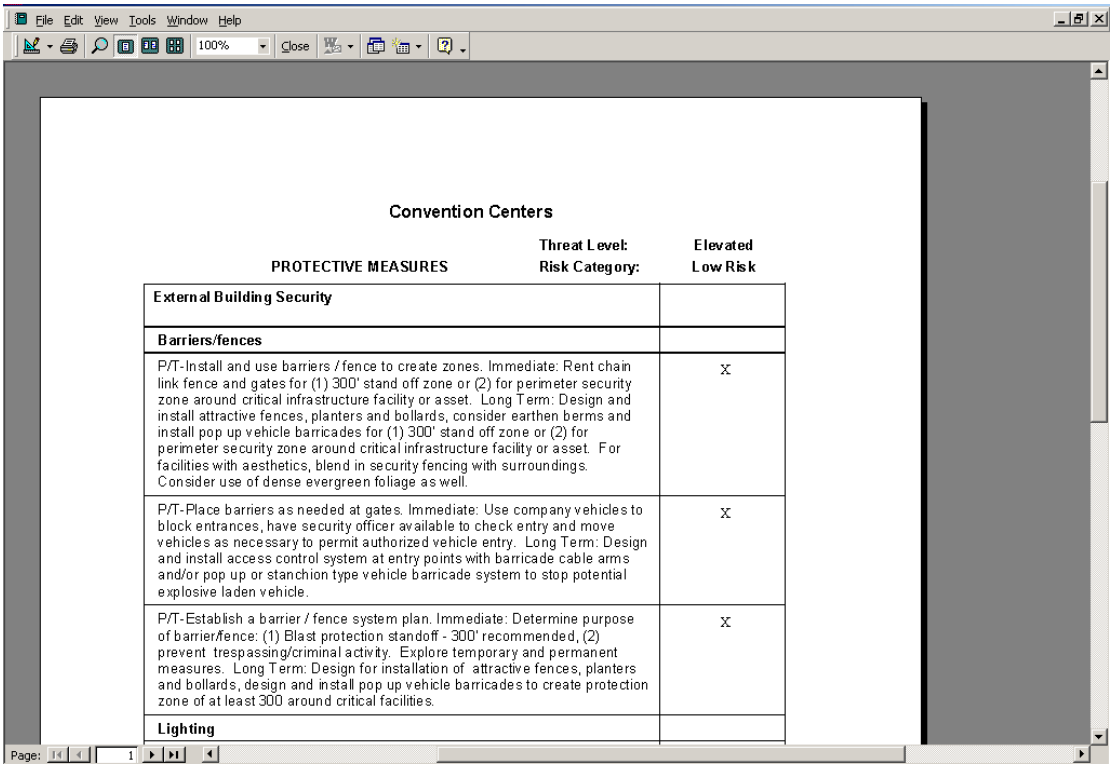
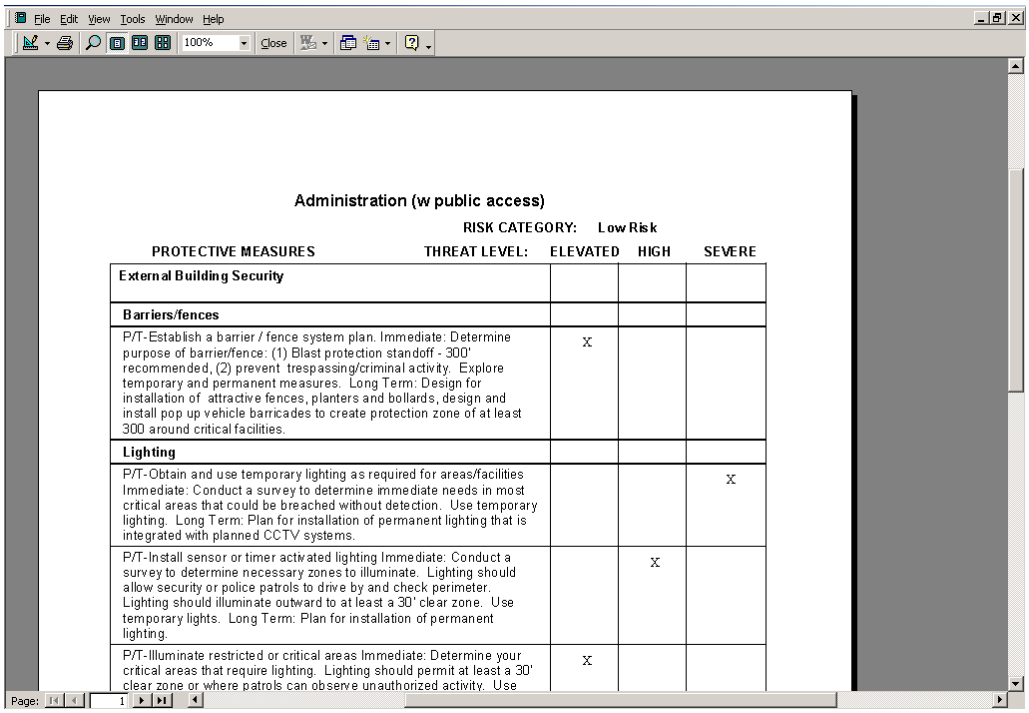


Figure 6. View Protective Measures Report

Note the arrows in the bottom left corner of the screen in **figure 6**. These arrows are used to move from page to page of the generated report.

To return to the protective measures matrix screen, the user simply selects the "CLOSE" button on the top of the screen.

Users can also select Step 5b as an alternative to display all threat levels (versus just one of the three listed options: elevated, high, or severe) (see **figure 7**).



Administration (w public access)

RISK CATEGORY: Low Risk

PROTECTIVE MEASURES	THREAT LEVEL: ELEVATED	HIGH	SEVERE
External Building Security			
Barriers/fences			
P/T-Establish a barrier / fence system plan. Immediate: Determine purpose of barrier/fence: (1) Blast protection standoff - 300' recommended, (2) prevent trespassing/criminal activity. Explore temporary and permanent measures. Long Term: Design for installation of attractive fences, planters and bollards, design and install pop up vehicle barricades to create protection zone of at least 300 around critical facilities.	X		
Lighting			
P/T-Obtain and use temporary lighting as required for areas/facilities Immediate: Conduct a survey to determine immediate needs in most critical areas that could be breached without detection. Use temporary lighting. Long Term: Plan for installation of permanent lighting that is integrated with planned CCTV systems.			X
P/T-Install sensor or timer activated lighting Immediate: Conduct a survey to determine necessary zones to illuminate. Lighting should allow security or police patrols to drive by and check perimeter. Lighting should illuminate outward to at least a 30' clear zone. Use temporary lights. Long Term: Plan for installation of permanent lighting.		X	
P/T-Illuminate restricted or critical areas Immediate: Determine your critical areas that require lighting. Lighting should permit at least a 30' clear zone or where patrols can observe unauthorized activity. Use	X		

Figure 7. Multiple Threat Level Display Report

Another report option available to users is to select the Export button, which sends the data selected using Steps 1 through 4 to a file type and location of the user's choice.

This Export option allows the user to transport current data to an Excel spreadsheet or several other format options, as shown in **figure 8**, and recall or manipulate the data as desired. Once the format is selected, the user is prompted to decide where to store this data, as shown in **figure 9**.

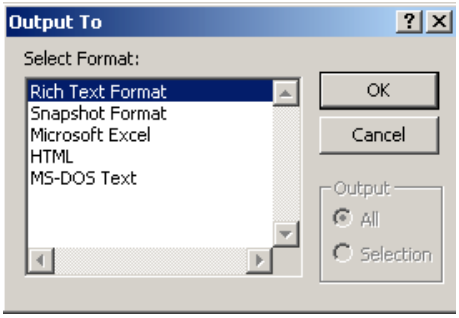


Figure 8. Export Screen

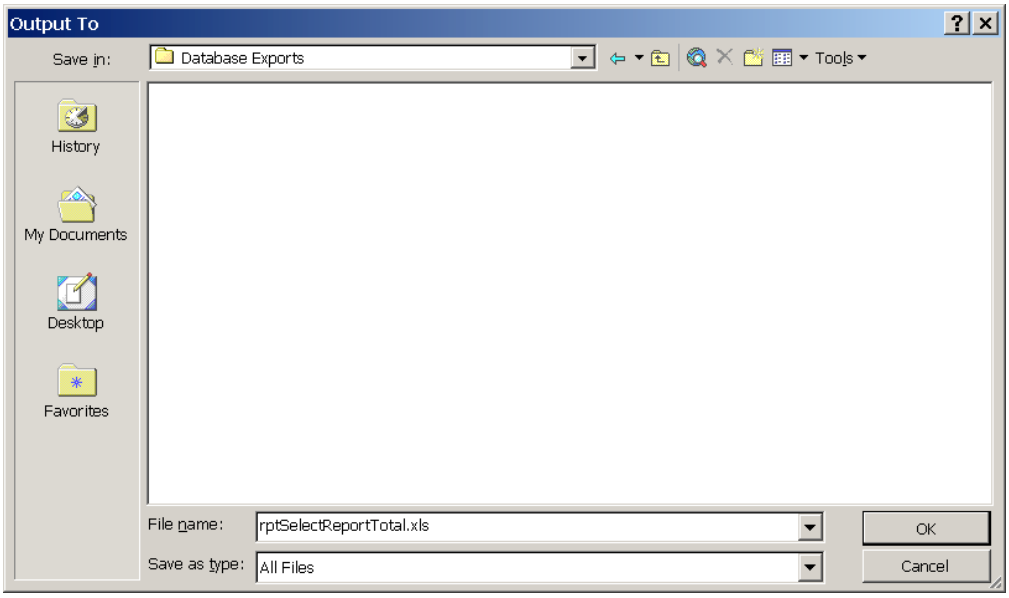


Figure 9. Export Report Storage Location

The .XLS suffix indicates that the file being exported is an Excel spreadsheet. The data that are exported to a spreadsheet include several data fields. A strong word of caution: any changes made to these fields will affect the data if they are reentered into the database tool. Saving work in a Microsoft Excel file enhances data transfer to Microsoft Access. This information may then be arranged and pasted into Microsoft Word or Microsoft PowerPoint, providing format flexibility and portability.

Remarks Database

An alternative version of the database has been included. This version works in the same manner as the standard version but it also allows users to enter remarks, comments, or cost data concerning the individual protection measures. The information can be updated or expanded at any time, allowing the database to serve as a tracking device for improvements or additions derived from particular protective measures.

Protective Measures Screen

With this version of the database, the screen used to identify the type of facility and the risk and threat levels includes an additional button. The button is entitled *Protective Measures Tracking* and is displayed in **figure 10**. All other elements of the screen work in the same manner as the previous version.

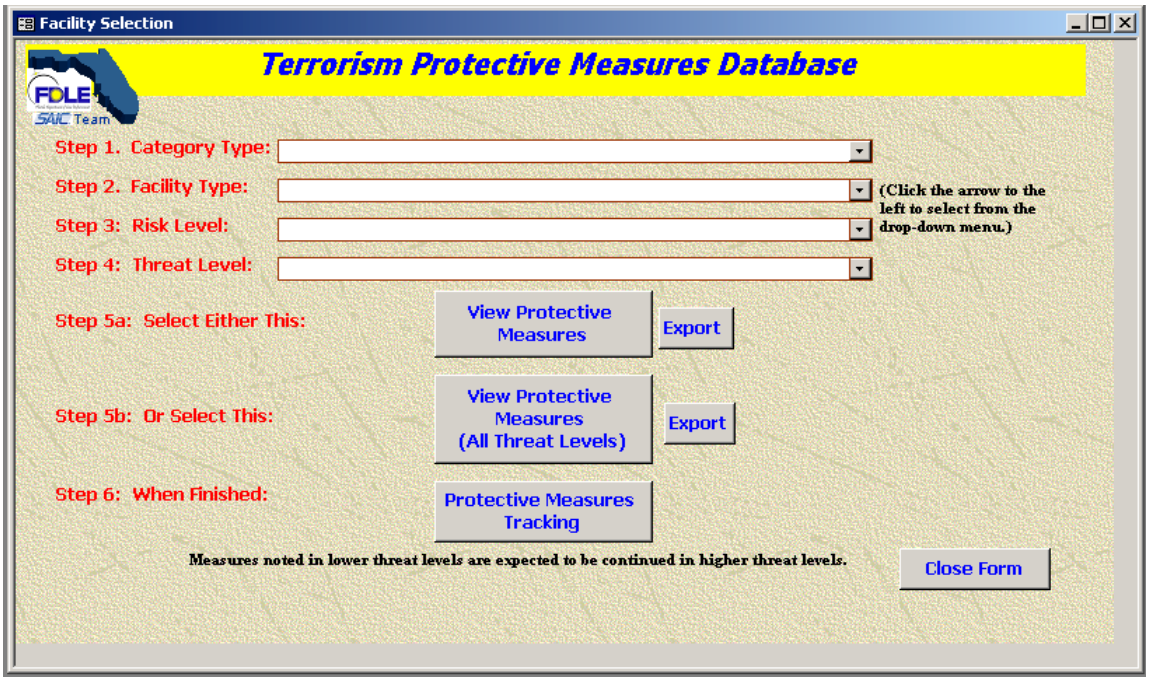


Figure 10. Protective Measures Matrix Screen

After selecting the desired criteria (facility type, risk and threat levels) the user can select this button to view a form containing each of the related protective measures (an example of this form appears in **figure 11**). If the user does not make selections in each of the drop-down boxes, they will receive an instructional error message upon clicking the *Protective Measures Tracking* button.

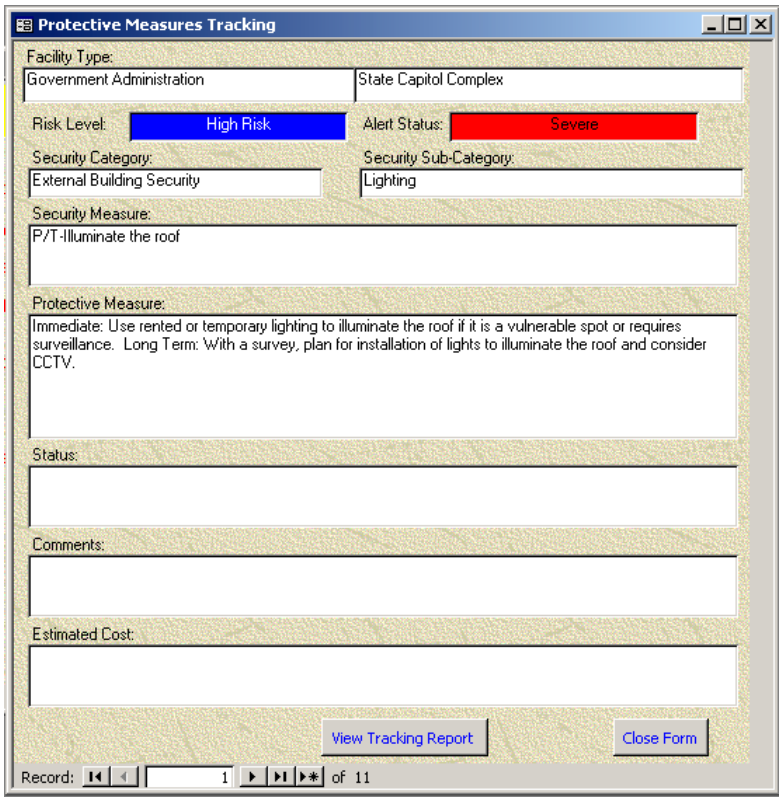


Figure 11. Tracking Screen

The tracking screen includes all the information that is presented in the protective measure reports. The arrow buttons located in the bottom left corner allow the user to navigate through the protective measures. In the case represented in **figure 11**, the user is viewing the High Risk measures under a severe threat status. The number to the right of the arrows indicates that there are 11 protection levels that apply to these conditions. As the user cycles through the different records the screen will update to display the correct information for the currently displayed protective measure. The three bottom fields are memo fields that allow the user to enter information they deem important with regard to that protective measure. These are memo fields that can hold a large amount of information and allow the user to cut and paste information directly into them. Scroll bars will appear along the right side of the field should the amount of information added be larger than the area displayed on the screen. Once the user has added information to these three fields (Status, Comments, Estimated Cost) that data will remain within the database until it is manually removed. To remove any information from these fields the user may simply highlight it with the mouse and press the *Delete* key on the keyboard.

Clicking on the button entitled *View Tracking Report* will open a report of all the protective measures meeting the criteria selected on the previous screen. In this example the criteria was State Capital Complex, High Risk and Severe Threat Status. An example of the report is displayed in **figure 12**.

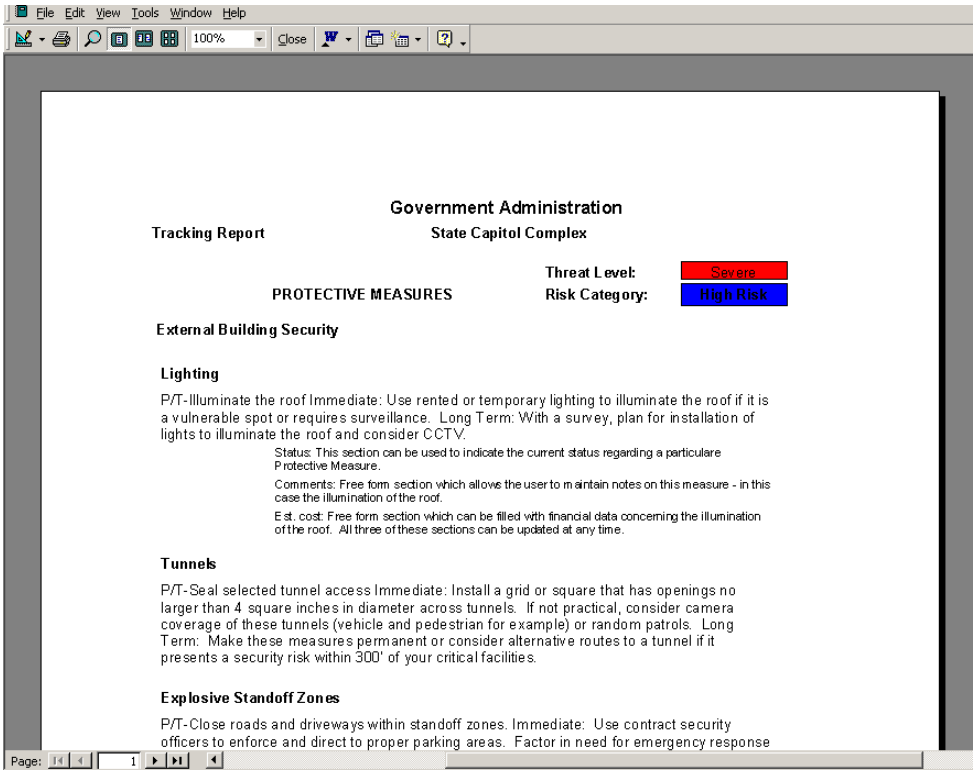


Figure 12. Tracking Report

The report gives all the information that appears on the checklist; it also includes information the user has added with regard to the three fields. In this example information has been added to all three fields to demonstrate how they will appear in report format. If no information is added to the Status, Comment, or Estimated Cost fields for a protective measure, that area within the report remains blank, as shown in the protective measure under the Tunnels category in **figure 12**.

Another Option

Users who do not have Microsoft Access but have Microsoft Excel can contact FDLE to obtain the protective measures matrices in a different format, as shown in **figure 13**.

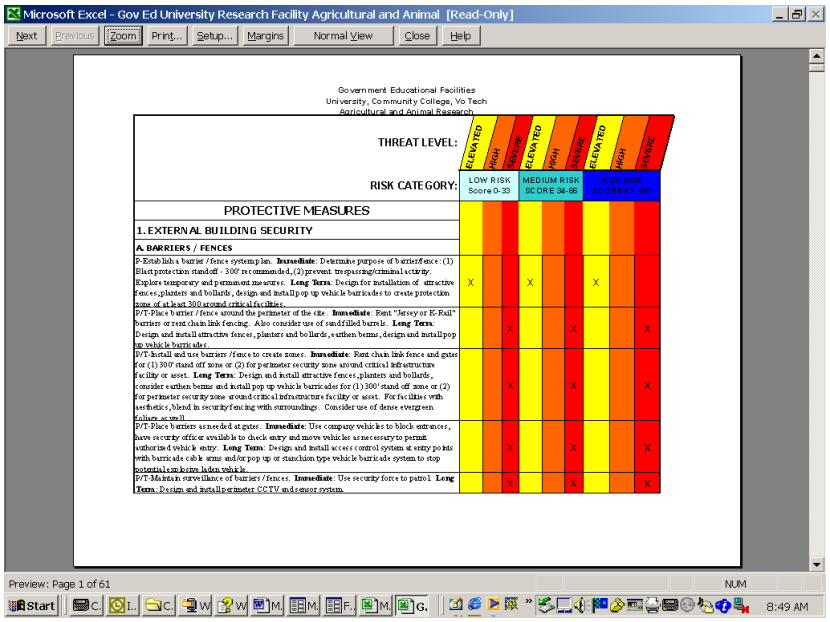


Figure 13. Microsoft Excel Protective Measures Matrix

The Excel spreadsheet contains more than 300 protective measures, including recommendations for immediate and long-term actions. The recommended measures for the specified facility are denoted by an "X" in the appropriate colored column.

There are nine colored columns, which are organized into three risk levels (low, medium, and high): each contains three threat level columns (elevated, high, and severe) which correspond to the Department of Homeland Security Threat Advisory System.

Locating Recommended Facility Protective Measures

Once the Microsoft Excel spreadsheet is opened, select File and Print Preview to view the spreadsheet with the header displayed. Next, locate the appropriate risk level for your facility and focus on the corresponding threat levels for your facility. Remember that these measures are recommendations.

Summary

Facility managers, owners, and state and local agencies have two options to determine their protective measures. The first option is the Protective Measures Database, which presents a revolutionary but simple method to determine the optimum protective measures to take. The second option, for those agencies and companies that cannot use this database, is the Microsoft Excel spreadsheet, which will help you select your protective measures based on your facility risk level and the corresponding threat level.

INTRODUCTION

Chapter 6: Summary of the Security Protection Process

From a macro perspective, there are three phases in designing a security program:

- Preparation
- Security Planning
- Implementation

These phases should be used as a guide for using the information in this Manual. Each phase should be completed before moving on to the next one—this process is designed so that each phase builds on the previous one. The result is a comprehensive assessment that enables users to select appropriate security measures. This Manual leads the user through the first two utilization phases (Preparation and Security Planning); the actual Implementation is up to the user and senior management

The Preparation Phase enables you to educate yourself on security concepts and assess the training needs of your organization. It instructs you to read the following information so you fully understand the concepts and terminology presented within this Manual:

Preparation Phase Steps:

1. Read the Introduction chapters and decide which facility category applies to you.
2. Read the Basics chapters to obtain an understanding of security concepts.
3. Read the Management chapters to understand roles, threats, planning, and training principles.
4. Review the security explanations in the Encyclopedia.
5. **Conduct a training needs assessment** by applying the principles discussed in the Training chapter (in the Management part of the Manual).

The following diagrams depict the planning process as a macro-level (high order) guide to security planning.

Figure 1 shows the flow of events recommended to organize your agency, department, or company's approach to using the TPM. It is designed to help you conduct your vulnerability assessment by using the sections of the TPM that apply to your facility. As the figure indicates, there are five steps in the Preparation Phase. As you initiate each phase, you should refer to the applicable areas in the TPM to assist you in each of the steps.

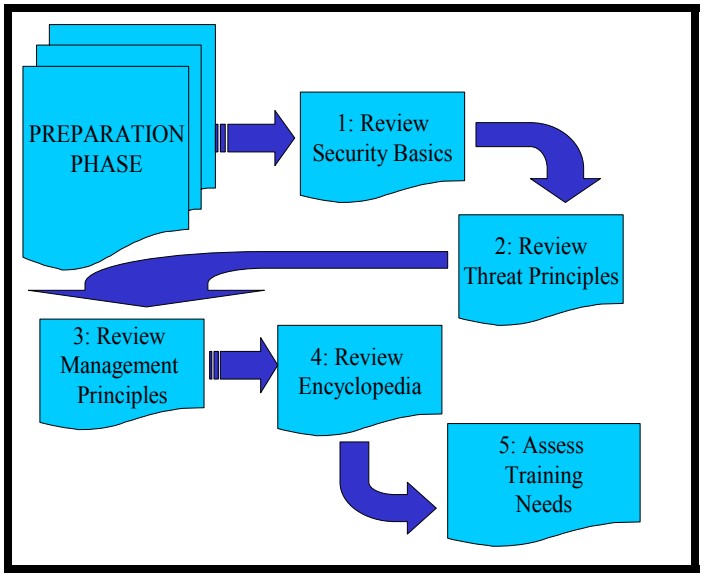


Figure 1. TPM Utilization Methodology (Preparation Phase)

The next step is to conduct the Security Planning Phase. You should now have some core security knowledge and should begin analytical planning work.

Security Planning Phase Steps:

1. Contact the FDLE RDSTF (or other intelligence source) and obtain the latest intelligence information in order to assess the current threat.
2. Select the facility category that most closely represents your building or site. Review the public, private, and special venue lists presented in Chapters 3-5 of this section.
3. Conduct one of the self-assessment options presented in Part III: Assessments.
4. Review the Protective Measures Database program and specific measures for your facility. Detailed use of the program is explained in Chapter 5 of this section.
5. **Use** the database output (matrix) as a **tool** to develop implementation strategies.

Figure 2 shows the flow of events for conducting your vulnerability assessment and preparing to implement protective measures. The TPM will assist you in determining your facility category (high, medium, or low) and threat level (using FDLE and the Department of Homeland Security threat levels), and conducting the self-assessment. After completing the assessment, go to the database and review the best practices that apply to the facility risk and threat levels. Then plan the training needed to implement your recommendations and review the final plan.

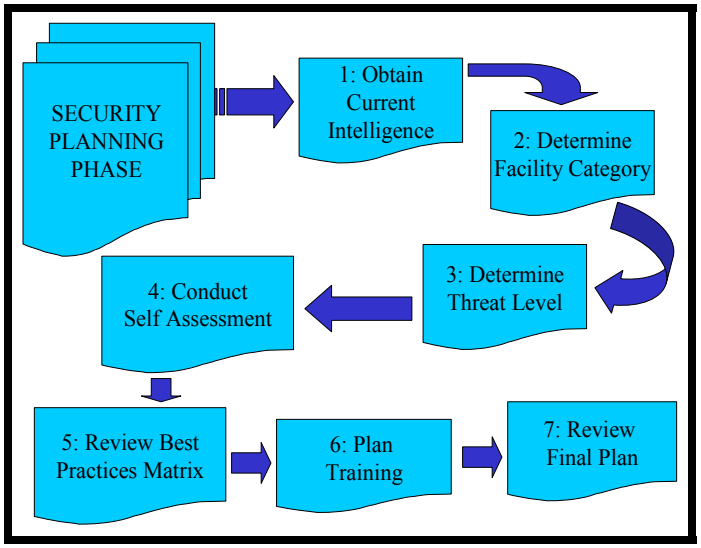


Figure 2. TPM Utilization Methodology (Security Planning Phase)

Implementation Phase Steps:

1. Implement the designated protective measures from the database matrix. This implementation step includes numerous tasks, such as writing policies and procedures, conducting training, changing or initiating employee security practices, and in some cases, purchasing and installing security technologies.
2. Evaluate (constantly) the results of the changes you've implemented. Conduct daily observations to correct and maintain a sound program. Schedule in-depth reviews, by an outside agency if possible, at least every 1-2 years.
3. Adjust the plans and procedures to enhance security and adjust to the needs of the organization.

Figure 3 shows the Implementation Phase in which you use the results of your self-assessment and the list of recommended best practices to begin to implement the

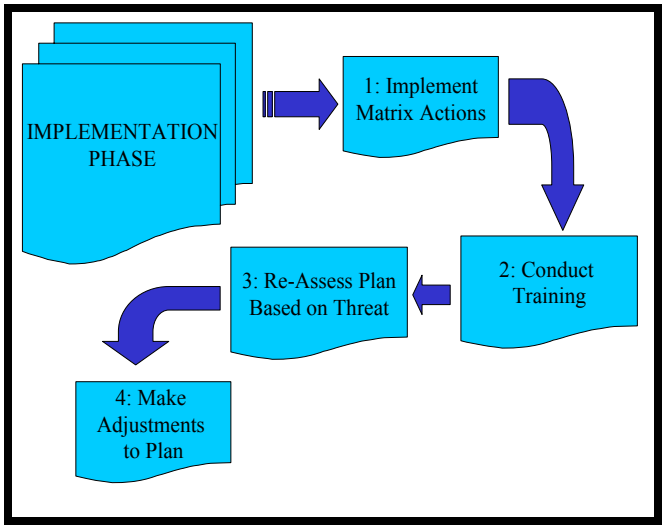


Figure 3. TPM Utilization Methodology (Implementation Phase)

recommended actions or security improvements. You then conduct training on the implementation, re-assess your plan, and make adjustments.

Management Role

It is critical for senior management to fully support protection efforts. This will require the time and resources of experts and professionals within the organization and, in some cases, outside expertise and assistance. Federal, state, or local governments may be able to provide support and/or experts may need to be brought in as consultants.

It is impossible to have a 100% risk-free facility, but with teamwork it is possible to greatly reduce risks. By reducing risks, an organization can:

- Provide a safer work environment
  - — Antiterrorism deterrence measures may also deter criminal activity
  - — Employees, visitors, and customers may feel more secure and may want to "do business" with you
- Reduce the consequences of a terrorist attack
  - — Strong security may deter the attack to a standoff distance, thus keeping your facility out of the explosion blast zone
    - The U.S. State Department's basic security measure for U.S. embassy facilities is to have the maximum standoff distance possible, but maintain some public access to the embassy or consulate
  - — Stronger windows and walls reduce blast effects
    - This proved valuable for the Pentagon in the September 11, 2001, attack
- Have a sound evacuation and recovery plan
  - — Trained personnel will know where to go and what to do in the event of a fire, explosion, or other emergency
    - Thousands escaped from the two World Trade Center towers before they collapsed. Reviews in the aftermath of the attacks indicated that many of those who were trained were able to safely escape
    - The Pentagon quickly assembled emergency teams for rescue and immediate medical attention for the injured—thus saving lives—and quickly shored up collapsed floors to allow rescue efforts to continue
- Reduce the time needed to get your facility back in operation
  - — Have a backup facility for your critical computer systems
  - — Have an emergency operations center to manage critical incidents
- Possibly obtain better insurance risk rates for your facility

PART I: BASICS

Chapter 1: Security Principles

Purpose

This Chapter presents an underlying foundation for an understanding of security. This Chapter will focus on those security and protective measures that respond to credible risks including that of terrorism.

It should be noted that security and protective measures designed to address risks of a general criminal nature or natural disasters will also, in most cases, mitigate the risk of terrorist attack. The most cost-effective measures are those that address multifaceted risks—and these may not be the most expensive or resource-intensive security/protective measures.

In addition, security measures should be viewed as part of an overall strategy rather than as individual components. Measures must be designed to work together to meet specifically defined protection objectives for an organization or facility. This will avoid the undesirable situation of security measures counteracting one another or significantly interfering with the organization's ability to perform its mission or effectively use its facilities.

This Chapter is intended to provide decision makers with a general background in security concepts and principles. In turn, this will assist in determining the best protective strategy for a particular organization or facility based on current best practices as well as cost/benefit considerations.

Fundamentals

There are a variety of security disciplines, each with specific requirements and essential elements designed to enhance protection efforts. Some disciplines will be more relevant to particular environments than to others. For example, an organization located in a multi-tenant office building might have less control over exterior physical security controls than an organization located in its own building that is closed to the public. In the case of the agency or organization occupying rented or leased space, the landlord or property owner is responsible for general security outside of the actual leased office space. However, the agency may have unique requirements for security that it will require the landlord or owner to fulfill as terms for occupancy and lease. Regardless, as is true for the General Services Administration (GSA)—the federal government's lease agent—such security requirements cannot unduly impose on other tenants in the building.

In all environments, regardless of the ownership of the building or facility, all security disciplines should at least be considered, and the appropriate elements of each included in an integrated security approach.

General Security Concepts

Security is different from law enforcement or police services. Law enforcement and police are concerned with protecting life and property; however, they do not have a general fiduciary or legal responsibility as does a landlord or property owner. In other words, the Miami Dade Metro Police cannot be held responsible for general crime conditions in Miami. Obviously they can be criticized for weak patrol tactics or a poor case closure rate, but in general they are not legally responsible for making sure you can walk down the street without being attacked. In contrast, if someone is attacked in a hotel room and the property owner demonstrated poor security practices such as broken locks and broken self-locking corridor doors, or perhaps there was a pattern of crime in and around the hotel, the property owner could be held partially responsible for the criminal act.

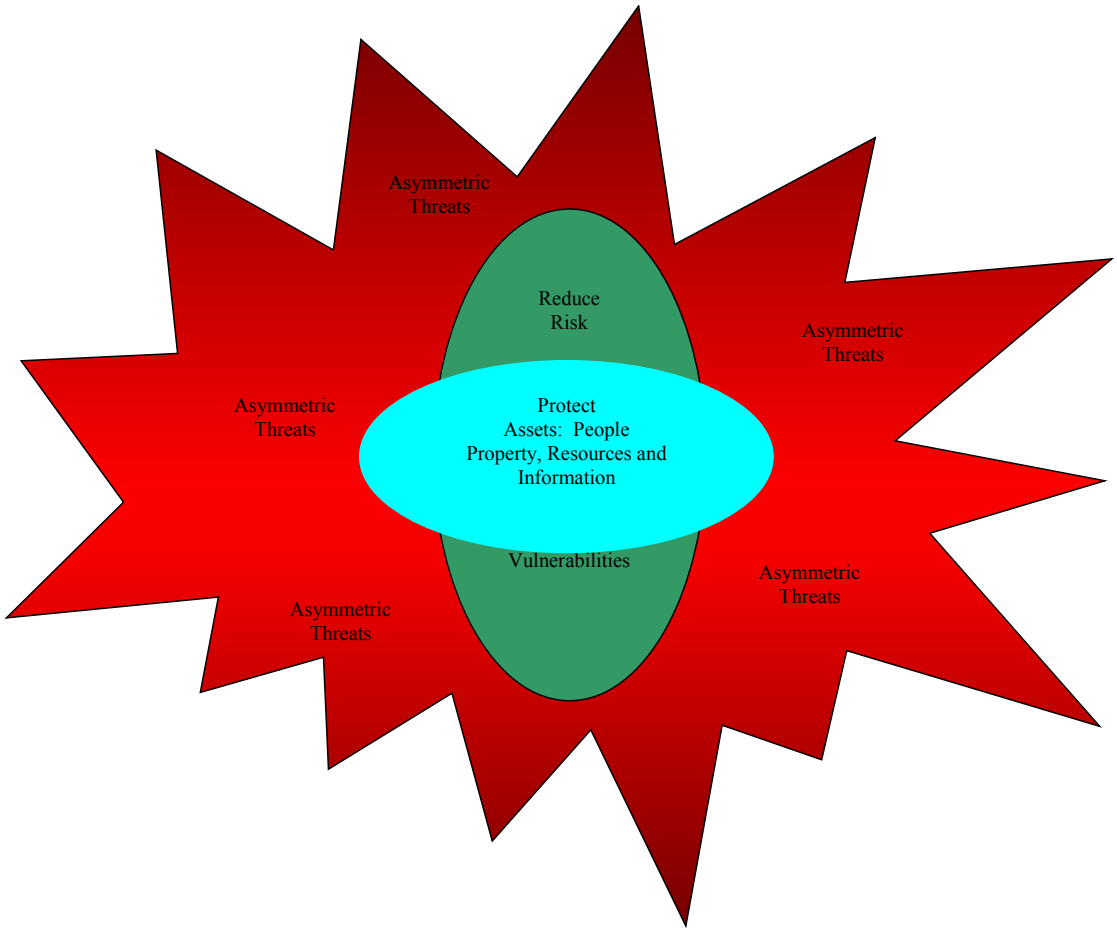
Because a property owner under some circumstances can be held responsible for allowing unsafe conditions to exist on his or her property, it is incumbent on that property owner to have reasonable security measures in place. While it is impractical to hold that owner responsible for all criminal acts, there is sufficient case law that indicates that property owners must take reasonable measures concerning lighting, locks, and other aspects of physical security to ensure the relative safety of their employees, customers, and the public. Therefore security is generally proactive, not reactive as is the case for law enforcement and the police. This does not mean that police departments can't be proactive in areas of crime prevention, but generally we do not expect the police to individually protect private property.

Security means that preventive, proactive measures are in place to reduce the likelihood of a criminal act or terrorist event or to mitigate the results of a disaster such as fire, earthquake, flood, or other occurrence. Security is designed to do the following:

- Reduce vulnerabilities
- Reduce risk
- Protect assets—people, property, resources, and information

You can in effect reduce your vulnerabilities by reducing your risk, which in turn protects your assets. The relationships among these three are interchangeable and mutually supporting.

The following diagram reflects that asymmetric threats can come from any direction. The vertically drawn oval shows how reduction of risk and vulnerabilities attempt to protect assets, but cannot, even under ideal conditions, cover all angles of threat. For example, you should note the lack of risk and vulnerability reduction on the right and left sides of the "protect assets" oval which shows there are always security gaps.



The primary challenge to reducing vulnerabilities, reducing risks, and protecting assets is:

Reducing the Threat. Although you cannot completely eliminate any threat, you can reduce the threat by implementing some security measures that will reduce your vulnerabilities, which in turn will reduce your risks and thereby increase the protection provided to your assets (people, resources, property, and information). These assets are categorized and defined as follows:

- *People.* Protecting your personnel should be job one. It is important that you offer the best protection possible for anyone who visits, works, or conducts business at your facility or site. Obviously it is important that your customers feel safe, particularly in the retail, entertainment, and hospitality industries. Any evidence of unsafe conditions in these industries will spell trouble for your business. There is nothing more disturbing to your customers than a retail shopping area with graffiti on the walls, trash strewn about, broken windows, and shuttered stores. In an office or business setting, employees must feel safe within the facility and in parking lots. This will require a 24/7 safe environment for those businesses with continuous operations and accompanying pedestrian and vehicle traffic. People are your highest-threat target. Protect your people and they will protect your business, agency, or department.
- *Resources.* Resources are the supporting components of your business or industry. They include administrative equipment such as computers, furnishings; mechanical equipment such as tools, spare parts, machinery; and inventory and merchandise that is critical to the retail industry. What separates resources from property is portability. We consider any moveable item to be a resource, including parts inventory, retail merchandise, fixtures, automobiles, aircraft, funds, and other depreciable items. Resources can be the target of a terrorist attack or criminal act for purposes of theft, sabotage, vandalism, or evoking a loss of confidence in an agency or industry.
- *Property.* Property is the physical plant, structures, and grounds of your organization or agency. Property can range from a regional or branch office in a quiet suburban campus to a multistory urban government courthouse and jail to an oil refinery. Property attacks are emotional events due to the high potential for loss of life and injury. Our three most significant terrorist attacks in the United States involved the mass destruction of property: the Murrah Federal Building, the World Trade Center, and the Pentagon. Property may be one of the easiest targets because of its high visibility, difficulty in securing, and likelihood to contain people.
- *Information.* Based on recent experience, it is clear that information has become a primary target of attacks of all types. Such attacks can be a malicious or revenge-type attack, an attack for economic gain, or a terrorist attack to exploit data or change safety or control settings. Information protection programs are now generally referred to as cyber security or Information Security (INFOSEC). Our nation's communications and computer systems are the primary target of economic and emotional attacks. Although these attacks do not generally result in loss of life (except as one example the disruption of our automated Air Traffic Control Enroute System, which could be devastating) such an attack could be economically devastating to our nation. One particular challenge of a cyber (online) attack is that it can originate in Singapore, with the attackers switching Internet Service Providers (ISP) several times via access points in Tokyo, Montreal, Boston, and Cincinnati, (or a variety of other ISP nodes) and terminating in Orlando, thus making the origin of the attack difficult to trace.

The Threat

With a basic understanding of the concept of security—a proactive and preventive method to reduce vulnerabilities, which reduces the risk, which reduces the threat, which

increases your protection of assets—it is then necessary to understand the nature of the threat and what we can do about it.

In the current environment, our security experts and national intelligence agencies with the support of the Department of Homeland Security (Customs, Immigration and Naturalization Service, U.S. Secret Service, U.S. Coast Guard, and Transportation Security Agency [TSA]), the Department of Justice (U.S. Attorney General and the Federal Bureau of Investigation [FBI]), the Department of Defense (U.S. Northern Command and the military departments) and state agencies (Florida Department of Law Enforcement) are actively engaged in developing and disseminating today's threat information.

Today's threat picture is that we face a real threat from transnational terrorist groups (groups whose sponsorship is not easily traceable to specific states such as the former Soviet Union, Libya, or Iraq) who are engaged in unconventional or *asymmetric attacks*. This term means that terrorist groups such as Al'Qaeda (also spelled as Al'Qaida) are using very basic but destructive means for their attacks.

Terrorists have moved from attacking individuals—as seen in the l980s when European groups such as Baader-Meinhof and the Red Army Faction attacked U.S. officials such as then-Ambassador to NATO General Alexander Haig and U.S. Army General Fredrick Kroessen—to more radical terrorist groups launching attacks of greater destruction, such as the attacks on the U.S. Embassy in Lebanon, the U.S. Marine barracks in Lebanon, and the September 11, 2001, attacks in the United States. As the U.S. strengthened major targets, the terrorists either chose less-secure targets or simply increased the size of their weaponry.

In the l990s and now, terrorists are not attempting to kill or kidnap generals and ambassadors, they are simply killing and kidnapping "ordinary" people who are not as well protected. If they cannot hit the White House with a truck bomb on E Street or Pennsylvania Avenue (both now closed beyond the standoff distance), they will simply hijack a B-767 aircraft or even a regional jet from Reagan or Dulles airports and crash it into the White House for much the same effect as a bomb. This is an example of an asymmetric attack.

Or, rather than directly attempt to injure Senator Tom Daschle, or NBC's Tom Brokaw, the terrorists mail anthrax-laden envelopes and cause much the same effect. That is also another example of an asymmetric attack and it is today's terrorist threat.

More prevalent today versus the l980s is the threat of attack using chemical, biological, radiological (defined as the use of nuclear material), and nuclear (the use of a weapon) technologies. Although the use of an improvised explosive device or an improvised incendiary device is common, improved security has led terrorists to resort to larger "vessels" for attack. This was seen in the l995 bombing of the Murrah Federal Building in Oklahoma City and the l996 bombing of Khobar Towers in Saudi Arabia.

We have witnessed this asymmetric tactic in the large-scale attacks involving thousands of pounds of fuel (Khobar) and improvised explosive devices (Murrah). These attacks culminated in the use of fuel-laden jet aircraft to destroy the twin World Trade Center towers and damage the Pentagon. A fourth aircraft was likely intended to crash into the White House or the U.S. Capitol building. Two post-September 11 attacks—the attack on the entertainment district in Bali, Indonesia, and the attack on the French tanker—demonstrate the willingness of terrorists to use unconventional and improvised methods to hit targets hard for maximum destruction and casualties.

We now know that the basic terrorist threat includes the use of weapons of mass destruction in forms such as the following:

- Explosives such as fuel and accelerants to form a bomb or improvised device
- Chemical agents such as industrial bleach, corrosives, and solvents that are used to create a chemical agent or gas

- Biological threats such as anthrax, smallpox, and viral agents
- Radiological agents such as nuclear waste or nuclear material used in power plants and medicine to contaminate an area and cause radiation poisoning
- Nuclear weapons such as an improvised or stolen nuclear warhead of military quality for a more widespread impact.

We also know the likelihood of a terrorist event is relatively high since terrorist groups have demonstrated the capability and capacity to launch an attack on U.S. soil. We know terrorists are very patient and do not have to be well organized simply because they set the ground rules, not us. It does not take an army of terrorists to attack, but it takes an army of many to defend.

What we do not know is where or when an attack will occur. Accordingly, we have to have major security programs in place to protect people, resources, and property by reducing our vulnerabilities, which reduces our risk, which reduces the threat.

With all of these factors in play, experts agree that the threat is high but the time and place of an attack is difficult to predict. Within this environment we have to secure our facilities without causing major disruption to our economy and way of life while protecting our citizens from undue risk.

Security Disciplines

Security practitioners have categorized the concept of security into several disciplines. These are areas of security that, if implemented separately or as part of a fully integrated security program, can contribute to the overall protection of a facility, site, or building to the benefit of an agency or corporation.

The following are recognized as the major security-related disciplines:

- **Physical Security** is generally and casually referred to as "guns, gates and guards." These are the obvious physical measures typically used to protect property but that also assist in protecting people, resources, and, sometimes, information. The features of physical security include the following:
  - Perimeter. The boundary of your building, facility, or site can be physically protected with a fence, which can be of solid construction using concrete block, stone work or poured concrete, chain link, wrought iron, wood, or PVC. Another way to physically protect the perimeter is with natural features such as earthen berms, large boulders, trees, and dense evergreen shrubs.
    - The perimeter may also be protected with cameras and sensors to aid in detection, assessment, and protection of the property.
    - Locks and gates are also features of the perimeter.
    - More sophisticated security applications might include access control to the property through vehicle and pedestrian gates.
    - Blast protection is becoming a more common feature, particularly in new construction for perimeter protection. Blast protection is critical in facilities with large glazed (glass) areas or high-risk facilities that do not have standoff features. A standoff feature simply puts distance between the facility and the locations where a truck or explosive device can be positioned.
  - Exterior. Although exterior might appear to mean the same thing as perimeter, it does not. The exterior of the property or building is the immediate outer layer of the building and close-in parking and access points. An example of this would be

referring to the airport perimeter as the areas surrounding the runways and parking lots. The exterior of the airport would be the terminal building.

- The exterior can be protected much the same as the perimeter. In fact, in urban areas, facilities and buildings may not have a perimeter because they are generally located on the street or in densely built-up areas. The "perimeter" may actually be the building exterior.
- Physical security for the exterior is much the same as the perimeter, but with access control and closer monitoring at many facilities. This may be as simple as having a receptionist in the lobby to register and direct visitors, or more elaborate measures such as having an armed security force (or sworn personnel in some government facilities) control entry and access to the building.

— Interior. The interior is the innermost area in which your physical security measures will be implemented. Often your most critical areas are in the building interior, such as command centers, courtrooms, detention centers, or retail and merchandise areas. Again, many of the physical security features of the perimeter and exterior can contribute to interior security. Here you will also have more stringent access control and alarm systems. The presence of a security force (or sworn personnel) will probably be a feature as well.

✺ **Personnel security** has long been standard in the U.S. government because many government agencies require security clearances for agency employees who handle and have access to classified information. The basic access levels are Confidential, Secret, and Top Secret, with these levels defined by the amount of damage to national security that would occur if the information were given to the wrong person. Generally speaking, most military personnel, special agents, and federal employees in law enforcement, intelligence, nuclear energy, and national security agencies have access to classified information.

— Personnel security programs require background checks and a means to screen, vet or otherwise verify the integrity, trustworthiness, or qualifications of individuals who are to be granted access to classified information, sensitive facilities, key personnel (elected officials, special agents, and agency directors), or other resources of an organization. Such programs may also require a mechanism to establish various levels of trust for employees or others who have any type of access. Although state and local governments may not handle classified information related to national security they do have distinct classification levels of sensitive information.

— Many state, local, and private organizations have implemented personnel security programs referred to as proprietary or protected programs in which firms and agencies conduct background checks, also called due diligence, to ensure that the people they hire and employ can be trusted. This often involves the need to ensure that employees will handle cash and resources honestly and will not engage in theft of funds or resources.

— In addition to ensuring trustworthiness in fiscal matters, some agencies must conduct due diligence checks to meet security requirements for workers in day care, health care, and private security jobs, for those with investigative or sworn authority, and for those in career areas such as accounting, law, medicine, and other professions. These checks can include a credit check, criminal history check, psychological screening, and screening for the ability to maintain the trust and confidence of the public. Another screening tool is the polygraph examination, which is authorized for some public agencies (law enforcement in particular) to further assist in the background and screening checks.

— Private corporations and agencies do not have the ability to conduct as thorough a check as the U.S. government and state agencies do, simply because of privacy protections for employees in the private sector. Generally, private companies can request a criminal history (restricted to adult convictions) and a credit check, plus the administration of a "pen and paper" honesty or psychological test such as the Reid Survey or the Minnesota Multi-Phasic Inventory (MMPI) administered by private companies. An additional measure is the use of the polygraph exam in cases where a company can make the exam a condition of employment. Managers must consult an attorney before administering polygraph exams for prescreening or as part of investigating an employee suspected in an incident. Also, an attorney should be consulted to determine the admissibility of polygraph results in either a criminal or a civil proceeding.

- **Technical security** consists of measures that protect against technical threats such as eavesdropping, electronic intercept, and wiretapping; it can also involve the use of special sensors or other technical systems to detect the existence of an unconventional threat. Government agencies, particularly the military and the Department of Justice, have access to very sophisticated tools to detect or intercept signals from radios, conversations, computers, etc. Corporations need to contract a private firm if screening, debugging, or constructing "secure rooms" for sensitive conversations is desired.
- **Crime prevention** is mostly an area for police, but if used by private companies, may be any measures taken to prevent criminal activity including neighborhood/area watch programs, the use of Geographic Information Systems (GIS) and statistical analysis, Crime Prevention Through Environmental Design (CPTED), awareness and reporting mechanisms, liaison, and loss-prevention measures.
  — Facility managers can consult with local police for crime prevention suggestions and advice, but in many cases police will not have the necessary manpower and time to actively manage a corporation's crime prevention program. Major developers of shopping centers, malls, housing, and complete neighborhoods often hire crime prevention experts during the design phase of a project; for existing projects, they also hire private crime prevention consultants. This may result in implementing improved physical security measures, using awareness programs, or employing private security guards to bolster the crime prevention program through fixed posts or patrols.
- **Antiterrorism** is specific measures to prevent, mitigate, respond to, and recover from terrorist attacks, including those that may use weapons of mass destruction. Antiterrorism differs from counterterrorism, which uses preemptive measures to disrupt, deny, delay, or mitigate a planned terrorist attack. Counterterrorism is usually the responsibility of select U.S. military elements and the FBI, unlike antiterrorism, which is everyone's responsibility.
- **Information technology (IT) (computer or cyber) security** consist of measures, both technical and nontechnical, to protect critical data and the systems (hardware, firmware, and software) that store, process, transmit, or otherwise handle it.
  — The physical protection of information technology centers is a very small part of the overall IT program. The most critical components are the security provided to the software and data, as well as the local area network (LAN), network, routers, and hubs to prevent malicious attacks on the information systems.
- **Personal safety** is any actions, techniques, procedures, or systems specifically designed to protect individuals including senior leadership, employees, staff members, visitors, users, customers, contractors, on-site vendors, tenants, occupants, and others.

— Personal safety is usually provided through security education and motivational programs to remind employees of preventive steps to avoid being a victim of a crime or a terrorist act. This can be done through motivation steps, posters, Web sites and banners, and education and training on detecting possible surveillance activity, planning routes of travel in high-risk areas, and using survival techniques.

— It may also involve directing employees who are on overseas travel in high-risk areas to undertake protection measures and to visit the U.S. Department of State travel advisory Web site.

— At the highest end of this program, some firms employ Personal Protection Operations or Personal Security Operations (PPO/PSO) personnel to accompany executives and others into high-risk areas. PSO operations are not simply a bodyguard service: often PSO personnel cannot be armed because of state and international restrictions, so they must use other protective measures such as armored vehicles, safe houses, alternative routes, advance reconnaissance of the travel route, and trusted local officials to assist with PSO operations. In addition, PSO personnel have no more authority than a private citizen to make an arrest or use force. Hiring an off-duty police officer does not absolve you of responsibility or liability.

Within each of these disciplines, the measures taken may overlap somewhat but are intended to influence one or more of the underlying factors in the risk management process. In other words, security measures are designed to do the following:

- Mitigate the threat to an asset by reducing risk
- Reduce or eliminate vulnerabilities
- Minimize the impact in the event that an attack occurs
- Help protect people, resources, property, and information.

When applied independently, these disciplines may provide some degree of protection or stopgap security; however, when used as part of an integrated strategy, they significantly decrease the likelihood of a security incident with a major impact on an organization's assets or operations. This is the concept of *integrated security* and represents a synergistic effect, putting often-scarce security resources and budgets to the most effective use possible.

Security measures address threats that are intentional (e.g., criminal acts and terrorism), inadvertent (e.g., human error, unanticipated failure of a machine or component), and natural (e.g., storms). Obviously, terrorism represents an intentional threat, but often the same protective measures can address all three categories of threats. Examples of measures that are particularly effective against all three threat categories are these:

- Policies
- Procedures
- Emergency planning
- Employee awareness and reporting mechanisms
- Exercises and drills
- Coordination and liaison
- Primary and backup communications.

These measures are discussed throughout this document and cannot be overemphasized.

The Basic Function of Security

Whether intended to address intentional, inadvertent, or natural threats, most security and protective measures are designed to serve one of four functions, commonly known as

the Four Ds. They are: Deter (criminal [including terrorist] activity); Deny (the perpetrator access to the intended target of the attack); Detect (an attack or attempt in progress and alert appropriate authorities and response forces); and Delay (an attack to allow adequate time for an appropriate response, or to make continuation of an initiated attack unreasonable to the perpetrator). These Four Ds should be considered whenever a new protection strategy is being developed or an existing one is being reviewed or revised.

Security and protective measures encompassed in the Four Ds relate to *prevention* and *response*. The remaining security protection measures are associated with the *recovery* function. Together, prevention, response, and recovery represent all facets of the security role in any organization.

Security and protective measures can range from highly sophisticated and expensive solutions to simple and inexpensive policy changes that can have significant results. They commonly fall into three types: policies, procedures, and technology/engineering. Each of these types will be addressed in the remainder of this chapter, along with cost considerations; however, two other fundamental concepts will be discussed first: layered security and security management.

Layered Security

Whether protecting a high-risk facility, an inventory of high-value merchandise, or critical information, a fundamental concept in asset protection is layered security (also known as defense in depth and the concentric rings of security). Layered security is sometimes illustrated as a series of concentric circles as shown in **figure 1**. The diagram presents two examples of how layered security might be viewed: one from the perspective of a local/state government site that stores a supply of dangerous material that may be an attractive target for terrorists, and the other from the perspective of a typical retail facility that needs to protect the cash on hand.

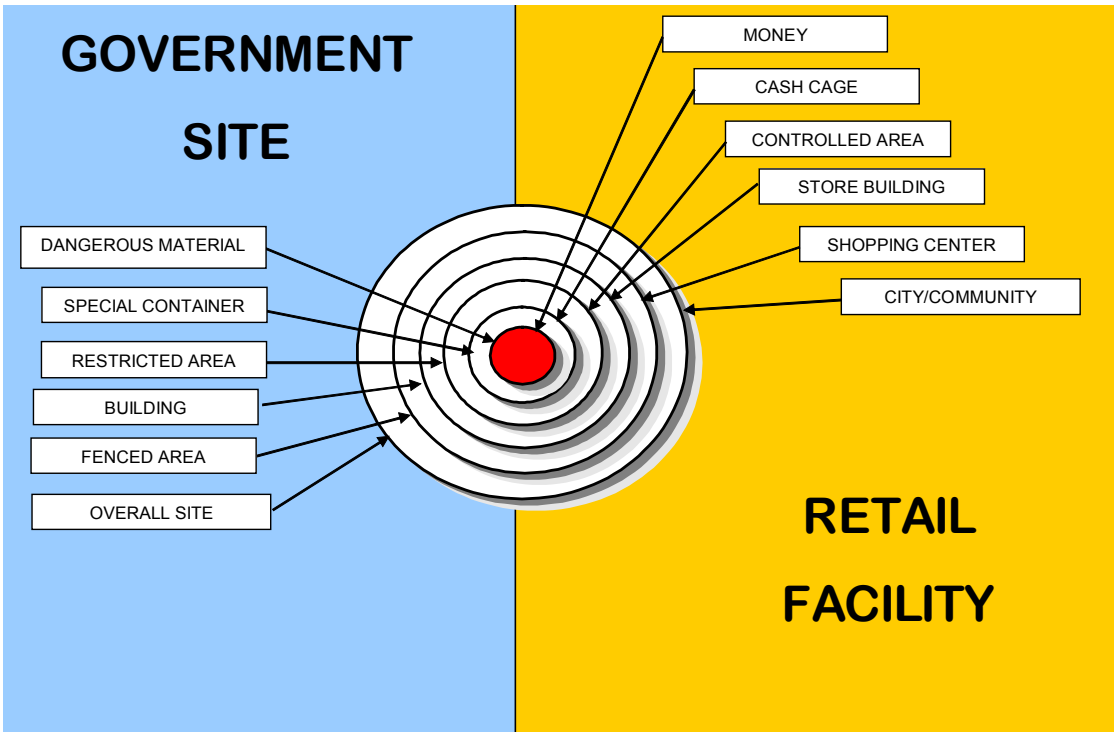


Figure 1. Layered Security Diagram

[1] Courtesy of Innovative Protection Solutions, LLC and ASIS International, 2002

As you can see from this figure, the most critical components of a facility or site are located in the innermost and presumably the most protected part of the facility or building. The figure shows an example for both the private sector (retail) and the government or public sector using this proven layered security concept. Having security layers reduces a facility's risk and vulnerability to an attack against the most critical areas of the facility.

This view serves to remind decision makers that the protective layers must defend against risks coming from any direction or angle—not just from the front door. It is also important to note that risks may originate internally as well as externally. When considering the layering concept, these internal-origin risks cannot be neglected.

Various security/protective measures may be applied at each of the layers and particular security roles and responsibilities also exist at each of the layers. For example, a retail center involved in a neighborhood watch program, or a state government site represented on a local security coordination committee (composed of neighboring businesses, local law enforcement, and others) actually represents an outer layer of security for the organization.

Depending on the nature of the assets, threats, and vulnerabilities, there may be a larger or smaller number of layers, and the individual layers may have varying degrees of robustness.

The concept of layered security is important in developing a comprehensive security strategy and should be carefully reviewed in any planning or assessment process.

Some concepts to use when implementing layered security:

- Extend your security zone to deter, deny, detect, and delay threats to the outermost point that is physically, fiscally, and legally possible. Example:
  - At the Orlando International Airport (ORL), the physical outermost part is probably the chain link fence that surrounds most of the airport property, particularly the runways and taxiways. Ideally, ORL would extend its protection zone as far as possible beyond the fence line and into surrounding areas. This does not mean that ORL can fence off the Beeline Expressway and the hotels and rental car agencies near the airport, but perhaps ORL can work with the Orange County sheriff and local agencies to patrol and be aware of any suspicious activity near the airport. In effect, ORL will have extended its protection zone beyond the fence line through information exchange, patrols by the sheriff, awareness of activity by shuttle drivers and taxi and limousine operators, and close coordination with the TSA, FBI, and other agencies.
- Bring security to the bad guys, not the bad guys to the security. In other words, present a strong security program or deterrence well away from the highest protected areas. Example:
  - In the case of ORL, the highest protected area is the Air Operations Area, also called the Security Identification Display Area (SIDA), where airplanes are parked. ORL should present a strong security presence as soon as anyone nears the airport property. This can be done through strong fencing, warning signs, the presence of police patrols along the airport boundary, and with airport police and even traffic wardens at the landside or terminal area of the airport. There should be no unlocked or unattended gates that lead into the SIDA. Security should extend to all areas of the airport: fuels, the airport rescue and fire fighting facility (ARFF), cargo, catering, and so forth.
- Increase security measures closer to the highest protected area. Example:
  - In the case of ORL, the TSA has a strong screener presence at the concourse (called the "sterile area" by the FAA/TSA). But additional security measures may require

access control through an access badge and biometric verification system, airport or other sworn personnel on patrol, and frequent security announcements. The highest level of security must be at the SIDA, the area where the planes are parked. This is the equivalent of the highest level of security for a bank being the vault, or for a hospital the central pharmacy.

Taken together, these measures must deter, delay, detect, and deny an adversary from engaging in a criminal act or a terrorist attack.

Security Management

Security management is the concept of not only implementing the measures outlined in this volume but having a total protection program for an agency, department, or company. The goal of security management is: *Determine the threat, identify and reduce risks, identify and reduce vulnerabilities, and protect people, resources, property, and information through a sustained and ongoing process.* Security management is not the total responsibility of an agency or department chief or manager or a CEO or business owner. Security management does not simply mean hiring a contract guard force to protect property. Security management is the implementation and the operation of a sound and complete security program.

A sound and complete security program starts at the top. Whether motivated by the threat of a terrorist attack, the need to protect cash and resources, or the need to protect the public, security management is everyone's concern. Although many agencies and companies will have a director of security or a security chief or manager, that official must have the buy-in and support of the leaders of the agency or company and the acceptance of security measures by the employees and customers.

Many departments, agencies, and companies will not have a security manager but may assign that responsibility to the facilities manager, a building manager, or the human resources manager. It may very well be an additional duty. Security management may not require a dedicated security professional, but we do recommend strong consideration of a full-time professional security manager for particularly high-risk facilities such as medical centers, refineries, transportation centers, and large venues.

To help you either start a security program or improve on your existing program, this section provides a road map for the journey. When considering a security/protective strategy, several management issues must be taken into consideration along with security issues. This section provides a brief overview of the most common issues and includes some valuable recommendations with respect to each.

The Need for Buy-In. Despite the various warnings and the major efforts of the Department of Homeland Security, FDLE, and local law enforcement to make Florida safer, security cannot be the "be all to end all." In other words, security is a supporting function, not the main function (except perhaps for a correctional facility), for your agency, department, or company.

Before September 11, 2001, security was not, in most cases, at the forefront of our national thinking and way of life. Most citizens, if asked, would think of security as being a private security officer at the mall, airport screeners, or a home alarm monitoring company. Security is not the primary function of most organizations; therefore, most employees—and often senior management—do not understand the concept of or need for many security policies and procedures. A major role of those responsible for security in an organization is to educate personnel not only on **HOW** security measures will affect them but **WHY** they are necessary. The audience for this education process is both senior management/decision makers and the general employee population. To some degree it is also important to educate your customers or clients on the need for a strong security program.

Obtaining Buy-In. The means used to achieve buy-in will depend on the culture of the organization as well as the nature of its operational mission. For example, the security program at a nuclear power plant will be very mature and ingrained in everyone who works at the facility. On the other hand, the need for a strong security program may not be so obvious to the owner of a manufacturing firm. In any case, the education process should be relevant to the mission and must be ongoing. One-time security education campaigns generally result in failure. Among the media that can be used for security education are newsletters, e-mails, Web sites, posters, signage, and corporate presentations (at executive committee/staff meetings, company conferences, brown-bag lunches, etc.). Executive/ management buy-in and employee/staff awareness are among the most cost-effective measures that enhance an organization's security posture and can have a tremendous benefit.

Security Systems versus People. A common mistake in both government and commercial organization security strategies is an over-reliance on either security systems or a guard force and the vigilance of the work force to detect and report security incidents. The best approach in almost any environment is to effectively balance the use of security technology (electronic access control, closed circuit television [CCTV], intrusion detection systems, etc.) with a properly trained security force backed by an engaged work force. A security officer force and/or employees with assigned security-related roles and responsibilities provide a very effective complement to security systems and technology.

Coordination and Liaison. Both internal and external liaison are absolutely essential for effective security management within any organization. Among the internal departments that may have an important role or contribution to the organization's security posture are human resources, facilities, legal, safety, logistics, public relations, communications, IT, operations, and transportation. Many organizations form a security working group or similar entity with representation from appropriate departments to serve as a forum for coordinating security-related policies, procedures, and issues. This is an effective way to garner support, obtain buy-in, and gain useful perspectives from other professional specialists.

The group can gather periodically to discuss issues as varied as terrorism preparedness, physical security procedures, emergency plans, workplace violence, information protection, IT security, safety issues, and threat information.

External liaison should be maintained with neighboring facilities/businesses, local law enforcement, other first responders, appropriate federal agencies, and utility companies (gas, electricity, telecommunications, etc.). As appropriate, these external liaison contacts should be included in emergency/disaster exercises and planning sessions for the organization or facility.

Legal Considerations. A wide variety of legal considerations bear on an organization's security policies, procedures, and overall strategy. Among the legal issues most commonly addressed are hiring and employee screening practices, CCTV surveillance policies, privacy issues (including e-mail and computer file access by company/agency officials), and perhaps most important, personal/vehicle inspection procedures. The security strategy and any anticipated changes to it should be carefully coordinated with the legal department as well as senior executives before implementation.

Security Officers/Response Force. A major security budget item for many organizations is the security officer force (or guard force). Two key decisions regarding security officers are: should they be a proprietary force or a contract force, and should they be armed or unarmed?

- *Proprietary.* Proprietary officers are employees of the agency or company they are protecting. The advantage is that these officers have buy-in to their protection role and

are usually long-term employees who become knowledgeable in the facility features and protection measures. Generally they do not cost more than a contract force, except for benefits such as health care, retirement, and other embedded costs. An advantage of a propriety force is that you can conduct more thorough background checks as a condition of employment and they fall under your disciplinary system. One disadvantage is they become perhaps too familiar with employees and may overlook security violations and may not have a neutral view of the state of the facility. Also, with the proprietary force you do not have the flexibility to expand and contract your security posture as the need dictates. You will also incur overtime expenses for nonexempt or wage employees.

- *Contract.* Contract officers are provided by national, regional, and local security force companies such as Guardsmark, Wackenhut, Vance, Allied, Whelan, Intercon, and others. Normally the quality of officer depends directly on your agency requirements and the reimbursement rate you pay the provider. One key disadvantage of contract officers is that they receive low wages, resulting in a high turnover rate which in turn weakens the training they receive. Many states have little or no regulations concerning background checks and training required for contract officers. However, because some, but not all, security firms rely on low margins by paying low wages, they keep their hourly billable rates low to be more competitive. Also, with contract officers you may have different officers assigned to your facility because of high absentee rates. However, you will not pay overtime if an officer fails to show and another officer must remain on that post, as the provider has to pick up that cost. But you may pay premium rates for additional forces on short notice or for holidays.
- *Armed.* This is a critical decision your agency must make. You should consult with your legal department and with the local police department for advice. Generally you should only arm your security officers if there is a likelihood they will have to use deadly force or if a requirement for armed officers exists because of federal law (nuclear power plant security, airport security, etc.). You will need to comply with state law on background checks, firearms qualifications, and the policy on the use of force.
- *Unarmed.* Again, this will be a critical decision because it is not good practice to put an unarmed officer in a high-threat area or where the use of deadly force is likely. You can consider nonlethal options such as using a collapsible or fixed baton (be sure that you know the state law on training with these devices) or arming them with tear gas or Mace/OC spray (again many states have a carry license requirement).

Regardless of whether your security force is armed, unarmed, contract, or proprietary, its value (and others with security responsibilities) is greatly reduced if the individuals do not know their specific roles, duties, and procedures. Such training, both initial and recurring, is of pivotal importance for security personnel. Security officers assigned to an organization should be well trained and required to meet certain minimum training standards. Bear in mind that those standards are a minimum, and often do not fully prepare an individual for duty in a moderate- or high-risk environment. In addition, all security officers should receive specific training and orientation relevant to the organization and facility to which they are assigned. The training should include site and mission familiarization, local procedures, emergency contact information, as well as a thorough background on the organizational culture and the associated security implications.

Post orders are specific instructions for security officers that are used as guidelines for their duties. They should be updated as necessary and reviewed at the beginning of each shift.

Varying schools of thought exist on the advisability of security officers taking on a customer service type of role. That approach works well in some organizations and, if

properly implemented, can contribute to the overall security posture of the environment. This aspect of the security function—no matter how it is defined—should be thoroughly covered during security officer training to ensure that there are no misunderstandings.

Finally, some organizations successfully use nonsecurity employees to augment security functions as needed in high-threat or emergency situations. These additional duty personnel, if properly trained, exercised, and motivated, can significantly enhance security and reduce the workload on regular security forces during short-term surge periods.

Policies

Many experts agree that security begins with sound policies. Policies are developed or approved by senior management officials in an organization and set the standard for a wide variety of issues that relate to the security and asset protection environment. It is prudent for organizations and agencies to maintain up-to-date, written policies on the following subjects, as a minimum:

- Facility security
- Firearms/knives and nonlethal weapons (especially Mace and OC spray) in the workplace
- Drugs and substance abuse affecting the workplace
- Sexual harassment
- Violence in the workplace
- Privacy (personal and electronic, including e-mail communications and computer files)
- Official and personal use of office automation equipment, vehicles, and supplies
- Reporting to work during emergencies (i.e., essential versus nonessential personnel)
- Use and security of wireless communications devices
- Personal safety (on and off the property)
- Travel safety and emergency procedures
- Fraud, waste, and abuse
- Employee assistance.

To be effective, however, policies must be supported and enforced at every level and location of the organization. The policies must also be realistic and practical within the organization's mission, culture, and environment, and adequate resources must be made available to comply with the policies. For example, a strong policy against fraud, waste, and abuse in an organization is hardly effective if there are no mechanisms for reporting allegations, investigating and resolving allegations, and enforcing the policy consistently and fairly. Policy compliance is something that, over time, becomes a part of an organization's culture and, if properly used, can significantly bolster the overall security posture, thereby improving everything from crime prevention to terrorism preparedness.

In addition, employers should recognize the need to establish specific security policies for the protection and security of personnel, facilities, or locations under their control and ensure that they provide a safe working environment. Besides being supported and enforced, the policies must be made known to employees (and other affected individuals) on a regular basis.

Publishing such policies establishes the foundation of the security program and addresses all company or department operating practices including response to crisis situations. The security program requires a fully coordinated approach and must include all levels of the organizational hierarchy. Subject to legal review, employers should consider disseminating security policies widely, including conspicuous posting of certain policies.

Sound security programs and policies deter potential criminal (including terrorist) elements from targeting the organization or facility. They serve as a preventive measure for a

wide range of hostile activities including property theft, industrial espionage, assault, substance abuse, property damage, computer abuse, safety violations, and even terrorism.

Security efforts (particularly manpower) can be costly, but when prudently applied can reap huge dividends in the protection of valuable resources. Ideally, several layers of security controls are used to protect critical resources. In any case, security policies must be practical and enforceable, recognizing the necessity of a prudent balance between security controls and credible risks.

Procedures

Procedures are the next step beyond policies. They translate policies into action and provide specific direction to people in various circumstances. Whether management-related or specific to security functions, policies must be backed by well-defined procedures and enforcement. Care must be taken to ensure that the procedures do not conflict with policies—something that can easily happen as policies and procedures evolve, as organizations grow, or as business practices change.

For security officers, procedures are embodied in their post orders, but written procedures should also be developed for other security personnel and employees at large. Typical topics for security-related procedures may include the following:

- End-of-day area checks
- Evacuation plans
- Computer security procedures
- Use of identification badges
- Access to restricted areas
- Visitor and contractor procedures
- Escort requirements
- Property passes (removal equipment)
- Parking restrictions
- Personal and vehicle inspections
- Public release of information
- Mail/package handling
- Response to emergencies.

Closely related to security is the subject of business continuity. This subject deals with applying security procedures to deal with the results of large-scale incidents such as natural disasters, facility losses, loss of key personnel, communications loss, major computer service downtime (or data loss), and terrorist attacks. It is primarily concerned with the *recovery* aspect of the *prevention, response, and recovery* equation. It attempts to answer the question: how do we get the mission up and running as quickly as possible with the absolute minimum disruption possible?

The development of security policies—and especially procedures—should thoroughly incorporate business continuity as a major factor. Among the measures that should be considered are these:

- Comprehensive contingency plans for credible loss events
- Off-site backup of data (and other critical assets)
- Backup hot sites for computer equipment or other critical systems
- In-place contingency contracts for personnel or services (including security) that may need to be replaced or augmented on short notice.

Procedures should be exercised periodically (in either a full-scale or tabletop setting) to ensure that they are realistic, practical, and do not conflict with one another. The results of these exercises should be documented and used as lessons learned (rather than for placing blame) to ensure that the best possible plans and procedures are in place and can actually be carried out by all personnel. One of the most common lessons learned during emergency procedure exercises is that the communications mechanisms do not work as planned. Therefore, communications should be a key element of any full-scale exercise and should be exercised more frequently than other aspects of the plans and procedures.

Technology and Engineering

The third major element of the security backbone is that of technology and engineering. Technology refers to security systems that can range from the simple (such as key-tumbler locks) to the complex (such as state-of-the-art biometric access controls). Engineering, on the other hand, refers to structural, design, or terrain features that can influence the security or safety posture of an organization, site, or facility.

Security Systems—Major categories of security systems are commonly used in conjunction with and complement one another:

Access Control Systems

This can include any device designed to limit access to a site, building, room, container, or area. Among these devices are standard key locks (including high-security locks), combination (spin-dial) locks, cipher locks (push-button locks that may be mechanical or electronic), card access-control systems (swipe, insert, or proximity), turnstiles, entrapment areas (including mantraps), seals, and biometric controls. An access control process can also be represented by a security officer, a receptionist, or a section employee who checks identification and grants or denies access to an area. Several considerations are involved with access control systems including expense, maintenance requirements, failure/error rate, ease of use, and traffic flow.

Security Surveillance Systems

The most common surveillance system is CCTV, which is offered in a variety of capabilities and sizes. When choosing a CCTV system, consider the intended use of the system as well as technical features such as resolution, image quality, color (ideal for well lighted interior spaces) versus black and white (more suited for low light outdoors), pan/tilt/zoom capability (more complex and expensive), and transmission mode including fiber optic, coaxial, and wireless.

Other considerations include the light level in the area to be covered by the cameras (and possible variations in light level), the need to protect the camera from weather or other elements, the visibility of the camera to observers, and the potential need for multiplexing. A key decision in surveillance strategies is whether to monitor the cameras in real time, record the output, or both. Again the available manpower and intended use of the cameras will aid in those decisions. The technology and configuration of monitors and recorders (analog and digital) is an entire subject in itself. Today, CCTV output can be transmitted over the Internet and monitored in an individual's home or office computer, if necessary. A wide variety of technologies and techniques are available and must carefully fit the particular application, security budget, and other systems in use.

Intrusion Detection Systems

Intrusion detection systems (IDS) can include any system designed to provide an alert of a possible intrusion or a break-in at a protected facility down to the specific room or office. IDSs often are referred to as alarm systems, but may be much more sophisticated such as when they include CCTV tied to the alarm that can show a view of what is happening at the intrusion point. Similar to surveillance systems, a wide array of IDS systems and technologies are available to meet varying needs, applications, and budgets. An IDS generally consists of a sensor component, a transmission medium, and an alert mechanism. Typical sensors in use today include motion sensors (ultrasonic and passive infrared), glass break sensors, contact sensors, and photoelectric beams. Each has particular applications to which it is well suited, and they often are used in concert with one another to protect an overall area.

Special-purpose sensors such as fence tamper and line tamper sensors also may be used. In addition, microwave systems that cover an open area such as an airport runway or buried line sensors can detect movement by vehicle or on foot along a boundary. The next component of the system is a transmission medium that may be wired or wireless. Transmission security and reliability are key issues that must be addressed in the design and maintenance of any IDS. Finally, an alert mechanism may be audible or inaudible (using a lighted display). If the system alert is monitored (which it is in most cases, except for the most rudimentary burglar alarms), consideration must be given to whether to monitor the system on site, off site, or contract with a monitoring service company. Again, each approach has pros and cons. The final decision will depend on the specific application, environment, and security objective.

Although not specifically included in any of the above categories, communications systems form an important aspect of an overall security strategy. Communications systems also cover a wide range of devices and include duress buttons, intercoms (both for emergency help and for access control) security force communications, IDS signal transmission, access control system lines, and CCTV transmission. For certain organizations and applications, the communications system should account for the possibility that the normal telephone system could be down during an emergency situation (either by accident or as part of an attack). One hospital, for example, has its own internal redundant telephone system for such situations.

Engineering Features

A variety of engineering features in both new and existing facilities can contribute to an enhanced security and antiterrorism posture. Some of these features include the following:

- Structural design for new facilities often includes some degree of blast resistance of the design itself, the materials used, or other features such as walls, windows, and doors.
- Retrofit design for existing facilities can include glazing with protective inner glazing to reduce the effect of a blast, Kevlar panels built into walls, stronger window frames to prevent windows from blowing inward, and structural upgrades to prevent floors from collapsing because of explosions.
- The use of concrete and masonry walls in place of fences to assist in deflecting a blast or making it harder to throw an IED over the fence onto property.
- The use of interior and exterior space to reduce large vacant or unused areas that can attract criminal activity.
- The use of natural surveillance by positioning offices and employees where they can see common areas or entries and exits while performing their normal duties.

- Exploiting or creating natural barriers such as berms, ditches, tree lines, dense evergreen shrubbery, and inclines that can offer both an aesthetic and a security (e.g., access control, surveillance, blast protection, obscuration) function.
- Design traffic flow within a site, building, or common area to facilitate security objectives.
- Establish conference areas or other public areas outside controlled space (e.g., at the main entrance/lobby) so that outside meeting attendees do not have to enter the access control point or the main part of the building.
- Design critical or restricted areas near the inner portion of the site or building and away from where visitors or cleared personnel typically traverse.
- Establish a mail and package delivery and screening area separate from the main building or on an exterior wall of the building away from critical or highly populated areas of the facility.
- Coordinate with security professionals in designs for new facilities and upgrades to an existing facility.

Security Costs

One final consideration is that of security costs. Like any business function, the direct and indirect costs of security or protective measures must be taken into account when making decisions. When developing a security strategy or purchasing security systems, consider the following factors:

- Initial purchase cost
- Installation cost
- Maintenance costs (short- and long-term as well as long-term availability of service)
- Technical support (from the manufacturer or third party)
- Periodic (e.g., monthly or annual) service fees
- Expendable supplies
- Support-equipment expenses (e.g., printers, monitors, telephone lines, power, personnel)
- Manpower requirements
- Vehicle requirements
- Office and equipment space needed for people and equipment
- Testing requirements
- System expandability and projected obsolescence
- The impact of a security system or procedure on operations, employees, and visitors
- Costs for consultants and security assessments (internal or external)
- Costs and operational impact of exercises and drills
- Regulatory requirements and the costs to meet them
- Insurance requirements and premiums (increase or decrease)
- Initial and annual training requirements.

"Do not spend 100% of your money to reduce the last 5% of your risk." This means not going broke trying to solve that remaining 5% risk factor. The best security program cannot be risk free.

Funding for security features sometimes can be obtained from other organizational budget lines such as facilities, maintenance, staffing, or general overhead. Although this may be viewed as a shell game by some, it is a legitimate approach to assigning funding sources that benefit or apply to more than one aspect of an organization's operations. It is a common approach in situations where significant expenditures are necessary for enhancing the security posture, but where the security budget may be small or the major portion of the security budget must be allocated to other items.

The best approach for garnering security resources is to view it as a value-added element for the organization's mission. To that end and to the greatest extent possible, security strategies should be integrated and consistent with the mission, culture, and environment of the organization. An effective strategy offers a flexible suite of security measures that can expand or contract according to threat levels and assessment of real-world risks without becoming cost-prohibitive.

Selling Security

- It is required. This may be a factor in a regulated industry such as nuclear power, transportation (airports, seaports, and intercity bus and rail [anticipated]), and oil-gas pipeline. You may be able to sell security simply because it is required.
- It is prudent. Risk management experts agree that security can assist in reducing risk of injury or death to employees, customers, and the public.
- It is cost beneficial. It is possible that liability and indemnity insurance will decline with the installation and use of security systems. Private companies should confer with their underwriters.
- Customers like it. All things considered, customers like a safe place to conduct their business, plan a hotel stay, eat in a restaurant, or shop at a mall.
- It does not have to be ugly. There are many creative designs in security systems, such as discrete CCTV and the use of wrought iron fencing and planters for barriers. There is no reason for the University of Florida dormitories to resemble a maximum security prison.
- It need not be intrusive. Many accept the reason for security, but it need not be intrusive. Except for the most high-risk categories (nuclear power plants, government operations centers, refineries, and chemical plants, for example), security should be built in and be integral to an agency or company operations to the extent possible.
- Security is necessary. Even for the most low-risk facility, given today's unpredictable threat environment, having at least a minimal security plan such as evacuating employees and customers or walking through the parking lot every so often should be considered.

Summary

You have now been introduced to the basic concept of security and the many components that make up a sound security protection program. Although security differs from law enforcement because of its mainly proactive nature versus the more reactive nature of law enforcement, the two are, and should be, mutually supporting.

It is important that facility managers and all officials involved in the security program for the agency, department, or company understand the basic principles of security and the advantages and challenges of implementing a complete facility protection program. We have provided strong but practical suggestions and information on implementing new measures or improving on the existing measures of your facility.

Exhibit 1 to Basic Security Principles

Recommended General Security Measures

Site Measures

These recommendations are derived from multiple security sources. Since needs and resources are often different, every suggestion may not apply to all facilities. Local managers should determine which are appropriate for their facilities and conduct periodic security reviews of their operations to identify needed improvements. The list below contains general security concepts and a few specific examples of how to accomplish them.

General Facility Preventive Recommendations

- Appoint a physical security technician (and an alternate if at a large facility or complex)
- Designate a facility manager
- Create, update, and review security procedures, disaster plans, and operating plans. Keep a backup copy of plan(s) off site (large facilities)
- Train personnel in policies and procedures relative to facility security, i.e., visitor controls, parking, end-of-day checks, bomb threats, suspicious activity, explosions
- Include from the staff, when possible, certified firefighters, biohazard handlers, and/or corporate safety, environment and health personnel, or train personnel in these duties
- Equip members of the team with cell phones/pagers; team should be available up to 24 hours a day, 7 days a week, as appropriate for the situation
- Publish and distribute information and updates about the personnel and response procedures companywide
- Publish an after-action report or incident report after every incident
- Have senior management buy in and sign off on company's security procedures.

Employee Security Procedures

- Maintain good hiring practices
  - — Provide in-depth screening and background checks when hiring new employees
  - — Make arrangements with one or two temporary employment agencies to ensure that a restricted, prescreened group of individuals is available when needed to supplement the work force
  - — Institute and enforce a probationary period for evaluation of employees
- Establish a strict employee identification/personnel security program
  - — Require employees to wear photo ID badges at all times
  - — Instruct employees to challenge any unknown person in a facility
  - — Where provided to employees, use uniforms stitched with names and logos
  - — Provide a separate, secure area for personal items (e.g., coats and purses)
  - — Prohibit employees from taking specified personal items into the main work space
- Establish incoming/outgoing personal mail procedures
- Hire or designate security personnel for mail center area (primarily for large mail centers)
- Establish health safety procedures
- Have on-site medical personnel or arrange for off-site facility/personnel to advise on and respond to a suspected bio-chemical event
- Encourage employees to wash hands regularly, especially before eating

- Encourage employees to see a doctor if suspicious symptoms occur
- Encourage employee attendance at health seminars, talks, and information updates
- As practical, establish or take advantage of company health programs, i.e., shots, check-ups, etc.
- Provide approved personal protection equipment according to Centers for Disease Control (CDC) guidelines.

We recommend consideration of these general security practices. They will provide an improved basic level of protection that you can build on as you embark on your program to improve the overall security of your people, property, resources, and information.

Exhibit 2 to Basic Security Principles
Low-Risk Facility Diagram

The diagram below offers a generic example of possible protective measures and configurations at a low-risk facility. This diagram provides a visual example of placement of physical security features used to protect organizational assets.

The low-risk building has the fewest security measures:

- With its low-risk rating, it requires the fewest number of security measures, particularly costly perimeter sensor systems, automated access control, and extensive CCTV coverage. The building structure (exterior) is the basic protective perimeter for the facility. A low-risk facility would not have significant vulnerabilities or risks and so would not warrant a major investment in security protection systems related to the terrorist threat.

Note: It still may be prudent to install a break-in or burglar alarm system to protect against general criminal threat.

- The concentric or protective rings of security essentially would be the parking lot, the exterior walls, and the entrances. It is prudent to limit the number of access points and to have an employee awareness program regarding who enters and who is in the facility.
- Parking is fairly unrestricted except for around the generator and HVAC system. There is some lighting at the rear of the building because it is not as visible from the highway as is the front. That would assist drive-by police patrols in viewing the rear of the facility. We have not restricted access to the public highway in front of the building. If this were a high-risk facility so close to a public road, we might need to consider restricting commercial truck traffic (because trucks can carry large explosives) from using this segment of the public highway.
- Examples of low-risk facilities might be general government operations that are open to the public such as DMV or driver's license offices, state or county employment security offices, an interstate visitor or welcome center, a retail center, a rural elementary school, or a small corporate office park or campus.

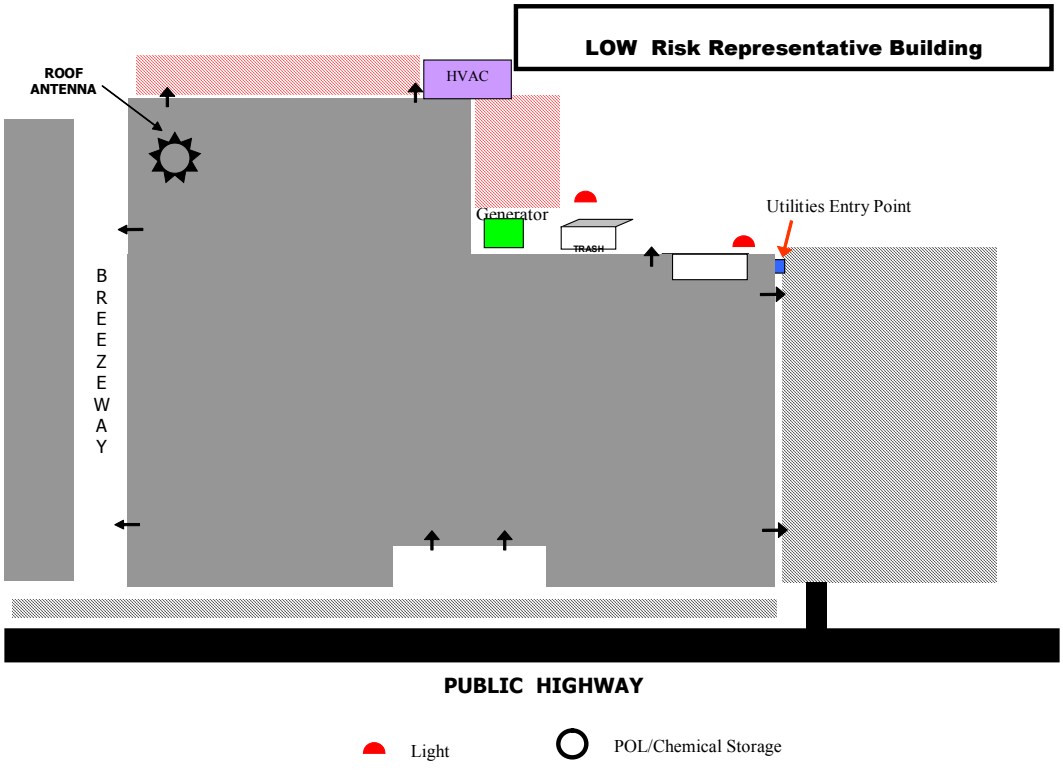


Exhibit 2 to Basic Security Principles

Medium-Risk Facility Diagram

The medium-risk representative facility has several more security measures than the low-risk facility.

- With its medium-risk rating, the facility requires slightly more security measures to reduce its vulnerabilities, which in turn reduces the risk to an acceptable level relative to a terrorist threat.
- Because it is a medium-risk facility, we have included concentric rings of security measures but have not invested in fencing or walls; we will rely on the exterior walls of the facility supported by CCTV surveillance to support the access points. Although we do not have an automated access control system, it is still prudent to have fewer entry points and to ensure that all can be monitored by employees in the facility.
- Parking is somewhat controlled, with some restricted parking near the generator and in the front of the building to increase the set-back distance of an explosive-laden vehicle. Note that we have not restricted access to the public highway in front of the building. If this were a high-risk facility so close to a public road, we might need to consider restricting commercial truck traffic (because trucks can carry large explosives) from using this segment of the public highway.
- Examples of medium-risk facilities might be general government operations centers with restricted public access such as a satellite fire station, a district police station, a highway department solvents/fuel storage area, an urban school, or a corporate headquarters.

Note: It is prudent to install a break-in or burglar alarm system if valuable property and cash are stored in the facility, to protect the facility against a criminal act.

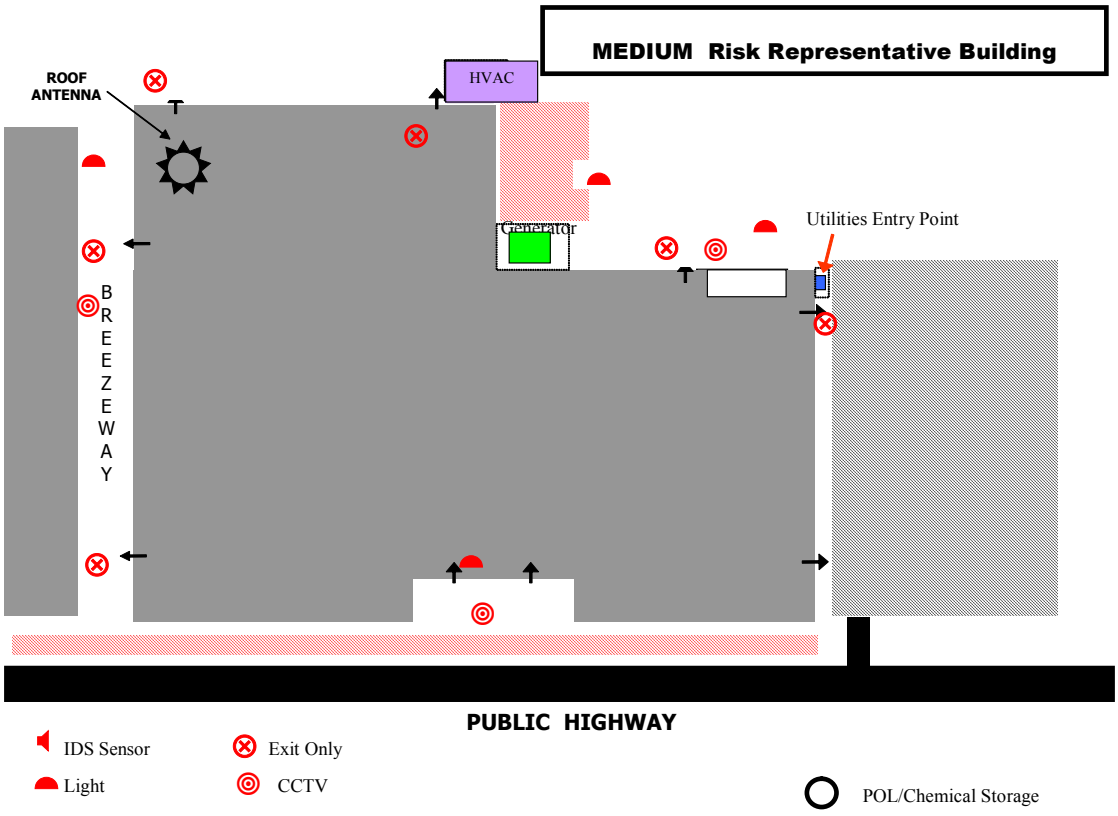
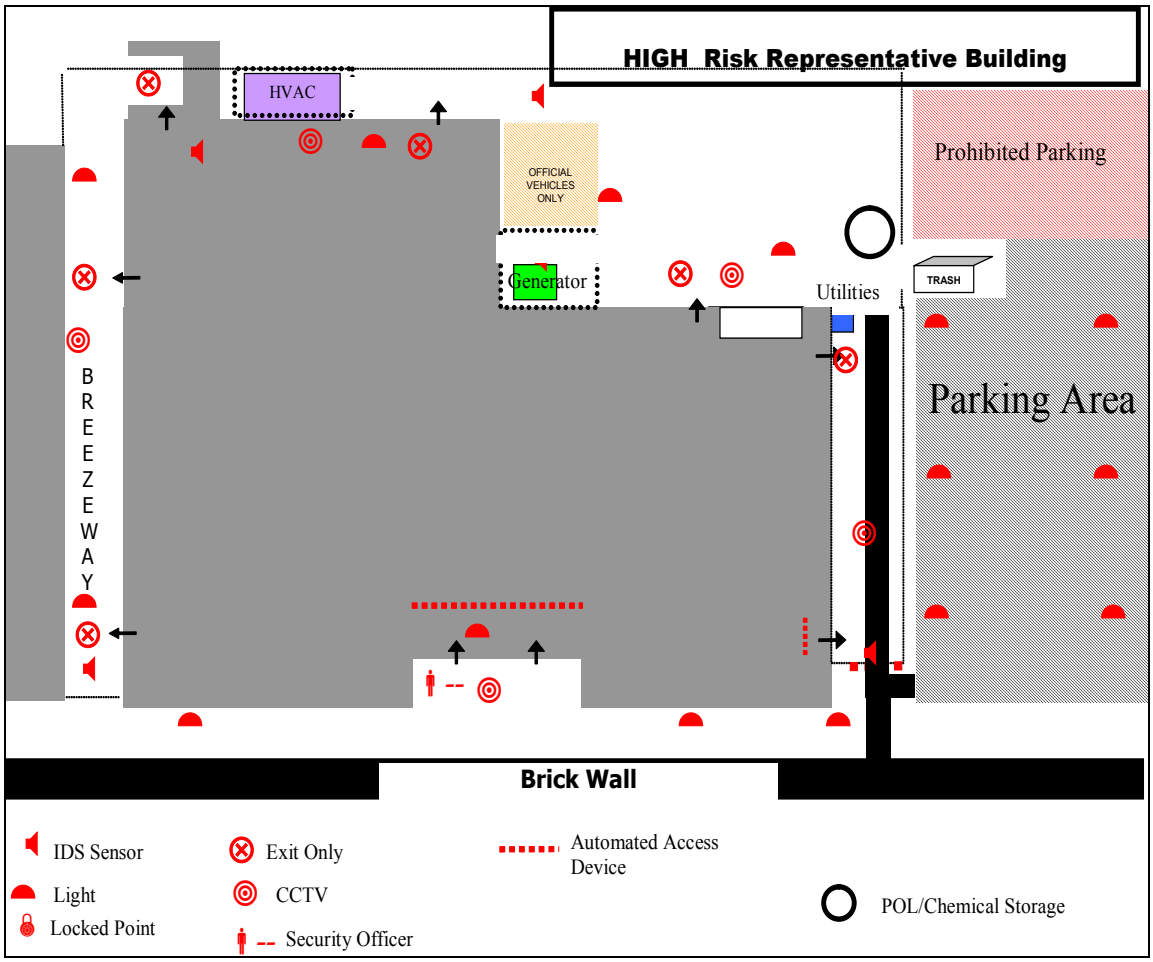


Exhibit 2 to Basic Security Principles

High-Risk Facility Diagram

The diagram below offers a generic example of possible protective measures and configurations at a high-risk facility. This diagram provides a visual example of placement of physical security features used to protect organizational assets.



This diagram shows a high-risk building depicting physical security tools and technologies. The intent is to show how these systems should be used to complement each other and to provide a layered and overlapping security approach to facility protection.

- This high-risk facility has a full array of security measures.
- With its high-risk rating, the facility requires significant security measures to reduce its vulnerabilities, which in turn reduces the risk from terrorist threats.
- Using the theory of the concentric or protective rings of security, we need to protect the innermost areas of the facility, working inward from the perimeter or boundary.
- Each security measure (brick wall, intrusion detection sensors, the security officer, locks, and access control) is designed to deter, detect, delay, and deny an adversarial force from attacking a facility.
- Restrictions on general parking and the use of just one or two entrance points reduce the vulnerability.
- Examples of high-risk facilities would be chemical and biological research and manufacturing facilities or laboratories, critical continuity of government operations centers (public safety, information technology), and university or medical nuclear research facilities.

PART I: BASICS

Chapter 2: Terrorism

The attacks on the World Trade Center on September 11, 2001, (9/11) focused attention on terrorism in a profound way—particularly on the use of weapons of mass destruction (WMD) and a possible campaign of violence against civilians on American soil. While previous terrorist incidents caused increased attention on terrorism, e.g., the bombings at the World Trade Center in 1993 and the Oklahoma City Federal Building in 1995, the response was not on the same scale that we witnessed after 9/11.

The FBI defines terrorism as *"the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political and social objectives."*

At the state level, terrorism has been considered a type of emergency. Many state emergency management and operations plans had terrorism annexes before 9/11; however, 9/11 focused a renewed interest in and concern for their adequacy. The unanticipated and destructive use of commercial jetliners under the control of suicidal terrorists has raised a new awareness of the power and potency of WMD, and potential WMD use in the United States. Public agencies now perceive a heightened need to deal urgently with this newer arsenal of threats, which includes the following:

- Conventional explosives, e.g., dynamite and gunpowder
- Unconventional explosives, e.g., combining chemicals, fuel, and accelerants
- Nuclear/radiological, e.g., nuclear bombs, radiation-releasing devices
- Biological, e.g., viruses, toxins
- Chemical, e.g., poison gases

WMD threats bring characteristics that may be quite different from conventional emergencies. It is both the possible scale of the threat and the differences in the terrorist threat that drive the need to modify existing emergency plans and procedures. Aside from WMD attacks, terrorists can spread fear and chaos throughout the American public with a wide range of options in their arsenal.

Historical Overview

Terrorism has existed for centuries. Initially, it was used in warfare as a method of instilling fear in rival belligerent combatants. However, in the early twentieth century that philosophy was modified and terrorists began targeting the general populace as a means of intimidation and influencing government actions. For many years, the United States was shielded from the levels of terrorist activity that plagued many other nations, such as Israel and Ireland. Our country did not experience the frequency of terrorist acts that occurred in other countries; therefore, it did not implement terrorism protective measures as soon or as fully as they were implemented elsewhere. Simply put, terrorism allows the few to affect the lives of many. Large standing armies are no longer necessary to affect a nation's way of life and political beliefs.

Terrorism Today

Over the past decade, terrorists, both domestic and international, gradually launched and increased their efforts to challenge the U.S. at home and abroad. They discovered and exploited security weaknesses that exist primarily because of the openness and freedom of the American society. Modern terrorists adopted an open target philosophy. This strategy gave them freedom of movement and significantly widened their range of targets. Under

their worldwide approach to target selection, terrorists have been able to complete their destructive missions successfully with little likelihood of interdiction or immediate capture.

Terrorists are becoming more adept at choosing high-profile targets, planning attacks, obtaining sophisticated weaponry, and using improvisation to conduct missions. More attacks, including the use of WMD, on the United States can be expected.

Organizational Structure of Terrorist Groups

- Currently, 28 organizations are on the State Department list of Designated Foreign Terrorist Groups, and 15 organizations are listed as "other terrorist groups." Many of these organizations specifically target American interests and maintain cells and/or sympathizers within the United States. In addition, a number of domestic terrorist groups, activist groups, and militias may represent a terrorist or terrorist-like threat to Americans. These are the commonly recognized domestic and international terrorist groups:
  - *Domestic.* Domestic terrorist groups are groups that are based in the U.S. and can be further characterized as:
    - *Extreme right-wing groups.* These groups disagree with the current state and direction of the U.S. government on taxation and our role in the United Nations and international peacekeeping, and they often espouse racial segregation and white supremacy. Usually these groups are very small and not organized into cohesive elements, i.e., state to state. The most notable example of terrorist association with a right wing cause was the l995 bombing of the Murrah Federal Building in Oklahoma City. Although not linked to an organized domestic terrorist group, that event was linked to two disaffected former Army soldiers with some support from fringe elements. Such groups, many with training camps, have existed primarily in Montana, Idaho, Arkansas, and Missouri. The FBI has had much success in breaking up these groups since the mid l980s. However, a neo-Nazi element still exists in many portions of the United States.
    - *Extreme Environmentalist Groups.* Groups such as Earth First! and select elements of the Animal Liberation Front oppose technology, the use of forests and natural resources to support modern society, any and all use of animals for experimentation, and in some cases the use of animals to support our diets (cattle, fowl, and fish). Eco terrorists have burned down ski resorts, set fire to new SUVs, and inserted spikes into trees to sabotage the lumber industry. They also have been linked to arson against university research laboratories.
    - *Anticapitalist Groups.* These groups strongly oppose major corporations and the international corporate presence in the Third World. They have aligned themselves with other left-wing groups to protest the International Monetary Fund (IMF) and the World Bank and effect change with their lending policies to Third World Nations. A very few self-described anarchists have resorted to violence and damage to property during anticapitalist demonstrations. Seattle and Washington, D.C., have hosted IMF and World Bank conferences and have experienced widespread demonstrations and incidents of violence.
  - *International.* These terrorist groups can be state sponsored or transnational.

    Al'Qaida/Qaeda. This group is the most recognizable terrorist group because of its direct involvement in the planning and execution of the multiple attacks on the United States on September 11, 2001. Al'Qaeda also has been linked directly to U.S. embassy bombings in Africa, the USS *Cole* attack, the bombings in Bali, Indonesia, and the attempted missile attack on an Israeli charter airliner. Experts believe that Al'Qaeda is funded through and led by Osama Bin Laden, an expatriate member of a wealthy Saudi family, and through donations from third-party, Islamic-based

charities. Al'Qaeda is an extreme Islamic fundamentalist group that opposes U.S. forces and presence in the Middle East and U.S. support of Israel.

- *Hamas and National Popular Front for the Liberation of Palestine.* Although these groups operate primarily in Palestine and have engaged in suicide bombing attacks in Israel in the past 2 years, they are terrorist groups that have the potential to bring their fight to the United States. In past years, radical terrorist groups have existed in Lebanon and Egypt, two nations frequented by U.S. citizens and tourists. Groups in Egypt have targeted tourists groups at popular tourist areas to bring discredit on the Mubarak government. Although less frequented by Americans, Iran, Iraq, Yemen, and Algeria remain areas of concern as well. Recent terrorist activity in Kuwait has been directed against U.S. forces and personnel in that nation.
- *Latin America Groups.* Except for Colombia, terrorist activity in Central and South America has abated somewhat. Although there is significant crime in Mexico City and kidnappings occur there with great regularity, experts attribute this to an active criminal element and some corruption in the Mexican law enforcement ranks. However, some breakaway separatist groups operate in the southern regions of Mexico. The oil-rich nation of Colombia, however, continues to experience significant terrorist activities by anti-government forces. Terrorist activities in Chile have abated somewhat and were directed primarily against the government of Chile.
- *Spain.* The Basque separatist group often engages in terrorism in the northern regions of Spain. It has targeted official government organizations such as police and military forces, but also has bombed government sites and buildings. There have been few American deaths and injuries, mostly in tourist areas.
- *Greece.* In Greece, the 17 November left-wing terrorist group was broken up recently by Greece's national police force and its leaders were arrested. Although many believe the government looked the other way for quite some time, experts believe that planning for the 2004 Olympics in Athens spurred that nation's police and security forces to take action against this group.
- *Turkey.* Experts remain concerned about the presence of Dev Sol and other Kurdish separatist groups operating in eastern Turkey (where Turkey borders Iraq and Syria). In the past, these groups have targeted U.S. forces and facilities in Turkey to discredit to the Turkish government and to strain relations with the U.S.

International terrorist organizations generally are dedicated to a cause and are well trained, well organized, and well resourced. Generally, they are organized into several small independent groups or cells with leadership elements managing each cell. This commonly-used security practice lowers the likelihood of significant impact on the organization's goals if individual cells are discovered or compromised. International terrorists typically practice excellent security measures including protecting communications modes, limiting knowledge of specific operations to a small group of individuals, compartmentalizing sensitive information, laundering funding sources, conducting countersurveillance, and changing base locations frequently. Terrorist groups often are divided into cells that have a functional organization similar to the following:

Terrorist Cells

- *Planning*—selects targets and times for attacks
- *Surveillance*—collects relevant details about sites and activities
- *Administrative*—develops credentials, obtains travel documents, etc.

- *Funding*—raises funds and funnels monies
- *Logistics*—obtains and transports explosives and/or weapons
- *Operations*—conducts attacks.

The recruitment and training of terrorist operatives are security sensitive. Ethnically-based terrorist groups recruit new members personally known to them, people whose backgrounds are known, and who often have family ties to the organization. Intelligence penetration of organizations recruited in this way is extremely difficult. Among groups that are not ethnic- and religion-based, the usual sources of recruits are high school and college students who show commitment to a cause.

The level of training varies considerably among groups. Those with military experience or who have received advanced training at sophisticated facilities are the equal of some state security forces. At the other end of the spectrum are the expendable operatives who get little more than inspirational talks before being activated. Typical training includes instruction in the use of small arms and explosives, intelligence collection tactics, and indoctrination. Often, as with suicide bombings, the instruction may be for only a few hours.

Domestic terrorists or activist groups may select a government or public facility as a symbolic target. By attacking a symbolic target, the group may be able to hit a soft target but have a major impact. Examples would be bombing the Statue of Liberty, the Gateway Arch in St. Louis, Missouri, or a state capital building.

Although some activist groups may not actually be officially considered terrorists, they possess the ability and intention to disrupt operations or damage public sector assets. Examples of these groups may include radical environmental activists, labor or antilabor extremists, or loosely organized groups objecting to global trade relationships/monetary policies. Some groups, such as the Earth Liberation Front (ELF), have recently been designated as domestic terrorist organizations by the FBI.

Many domestic group goals exhibit characteristics indicative of a traditional terrorist operation, such as the following:

- Operating small, loosely connected cells rather than using a highly centralized command structure
- Maintaining anonymity among cell members or using what the military calls a compartmentalization approach, so that one member does not know what another is doing
- Claiming credit for well-publicized acts
- Using inflammatory language in communiqués and public statements
- Using terrorist tactics such as firebombing and arson.

Capabilities and Tactics

Historically, 85% to 90% of terrorist attacks against American targets have involved bombings. Based on increased technical capabilities and on the recent extensive coverage of unconventional attacks, the likelihood has increased for more exotic forms of future terrorist activity.

For target selection and potential attack modes, the possibilities are virtually endless. For instance, a terrorist group may opt to attack petroleum products and chemicals at a port operation because they represent a lucrative and dramatic potential target. Typically, ports lack security measures for most shipments, including those involving dangerous, hazardous, and toxic cargo. Judging from the fall of 2002 sniper attacks in the Washington, D.C. area, terrorists conducting similar sniper attacks across a city, region, or the entire country could cause widespread panic and potentially halt a significant portion of U.S. retail trade.

The figure above shows the array of methods used by terrorists, protesters, gangs, insiders, and others, and the weapons and actions they may take against a facility and personnel. It is designed to show the possible methods of attacks so that you can plan accordingly.

The growing sophistication of international terrorist groups and their extensive use of information technology may increase the possibility of cyber attacks against American critical infrastructure targets. Several foreign countries, including some known to have supported terrorist groups in the past, are establishing and developing dedicated offensive information operations capabilities.

The possible use of chemical, biological, radiological, and nuclear (CBRN) weapons must be considered when planning for preventing or mitigating the effect of a potential terrorist attack. A direct CBRN attack could be mounted against a variety of targets within Florida. Materials to support such an attack could be smuggled into the state, just as drugs, weapons, and contraband have been in the past.

Defining the Threat

In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis reviews the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the protective measures provided by law enforcement, security officers, or other community assets. A threat analysis is an essential step in identifying the probability of terrorist attacks.

Elements of the federal and Florida governments, as well as local and Regional Domestic Security Task Forces, assess the threat posed by various terrorist groups and issue notices on known tactics, weapons, tools, explosives, organization, and likely targets.

The most likely, potential adversary or aggressor and the tactics and weapons, tools, and explosives that might be used in carrying out an attack against Florida's critical infrastructure or public facilities are listed below. National terrorist threat information and crime statistics support the identification of these potential threats.

Figures 1 and **2** show the typical tactics and weapons used by terrorist groups and criminal elements and the transport method they will likely use. These figures provide useful information about the potential methods and weapons a hostile force may use for attacks.

Tactic	Terrorists	Protestors	Gangs	Insiders	Others
Vehicle bomb	✹				
Placed bomb	✹			✹	
Mail bomb	✹				
Ballistics	✹		✹	✹	
Fire bomb	✹				
CBRN mail	✹				
Water contamination	✹			✹	
HVAC contamination	✹			✹	
Murder	✹		✹	✹	✹
Assault	✹	✹	✹	✹	✹
Hostage	✹	✹[1]	✹	✹	✹
Kidnapping	✹		✹		
Vandalism	✹	✹	✹	✹	✹
Arson	✹	✹	✹	✹	✹
Civil disobedience		✹			

[1] Refers to holding facility hostage

Figure 1. Potential Tactics for Each Adversary

Tactic	Weapon	Tool
Vehicle bomb (moving and stationary)	20,000 pounds TNT	60,000 pound truck
	1,000 pounds TNT	5,000 pound truck
	500 pounds TNT	4,000 pound car
	220 pounds TNT	4,000 pound car
	50 pounds TNT	4,000-pound car
Placed bomb	50 pounds TNT	NA
Mail bomb	2 pounds TNT	NA
Ballistics	7.62 mm	NA
	.44 Magnum	NA
	.38 Special	NA
Fire bomb	Glass bottle with gasoline and wick	NA
CBRN mail	Airborne pathogen such as anthrax	NA
CBRN mail	Chemical or radiological poison	NA
Water contamination	Water borne pathogen	NA
Water contamination	Chemical or radiological poison	NA
HVAC contamination	Airborne pathogen such as anthrax	NA

Figure 2. Weapons and Explosives

United Front

American citizens will not be able to eradicate terrorism; however, they can certainly protect themselves and deter terrorists from striking.

Combating terrorism involves two sets of actions to oppose terrorism: antiterrorism (defensive measures) and counterterrorism (offensive measures). Antiterrorism is defined as "defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local and military forces." Counterterrorism involves those offensive measures taken to prevent, deter, and respond to terrorism. Counterterrorism programs, which will not be addressed here, are classified and addressed in various national security decision directives, national security directives, and contingency plans. The general objective of combating terrorism programs is to neutralize terrorist groups. As in most stability and support operations, neutralization in this context means rendering the source of threat benign, not necessarily killing the terrorists. In antiterrorism, the objective can be further refined to focus on preventing attacks and minimizing the effects of an attack. Antiterrorism includes any action to weaken the terrorist

organization and its political power and to make potential targets more difficult to attack. Counterterrorism includes spoiling action, deterrence, and response.

Unity of Effort

Interagency action is required to combat terrorism; unity of effort provides ways to integrate the actions of various responsible agencies of federal, state, and local governments. Intelligence is particularly important and sensitive. It is a key to successful interdiction efforts and ultimately to combating terrorism at all levels. The dissemination and sharing of information gained through intelligence gathering and countersurveillance efforts at all levels are essential to thwarting terrorist plans and ultimately to decreasing the frequency and impact of terrorist acts.

Unfortunately, it is easier to recommend unity of effort than to achieve it. In circumstances where multiple law enforcement agencies have vague and overlapping charters and jurisdictions, conflict and inefficiency will likely occur. As in other aspects of stability and support operations, the solution typically lies in negotiation and cooperation. Fortunately, experience has proved that cooperation at the local level is relatively easy to obtain, especially between smaller agencies and facility managers.

Patience and Persistence

Antiterrorism efforts require much patience and certainly is contrary to American norms, as most Americans typically are impatient and expect instant results. Deterrence is a tool whose effectiveness is impossible to measure, so a properly-designed antiterrorism campaign likely will have little recognition for a job well done—success is very hard to measure. For example, if no attacks occur, it could be because no threat was pointed at a particular resource or because the protective measures were very effective. Remember, it was 8 years between the first attack on the World Trade Center and the second, but more devastating, attack.

Conclusion

The war against terrorism will be a very long, arduous struggle. There are no clear boundaries, no lines in the sand, and no clear enemy or target. Terrorism is a new challenge for America. Fortunately, our nation has faced many uniting challenges in our history, from natural disasters to world wars. Terrorism requires a united, firm, but measured response. Together, if we remain vigilant and are proactive in developing protective strategies, we will prevail—as we always do.

PART II: MANAGEMENT

Chapter 1: Roles and Responsibilities

Introduction

This chapter outlines the roles of the key managers, subject matter experts, and support personnel and of employees and customers in a comprehensive security program. Every individual at all levels in the organization plays an important role in the effort to protect, detect, assess, and respond to acts of terrorism. The roles and responsibilities are identified to provide a deeper understanding of them and to serve as a guide for the American anti-terrorism campaign.

Executive Level: Agency director or department manager (public facilities) or chief executive officer (private infrastructure)

Responsibilities:

- Sets the goals to protect, detect, assess, and respond to a possible terrorist act and to reduce the consequences
- Supports the vulnerability assessment process through encouragement and empowerment of team members
- Based on the findings and consistent with sound financial principles, supports the budget requests and capital improvement necessary for implementation
- Oversees the project from beginning to end
- Ensures that progress reviews, follow-up reviews, and action plans are completed
- Principal advocate to either cabinet-level or executive-level officials (public) or to the boards of directors, shareholders, or governing boards (private infrastructure).

Operations Level: Division manager or chief (public facilities) or chief operating officer or manager (private infrastructure)

Responsibilities:

- Develops and refine goals and objectives in support of the business security plan
- Communicates with upper-level management on all matters relating to security incidents or threats
- Maintains security awareness of policies, procedures, and business environment changes that affect the organization
- Maintains and ensures that department manuals relating to security measures are up to date
- Coordinates departmental meetings with appropriate levels of management
- Represents the department at meetings and conferences
- Maintains statistics and quarterly and annual reports to assess the quality of work and the department's progress relative to the overall security plan
- Prepares and approves the departmental budget, then submits it to upper-level directors
- Maintains departmental records
- Coordinates security goals and objectives with subordinate managers and supervisors.

Agency/Department or Corporate/Company Security Adviser or Director of Security

Responsibilities:

- Manages the agency security program
  - — May be a full-time position or an additional duty for a person at a smaller agency

- Develops sound security practices through professional education, training, and possibly membership in recognized security associations
- Provides written procedures to ensure that all security requirements are met
- U.S. government contractors must comply with the Defense Security Service's *National Industrial Security Program Operations Manual* (NISPOM)
- Regulated industry (oil/gas pipeline, nuclear energy, public transportation, aviation, banking and finance, Food and Drug Administration [FDA]-regulated and Department of Agriculture-regulated) must ensure compliance with the Code of Federal Regulations (CFR) and public law
- Processes security clearances for required contracts or conducts background and "due diligence" checks
- As allowed by state law, conducts criminal history, fingerprint, and credit history checks
- If required, conducts a more extensive background check to include "friends and neighbors" interviews and checking reference and previous employers
- Manages key and lock control program
- Provides guidance on information controls (e.g., document security)
- Manages the administrative security requirements for the facility
- Inspects security systems such as locks, keys, gates, and doors
- Manages the use and maintenance of lights, barriers, access control, alarms, and other physical security requirements
  - The security manager or director may contract this out, but will remain responsible for the overall security program
- Develops security procedures
- Manages a security officer force where required
  - Determines if best to have a proprietary security force or a contract force
    - May depend on the policies and procedures of the jurisdiction's human resources and civil service policy
    - Determines if the security officer force will be armed
    - Determines "post and patrol" requirements
    - Establishes policy and requirements for both proprietary and contract officer force
- Coordinates and maintains liaison with the director of security or the security coordinator on physical security matters, including participation in working groups and committees
- Establishes procedures for sharing threat information in a timely manner through law enforcement, security, or intelligence channels
- Formalizes security procedures for appropriate response to contingencies
- Develops physical security threat assessments and updates them annually or as needed
- Coordinates regional sharing of threat information
- Forwards threat assessments to appropriate department heads
- Encourages establishment of agreements between agencies for mutual support against terrorist incidents (that is, sharing intelligence and coordinating terrorist threat conditions)
- Implements security education and training programs.

Line: Agency/department branch supervisors and managers (public) and company division or branch supervisors and managers

Responsibilities:

- Assist the security manager in educating and motivating employees to support the security program
- Enforce the rules concerning security practices and procedures such as end-of-day checks, protection of information, reporting suspicious events, and maintaining passwords as needed
- Communicate issues and concerns of the employees and customers to the security director and operational level managers
- Address issues of security as they impact bargaining unit or labor union local concerns
- Support the efforts of the vulnerability assessment team

Building Managers and Building Engineering and Maintenance Technicians

Responsibilities:

- Maintain current riser and as-built diagrams for structural; environmental; heating, ventilation, and air conditioning (HVAC); communications; power, water, and sewer to assist in the vulnerability assessment and security upgrades
- Comply with current environmental health and safety standards
- Prepare and maintain an emergency evacuation program including frequent evacuation drills, to assist the security manager/director and the supervisors
- Ensure that the facility is functioning properly, coordinate any necessary repairs, and permit only authorized access to critical areas of the building—HVAC, power generation, boilers, information technology (IT) and hub router closets, communications rooms, emergency generators, and fuel storage
- Assist in the development of a security threat assessment and share it with authorized team members and agency/department officials
- Share with other agencies/departments/companies best practices and solutions
- Coordinate state agency efforts or private sector efforts with utility providers in support of utility restoration
- Establish procedures for providing support to and requesting support from other local agencies, in coordination with the security director and management, in the event of a terrorist incident
- Encourage establishment of agreements between agencies for mutual support against terrorist incidents (that is, sharing intelligence and coordinating terrorist threat conditions) in the public sector and, in the private sector, become involved in private security associations
- Coordinate security procedures pertaining to the physical plant (buildings, storage tanks, approach roads, general property features) for appropriate response to contingencies
- Assist in maintaining personnel and property protective measures against trespass, terrorism, sabotage, theft, arson, and other illegal acts
- Provide the level of security required based on a thorough assessment
- Assist with the assessment of the vulnerability of the building, including construction and physical layout, geographical location, social and political environment, and attractiveness of assets to current threats

- Work with security director or coordinator and public safety and law enforcement officials to disseminate information regarding potential threats
- Maintain current telephone list of all critical employees
- Ensure that emergency communication systems are maintained
- May have responsibility for planning and maintaining an identification card program
- Working with security officials, determine the need to install permanent or temporary barriers and sign plans and write guidelines for receiving deliveries
- Working with the appropriate security officials, or if no security official is assigned, coordinate emergency responses among local, state, and federal law enforcement agencies
- Working with the appropriate security officials, or if no security official is assigned, ensure that a perimeter and building lighting plan provides adequate lighting levels for the safety and security of employees
- Assist the security official in establishing a building parking plan to be used during increased threat levels
- When directed, oversee personnel, package, and vehicle inspections
- Ensure that building utilities are properly protected from unauthorized access
- Assist security, or when directed, create a "zone plan" as deemed necessary to control vehicle traffic and employees entering the site
- May be assigned the responsibility of implementing company established guidelines for background checks (however this typically is done by either the security coordinator or human resources department)
- May be assigned responsibility for installation and maintenance of an intrusion alarm and detection system and a closed circuit television (CCTV) system
- Prepare for and have a plan to safely secure the facility if warranted
- Protect, maintain, and restore critical transportation routes into the facility
- May be responsible for activating or using a card access control system
- Evaluate the need to limit site access by closing gates and entrances
- Working with the security director and the vendor (or proprietary locksmith), ensure that locks meet National Fire Protection Association (NFPA) and local and federal application standards for safety
- In coordination with the security director, ensure that emergency evacuation plans are current and tested regularly
- In coordination with security or support (administrative) department manager, ensure that adequate precautions are made for securing and screening mail
- In coordination with the security department or agency managers, plan for and maintain a contingency command center
- In coordination with security or appropriate managers, protect and when there is an official need, provide building plans to local, state, and federal officials
- Maintain response and recovery plans; coordinate with emergency response teams
- Take measures to protect the facility from weapons of mass destruction (WMD)
- Ensure that communications testing is conducted
- Participate in information dissemination meetings

- In coordination with the security manager and the chief information officer (or appropriate official), maintain adequate IT and threat warning plans
- Ensure that the facility has provided for emergency backup power
- Ensure that measures are taken to secure doors and windows from explosive devices
- Coordinate security officer contracts and requirements for the facility based on their knowledge of the building structure, grounds, and physical features with the security director or manager including contingency planning.

Employee

Responsibilities:

- Becomes familiar with security procedures
- When required, wears identification pass or badge
- Cooperates with necessary hand-carried items checks at entry points
- Maintains security awareness and attends security awareness training
- Instructs other employees to wear their badges and ensures that they report lost or missing badges
- Does not allow unauthorized entry or access to non-badged personnel in restricted areas, particularly tailgating or piggybacking at access control points
- Reports any suspicious items, persons, or vehicles on the site or in the building
- Immediately reports a bomb threat or suspicious device as directed
- Follows building management's guidelines for emergency evacuation
- If assigned as an evacuation warden, ensures that employees know evacuation routes and assists personnel in the evacuation sector
- Ensures that the work area is checked for suspicious items or individuals upon arrival and at the end of the work day
- Maintains measures to secure IT and computers from unauthorized access
- Ensures that all building plans or reports relating to facility security plans are secured in locked file cabinets or safes
- Follows building management guidelines for prenotification control, and escort of visitors
- Secures company keys and access cards from unauthorized use
- Does not disclose facility security information to individuals who do not have a "need to know"
- Reports inoperative or malfunctioning security protection systems, such as lighting systems, to building management for repair.

Customer or Visitor

Responsibilities:

- Understands the necessity for security, particularly for critical facilities and public venues
- When requested, wears visitor identification pass or badge
- Cooperates with necessary hand-carried items checks at entry points
- Maintains security awareness.

As you embark on your plan to conduct your vulnerability assessment, it is important to know who needs to be involved and their roles in the effort. This chapter provided you with a complete outline of the "players" and their responsibilities and contributions to the vulnerability assessment of your facility. Although we emphasize that security is everyone's responsibility, we recognize that you will have a core group of professionals and experts to support your security program.

PART II: MANAGEMENT

Chapter 2: Security Policies

Introduction

A basic knowledge of general security principles and policies is important as the vulnerability assessment of your facility, site, or building begins. Some organizations have limited experience with security, others have extensive experience.

Regardless of the maturity of the security programs, a review of this section serves to introduce general security principles or refresh users with some knowledge of them.

The Basics

Well-developed policies provide direction and boundaries for procedures or decisions to be made. Policies are necessary as an overarching tool to give direction in establishing methods and procedures. To develop prudent security policies, agencies should establish and organize bodies of decision makers to review and approve security policies periodically.

Security programs and policies are designed to deter both criminal and terrorist elements from conducting hostile operations or espionage against facilities, buildings, sites, or public venues and to reduce the opportunity for destruction or theft of critical assets or information. The approach to security programs should be designed around a threat-based scenario.

Security Council

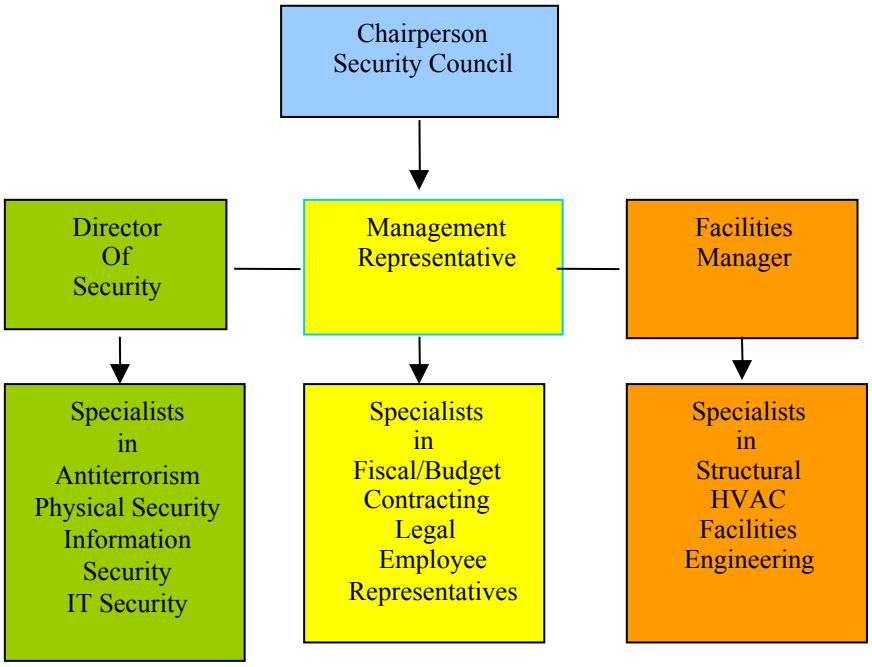
Because of today's threat environment, the establishment of a security committee or council is becoming more common in nonregulated industries and in state and local governments. Once the exclusive province of the military and the federal government, and in select regulated industries (nuclear power, oil/gas pipeline, banking and finance, and transportation), agencies, departments, and companies are now establishing their own security councils (SC) or committees.

This trend has become more prevalent because security concerns in business, government, and industry are ever present, and a united front is essential to implementing sound security practices and policies. Forming an SC also makes good fiscal sense because it promotes cost-effective solutions to security challenges. The SC uses local threat assessments in developing security policies because the threat assessment forms the basis for all security planning and considers all threats to assets. Ideally, SC membership includes senior personnel at the executive level. Subordinate agencies or facilities should be organized under a centralized SC to ensure that adequate security practices are developed and implemented and to facilitate rapid dissemination of threat warnings.

SC Core Elements

- Appoint a chairperson, typically a senior or deputy organizational leader
- Identify senior-level multifunctional team members
- Include other essential functional experts regardless of their management level (e.g., budget analysts, contracting officers, antiterrorism advisers)

Listed below are the recommended members for your company, agency, or department SC. These team members will assist you in both immediate and long-term security program management and coordination.



SC Charter

- Establish security policies
- Review threat warnings
- Direct protective measure implementation
- Approve/disapprove security proposals
- Oversee subordinate security or threat working groups (TWG)

The SC should meet at least once every 6 months to review and address security issues. The SC should also meet upon declaration of an increased state of security or threat level.

SC Responsibilities

- Document each security concern
- Appoint a responsible party to act on and track the progress of each security concern
- Follow up on open items at each meeting and conduct a quality control check to ensure that actions taken meet the SC's intent
- Review threat and vulnerability information
- Review and approve:
  - Security enhancements
  - Prioritized critical asset lists
  - Security policies, especially those regarding access control procedures
  - Security practices and physical security programs
  - Procedures for public events (e.g., open house)
  - Crises response procedures
- Appoint subordinate working groups to address specific needs:
  - Threat Working Group (TWG): Chartered to prepare the threat vulnerability assessment based on crime analysis, loss statistics, assessment of high-risk facilities, and other data and to advise on implementing crises response procedures
  - Physical security working group: Normally composed of law enforcement representatives, engineers, communications specialists, and representatives from agencies requiring enhanced security protection such as fences, automated access control, or intrusion detection systems

TWG

A subordinate element to the SC, the TWG is made up of as few as three or as many as 25 people, depending mostly on the complexity or size of the agency, department, or company. This group focuses on developing and facilitating implementation of SC mandates and daily reviews of threat information.

Charter

- Provides departments with a single focal point for coordinated all-source threat analysis for protection decisions
- Conducts daily threat reviews to recognize the diverse nature of Florida assets and the varied threat potential
- Regularly reviews and monitors departmental security enhancement efforts

The TWG regularly confers with agencies across the agency or department and subsequently reviews and evaluates security proposals or concerns. The private sector will be limited because federal, state, and local law enforcement and intelligence agencies cannot share sensitive law enforcement data with the private sector.

The private sector could work closely with local, state, (especially the Regional Domestic Security Task Force [RDSTF]) or federal agencies to obtain threat or intelligence data. They may also subscribe to private organizations that analyze and disseminate threat and intelligence data.

The TWG formulates ideas, considers short-, mid-, and long-term possibilities, while remaining cognizant of low- and high-cost solutions or procedural measures to reduce vulnerabilities to resolve open action items. For proposals requiring policy and guidance, the TWG researches or develops documents and submits them to the SC for approval.

Core Security Policies

Once the governing SC is in place and understands its purpose, it should direct development of a core security document to serve as the foundation of the security protection program. This document, at a minimum, does the following:

- Includes an inventory, in order of importance to safety of life, prevention of injury, and necessity to support key economic activity, of all critical assets (people, property, resources, and information)
- States the security responsibilities of personnel working in controlled areas
- Specifies controlled areas to be established pursuant to public law regarding trespassing or federal mandates
- States that controlled areas for the private sector be established pursuant to the law concerning protection of private property and for employee, customers, and visitor safety
- States that all personnel must obtain written permission to enter controlled areas
- Designates controlled areas by describing their location and noting that they are marked with warning signs
- Establishes entry and internal controls for all controlled areas
- Grants or restricts entry into the site and authorizes inspections of certain items
- Establishes roles and responsibilities
- Explains information and threat warning dissemination
- Identifies the need for procedural development (e.g., access control procedures)
- Specifies development of protection plans.

When the core security document is available, appropriate policies are developed and operational procedures are implemented based on these policies.

This brief chapter recommends that you form an SC for both short- and long-term security needs. It advises on member selection for the SC as well as their roles and responsibilities.

PART II: MANAGEMENT

Chapter 3: Risk Management

Introduction

Risk management (RM) is a tool used to make balanced and objective decisions after careful consideration of existing or anticipated conditions and vulnerabilities. Security RM allows leaders to review their security program and implement cost-effective mitigators to reach an acceptable risk level. Many RM methodologies exist, offering a range of techniques and processes.

Risk avoidance, a model used by security professionals to address security in the past, focused only on *preventing* loss or damage without reference to the degree of risk. In contrast, risk management does the following:

- Identifies weaknesses in an organization or system (such as a water system, electric power grid, or building)
- Offers a rational and defendable method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valuable assets
- Improves the success rate of an organization's security efforts by emphasizing the importance of communicating risks and recommendations to the final decision-making authority
- Helps security professionals and key decision makers answer the question: How much security is enough?
- Prevents spending 90% of a budget to reduce the final 1% of risk.

This document helps managers consider security reviews or risk assessments by providing guidance on how to review those assessments for thoroughness. Essentially, the RM model is a threat-appropriate response. The following sections define the terms used in the RM cycle and describe the basic steps of this cycle. Whether an organization plans to conduct RM itself or hire a company to do it, the assessment should follow the steps in this guide.

Simply stated, RM is a systematic and analytical process by which an organization identifies, reduces, and controls its potential risks and losses. This process enables organizations to determine the magnitude and effect of the potential loss, the likelihood of such a loss occurring, and countermeasures that could lower the probability or magnitude of loss. Alternative countermeasures should be identified and evaluated to select those which offer an optimal trade-off between risk reduction and cost. Organizations should seek an "acceptable" level of risk that reflects the best *combination* of security and cost.

Terms

Risk is a function of assets, threats, and vulnerabilities. These terms are defined below.

- *Risk* is the potential for an unwanted event to occur. Examples of unwanted events range from loss of life or injury (the high end of risk) through loss of information, money, organizational reputation, to unauthorized access to a computer system. Risk is a function of the likelihood of the unwanted event occurring and its consequences; therefore, the higher the probability and the greater the consequences, the greater the risk. The likelihood of the unwanted event occurring is based on threat and vulnerability.

- *Threat* is the capability and intention of an adversary to undertake actions that are detrimental to an organization's interests. Threat is a function of the adversary only; it cannot typically be controlled by the owner or user of the asset. However, the adversary's intention to exploit his capability may be encouraged by vulnerability in an asset or discouraged by an owner's countermeasures. Countermeasures can also reduce the consequences of a threat.
- *Vulnerability* is a weakness in an asset or countermeasure that can be exploited by an adversary or competitor to cause damage to an organization's interests. The level of vulnerability, and hence the level of risk, can be reduced by implementing appropriate security countermeasures.
- An *asset* is anything of value (e.g., people, property, resources, and information, including hardware, software, facilities, reputation, activities, and operations). An organization needs assets to carry out its mission. The more critical the asset is to the mission, the greater the consequences of its damage or destruction. An example is the loss of a company's central gas pipeline that carries refined products from Jacksonville to Orlando. It would significantly reduce that company's ability to provide refined oil products to a major metropolitan area in Florida. The loss would have greater consequences if it occurred during a critical operation or if the company did not have economically feasible alternative means to move its product to Orlando.
- *Countermeasures* are actions or devices that mitigate risk to assets, threats, or vulnerabilities. This manual suggests countermeasures to reduce vulnerabilities.

Several useful tools are provided, with no endorsement of any RM process intended. Common to all models, however, is a shared philosophy acknowledging the fact that, to make an informed decision, certain factors must be assessed. These factors are assessed in a six-step process.

After each assessment step, a review is conducted to determine if the information may have an impact on previous steps. This RM technique is an iterative process—the process is ongoing and the information garnered may be interrelated.

Step One—Asset Assessment

In the first step, managers must inventory their assets and the consequences associated with the loss of critical assets. An assessment of each asset should reveal the net replacement cost, political impact of loss, and loss consequence affecting overall operations. A macro-level perspective is usually easiest for defining categories of assets. Typically, there are four categories:

- *Property:* Buildings, warehouses, storage areas, and land
- *Information:* Computers, documents, software, patents, etc.
- *Resources*: Vehicles, furniture, merchandise, utilities, etc.
- *People*. Except when traveling, people generally are considered part of the three categories listed above.

Employees at all levels should be an integral part of identifying and prioritizing assets. Functional experts can quickly identify the potential impact of loss of or damage to an asset.

After assets are prioritized in each category, the "cost" of loss is assessed.

Step Two—Threat Assessment

This step identifies potential threat categories and types of viable adversaries. When compiling the list of adversaries, review their intent and motivations to determine the likeli-

hood of attack. In addition, assess their capabilities in terms of knowledge, skills, and abilities. While history often reveals much about an organization, do not exclude adversaries simply because they have never attacked a certain type of facility or have not used a certain tactic before. Terrorists and criminals regularly change their approach so that their activities are not predictable.

Surveillance is a common tactic used by most terrorists and criminals (especially when it is an inside job). Adversaries review in-place security measures to determine potential vulnerabilities that they could exploit. Even the best security systems, if not installed properly or not maintained well, have vulnerabilities that terrorists can exploit. Managers must review the security system from an integrated perspective and determine if the vulnerabilities are significant enough to cause concern after reviewing the asset value and potential threats.

Threat assessments are a subjective undertaking and can be highly speculative unless a reliable intelligence system is available. Even with the best intelligence networks and systems, threats often materialize without warning; therefore, this element of the RM process is of most concern.

Continuous intelligence gathering and analysis is critical to effective security. Working closely with intelligence and law enforcement agencies will typically provide a more thorough understanding of how to plan and implement adequate protective measures. These experts should assist by furnishing counterintelligence information related to the security threat. They should evaluate any intelligence information regarding the intentions and capabilities of hostile elements.

This analysis considers current local, regional, and international factors bearing on the security threat to likely resources. It stresses the known capabilities of hostile elements to damage, destroy, or impede the planned use of company assets. You should include information concerning all threats from all sources, including the local criminal threat. If precise information is not available, base the analysis on reason and logic. The relevant threat information must be evaluated and synthesized by intelligence experts and subsequently divulged to managers.

The motivations of people to do harm, damage property, or steal are key elements to understanding categories of threats other than environmental. Once you understand the motivational aspects (the psychology of the behavior), then you can begin to select and implement protective measures to thwart potential acts. These threats are divided into four categories for ease of identification and discussion:

- *Environmental.* Includes natural events such as tornadoes, earthquakes, hurricanes, and storms as well as man-made events such as hazardous material (HAZMAT) and chemical spills. Natural threats can be as unpredictable as and often more devastating than the act of a terrorist or criminal. An earthquake, for example, can strike without warning and may trigger a chain of events resulting in severe damage to critical assets. A chemical spill near a highly congested area can cause panic among residents, workers, and even emergency response units if they are not well trained to handle such an event.
- *Criminal.* Business espionage, theft, vandalism, violence, harassment, kidnapping. Criminal acts generally are categorized as motivated by greed or violence, which is often the result of mental imbalance. Criminal threats are fairly unpredictable, often even more unpredictable than a terrorist threat, unless the perpetrator is observed conducting surveillance before the event. A disgruntled worker who uses harassment or commits violent acts can also be classified as a criminal.
- *Insider.* Theft, divulging or losing information, violence, harassment. Passive insiders assist others in perpetrating a criminal act. They may provide information or ignore a

required procedure, such as locking a door. An active insider is one who actively participates in destruction, violence, or theft.

- *Terrorist.* Bombs, WMD, kidnapping, assassinations, violence. Terrorists typically are motivated by political or religious beliefs, but may steal to finance their operations. Ultimately, their intent is to gain public attention and change the political will of a government.

Once the type and motivation of the adversary are identified, the potential impact can be interpreted. The next step is the assessment of the vulnerabilities of assets and how the adversaries might exploit these vulnerabilities.

Step Three—Vulnerability Assessment

Managers are strongly encouraged to conduct or direct a vulnerability assessment at least every 1 to 2 years. With the publication of this Manual and given today's threat environment, agencies, departments, and the private sector should consider conducting their initial vulerability assessments as soon as possible. Managers can then evaluate vulnerabilities identified based on existing threats and determine the level of risk versus recommended corrective actions.

Step Four—Risk Assessment

Use formal risk assessments to validate increases or decreases in security personnel requirements, changes in security operations and procedures, and security equipment and system upgrades needed to reduce unacceptable risks.

Step Five—Identify Mitigators

Mitigators are measures that can be taken to reduce the impact of an event. They are commonly called countermeasures because they involve actions or a physical device to reduce vulnerabilities. In the *Terrorism Protection Manual*, mitigators are referred to as protective measures.

Step Six—Decision

Upon completion of steps 1 through 5, managers apply a holistic, integrated systems approach to implementing actions to detect, delay, and deny potential terrorist acts. Managers consider each of the previous steps in their decision-making process and formulate a reasonable approach to securing assets while still conducting business, if possible.

This chapter introduced you to the concept of RM, which is a key part of your overall security program. RM is a technique to ensure that you are protecting your property, resources, people, and information. It allows you to make balanced and objective decisions as you consider your current threats and vulnerabilities. Risk will always exist to a certain extent; the object is to reduce it to an acceptable and manageable level.

PART II: MANAGEMENT

Chapter 4: Threat Levels

This section explains the United States Department of Homeland Security (DHS) supported by Presidential Decision Directive-63, which promulgated threat levels. Using a graduated scale, managers are advised to take specific actions as the threat increases.

The measures outlined later identify recommended minimum level of actions. Managers should localize these measures as their threat dictates. They may take more stringent actions to mitigate the local threat. If managers cannot achieve specified actions, they should request advice and direction.

The chart on the right is derived from the DHS and is referred to as the Homeland Security Advisory System. Each of the five threat levels is identified by a description and corresponding color. From lowest to highest, the levels and colors are as follows:

Figure 1. Homeland Security Advisory System

The following threat levels represent an increasing risk of terrorist attacks:

Low (Green) is declared when there is a low risk of terrorist attacks.

Guarded (Blue) is declared when there is a general risk of terrorist attacks.

Elevated (Yellow) ***is the baseline minimum for the state of Florida and is defined as normal***. An Elevated Level is declared when there is a significant risk of terrorist attacks. The measures in this level must be able to be maintained for weeks without causing undue hardship, affecting operational capability, or seriously aggravating relations with local authorities and the community.

High (Orange) is declared when there is a high risk of terrorist attacks. ***In Florida, this level is defined as increased (security preparation and vigilance)***. Implementation of measures at this level, for more than a short period of time, may create hardship and affect the normal activities of the agency and its personnel.

Severe (Red) ***is the level at which a terrorist attack is considered imminent for the state of Florida and requires swift, decisive, and immediate protective measures***. Under most circumstances, the protective measures for a Severe level are not intended to be sustained for substantial periods of time. This level usually is declared as a localized condition.

State Level

The decision to publicly announce threat levels is made on a case-by-case basis by the governor in consultation with the Florida Department of Law Enforcement (FDLE) commissioner, chief of domestic security, and regional domestic security task forces. Every effort should be made to share as much information as possible regarding the threat, consistent with the safety of the state. The commissioner ensures, consistent with the safety of the State, that local government officials and law enforcement authorities are provided with the most relevant and timely information. The commissioner is responsible for identifying any

information developed in the threat assessment process that would be useful to state and local officials and others and conveying it to them as permitted, consistent with the constraints of classification. The commissioner establishes a process and system for expeditiously conveying relevant information to federal, state, and local government officials, law enforcement authorities, and the private sector.

The FDLE commissioner also ensures that a continuous and timely flow of integrated threat assessments and reports is provided to the governor and other state designees. Whenever possible and practical, these integrated threat assessments and reports are reviewed and commented on by the wider interagency community.

Threat Levels

The decision on which threat level to assign includes many considerations. This combination of factors relies on qualitative assessment, not quantitative calculation. Higher threat levels indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that at any given threat level a terrorist attack will not occur. An initial and important factor in determining threat level is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

- To what degree is the threat information credible?
- To what degree is the threat information corroborated?
- To what degree is the threat specific or imminent?
- How grave are the potential consequences of the threat?

These terms, definitions, and recommended security measures are intended to facilitate interagency coordination and support of U.S. antiterrorism activities. Selection of the appropriate response to terrorist threats in the public sector remains the responsibility of the agency director or manager and, in the private sector, the responsibility of corporate or company officers or managers having jurisdiction, control, ownership (fiduciary responsibility), or control over the threatened facilities or personnel.

The world has changed since September 11, 2001. The nation is still at risk for terrorist attacks and will remain at risk for the foreseeable future. All threat levels require vigilance, preparedness, and readiness to deter terrorist attacks.

You now have the official threat levels as developed by the U.S. DHS and recognized by the FDLE. These are the levels to use in determining the protective measures of your high-, medium-, and low-risk facilities.

PART II: MANAGEMENT

Chapter 5: Threat Planning

Introduction and Purpose

In applying a deliberate risk management approach to the issue of facility security, a threat assessment is a key element. This chapter provides a brief overview of threats relevant to Florida public facilities, private infrastructure, and public venues. It incorporates a general overview of the potential range of threat-specific environmental factors at public and private facilities that may influence the threat posture.

Included are postulated threat scenarios and baseline planning assumptions that contribute to a comprehensive view of the threat. Because of the dynamic nature of the threat and evolving security enhancements, a site-specific threat assessment and trend analysis should be conducted annually.

This chapter presents threat considerations that provide a basis for subsequent vulnerability assessment and recommendations for enhanced protective measures and strategies for the state of Florida's public facilities and private infrastructure. Potential, probable, and most likely threats will be addressed relative to the state.

Threat Assessment Considerations

A thorough assessment of terrorism and security-related threats relies heavily on the consideration of various underlying factors. Two of the basic considerations are: a) the potential targets of attack, and b) the sources of the various threats. These two considerations will be addressed as general categories. The table below illustrates these considerations and indicates in general terms the asset categories that may be targeted by various threat sources.

Threat Sources and Their Most Common Target Categories

Target	Radical Islamic Terrorist Groups	Domestic Eco-Terrorist Groups	Domestic Extreme Right Wing	Domestic Anti-Capitalist Groups	Other International Terrorists
People	Very High Impact: Government employees and others in high symbolic government facility High Impact: General population working in or near high symbolic government facility	Very Low Impact	Very High Impact: Government agency employees High Impact: Media representatives Low Impact: General population working in private sector facilities	Extremely Low Impact: (except possible collateral damage to government) World Bank, World Trade Organization, International Monetary Fund or global corporate facilities	Medium Impact: All population groups Activities confined primarily to U.S. targets overseas
Property	High Impact: Property destruction as a by-product to cause mass casualties	High Impact: Property damage is the prime objective	High Impact: Government agencies Low Impact: Private property (Except Jewish related)	Medium to Low: These groups generally conduct vandalism and disruptive demonstrations only	Medium Impact for all property

Target	Radical Islamic Terrorist Groups	Domestic Eco-Terrorist Groups	Domestic Extreme Right Wing	Domestic Anti-Capitalist Groups	Other International Terrorists
Resources	High Impact: As collateral damage	Very High Impact: As collateral damage	High Impact: As collateral damage	Medium to Low: These groups generally conduct vandalism and disruptive demonstrations only	Medium Impact for all resources
Information	Medium Impact: As collateral damage	Medium Impact: As collateral damage	Medium to Low Impact: As collateral damage	Medium to High: Disrupting IT systems is an effective way to cripple organizations	Medium to Low Impact: As collateral damage

Although terrorism was explained in more detail in Part I: Basics, Chapter 2, the information displayed above is about the most typical terrorist groups (or minimally, groups that use the methodology of violence to influence political thought or change) and their likely targets that you need to consider in your overall threat planning approach.

Planning Scenarios

Planning for terrorist threats can be supported by reviewing postulated scenarios. Such scenarios can provide ideas to security planners and test (in a tabletop manner) the current procedures and assumptions on which the security strategies are based. The following scenarios are provided for that purpose. They are not based on any known or specific threat information but rather on techniques and approaches that may be used by terrorist elements.

Scenario 1

General criminal. A recognized, organized crime group recruits an employee in the IT section of the State Technology Office to serve as an informant. Its motivation is money and it entices the newly hired IT worker with large sums of money to take undue advantage of inside information. Later, the organization convinces the insider to expand the activities into collecting specific information and manipulating computerized information in the system. The organization threatens to expose the employee's misdeeds and harm the insider's family if his or her support for the organization diminishes.

The organized crime group now develops ties with a Tampa-based cell of an international terrorist group. The organized crime group offers the services of its insider to the terrorist cell.

Insider information is later used to target and car-bomb key technology facilities.

Scenario 2

An international terrorist group determines that a dramatic event needs to take place and that the northeast sector of the United States is becoming "old news" as a terrorist target.

It chooses Florida as a target, specifically Tallahassee and Miami. Its intent is to disrupt the banking and financing and communications sectors by targeting communication distribution systems of each. It conducts surveillance of two facilities and subsequently uses explosives smuggled through the Port of Miami to conduct near-simultaneous attacks.

Scenario 3

With tightening security controls at airports and land borders based on threat information received by law enforcement agencies, an international terrorist group decides to use the Port of Jacksonville as its primary shipment point into the United States.

The group establishes relations with a long-standing drug cartel with an operation in Somalia and uses its services to get small amounts of biological toxins, supplies, and money into the United States via the Port of Jacksonville.

The group begins to develop its own mechanism, including a network of insiders at the port, so it can eventually break away from its reliance on the drug cartel. To minimize resistance by potential supporters, it poses as a drug cartel. Eventually, it establishes an "import" system that it can use at any time via containerized cargo shipments.

Meanwhile, another cell of the terrorist group identifies several strategies to attack agriculture products in warehouses across the state of Florida.

These scenarios represent the possibility of postulated threats assessed as the following:

- Outside terrorist groups acting alone
- Outside terrorist groups with planted insider knowledge and assistance
- Outside terrorist group with coerced insider knowledge and assistance
- Outside terrorist group with novice insider knowledge and assistance
- Planned insider attack by disaffected employees, customers, vendors, or criminals.

These groups or individuals must be considered in the threat assessment. Coupled with information of the suspected domestic and international terrorist groups, it is possible to minimally determine the type of group that might pose a threat.

Antiterrorism Plan

Planning is critical to deterrence, detection, defense, and response to terrorist incidents. The antiterrorism plan should clearly describe site- or building-specific antiterrorism measures and should stress proactive techniques and resources to thwart terrorist attacks. The antiterrorism plan can be part of an existing plan, but, at a minimum, should include the following:

Key Plan Elements

- Terrorism threat assessment
- Vulnerability assessment
- Risk assessment
- Terrorism protective measures
- Incident response actions
- Consequence management measures

To carry out the state's roles and responsibilities and to maximize federal assistance in emergency response situations, substantial local government or agency resources and plans/procedures should be in place. The addition of terrorism and WMD to the existing emergency management context introduces a number of new considerations. The strategies in existing plans may need to be adjusted for characteristics such as scale, lack of lead time, crime scene management, and other issues. The need for special transportation and other agency responses may have to be considered (evacuation other than for a natural disaster, mass inoculations, etc.).

Managers may determine that, under certain threat conditions, they need to impose access controls and other security measures to protect critical assets or all assets. For example, after September 11, 2001, the Pentagon expanded its security zone well beyond the federal boundaries and still restricts all commercial truck and bus traffic, using the Virginia State Police, on two major arterial roads that run along the east and west sides of the Pentagon complex.

In the exhibit following this section are several elements that should be included in an antiterrorism plan and that should be published by the responsible agency owning or leasing the sites or facilities that have been scored, to prepare for acts of WMD terrorism. The appropriate governing agency (as determined by FDLE) should prepare an antiterrorism plan based on the elements identified below. Managers should safeguard their antiterrorism plans with a "For Official Use Only" label and should not post them on a public Web site.

Exhibit 1 to Management Planning
Antiterrorism Plan Outline

Copy No._____ **Issuing Agency**_____

Place of Issue_____ **Date of Issue**_____

Purpose: State the plan's purpose
Area Security: Define the agency sites or facilities (assets) placing priority on those assets scored as high.
Access Restrictions: Define and establish restrictions on access and movement into critical areas. Categorize restrictions to personnel, materials, and vehicles.

1. Personnel Restriction
   a. Authority for access
   b. Criteria for access
   c. Employees
   d. Visitors
   e. Contractors
   f. Vendors
   g. Emergency responders
   h. National Guard
2. Material Restrictions
   a. Requirements for delivery and acceptance of material and supplies
   b. Search and inspection of delivered materials and mail for possible sabotage
   c. Special controls on delivery of supplies or personal shipments in restricted areas
3. Vehicle Restrictions
   a. Policy on search or inspection of departmental and privately owned vehicles, parking regulations, controls for entrance into restricted and administrative areas, particularly underground garages
   b. Departmental vehicles
   c. Private vehicles
   d. Emergency vehicles
   e. Vehicle registration

Countermeasure: Indicate the manner in which the following countermeasures will be implemented for the site or facility.

1. Protective barriers
   a. Definition
   b. Clear zones
   c. Criteria
   d. Maintenance
2. Signs
   a. Types
   b. Posting
3. Gates
   a. Hours of operation
   b. Security requirements
   c. Lock security

4. Barrier Plan
   a. Permanent
   b. Fixed, but adjustable
   c. Portable
5. Protective or security lighting system
   a. Use and control
   b. Inspection
   c. Action taken in case of commercial power failure
   d. Action taken in case of failure of alternative power source
6. Emergency lighting system
   a. Stationary
   b. Portable
7. Intrusion Detection System
   a. Security level of the facility
   b. Inspection
   c. Use and monitoring
   d. Action taken in case of alarm conditions
   e. Maintenance
   f. Alarm logs or registers
   g. Tamper-proof provisions
   h. Monitor-panel locations
8. Communications
   a. Locations
   b. Use
   c. Tests
   d. Authentication
   e. Backup

Security personnel: General instructions that would apply to all security personnel. Detailed instructions such as special orders and procedural information should be attached as annexes for more detailed instructions.

1. Security personnel include:
   a. Composition and organization
   b. Length of assignment (watch or duty shift)
   c. Essential posts and patrol routes
   d. Weapons and equipment
   e. Training
   f. Authority and responsibility
   g. Enforcement policy
   h. Challenging methods to a suspect
   i. Integrating with the local incident command system

Contingency planning: Required actions in response to various emergency situations. Detailed plans for situations (e.g., counterterrorism, bomb threats, WMD event, hostage negotiations, disaster, and fire).

PART II: MANAGEMENT

Chapter 6: Training

Benefits of Training

From a systems approach, it is most beneficial to analyze all security aspects and subsequently design an integrated system, of which an effective training program is a key component.

Based on the need to enhance security and counter potential terrorism, a tailored training program should be developed, implemented, and evaluated. A training program should be easily adaptable as threat conditions, technology, and regulations change and it must be tailored to any unique needs.

An effective security training program educates and motivates employees to be aware of risk. By increasing their awareness and offering methods of response to crisis events, employees are better prepared to identify potential risks early, thereby providing a better opportunity to thwart or mitigate risks. Reducing the risk of loss of personnel and assets is an incalculable outcome.

Successful Training Programs

Terrorist protection requires all levels of the organization to be visibly and actively involved, from the executive to the individual worker. *Involvement must be a priority*. An effective program requires alignment throughout the organization and full integration into existing operating procedures, specifically from initial hiring of new employees, where it is part of the orientation and new hire training, to offering annual incentives and rewards. Human resources, the training office, the safety office, facility and department managers, and working groups offer opportunities to educate and motivate employees. These actions will keep the program functional and viable.

Educational Process

To properly implement a new program, managers must recognize the importance of training and of securing employee buy-in. This section briefly outlines the basics of the educational process to assist users in implementing an integrated learning approach to security. Based on the Instructional Systems Design (ISD) concept, there are five core elements to the educational design process: analyze, design, develop, implement, and evaluate (ADDIE).

- *Analyze* the needs of the organization and the individual learner in terms of desired security knowledge and motivation for learning.
- *Design* a system or approach to incorporate and meld required and desired knowledge into a useful educational experience.
- *Develop* techniques and tools, such as tailored lesson plans, guidebooks, handouts, visual aids, demonstrations, stories, activities, examples, questions, group discussions, brochures, bulletins, and textbooks.
- *Implement* a well-prepared, rehearsed educational campaign.
- *Evaluate* what you accomplished. Conduct a top-to-bottom review with workers, educators, managers, and anyone else associated with the venture. This step is crucial to continuous improvement and assists with future student/worker buy-in.

Using ADDIE: From a teaching perspective and to maximize program effectiveness, a holistic approach should be used to optimize security training. The five steps of the ADDIE system are briefly outlined below.

Step 1: Analyze the Problem

- Collect data relevant to the problem
- Conduct group collaboration
- Use problem-solving tools.

Step 2: Design a Course of Action

- Form a threat working group
- Identify goals and objectives
- Outline potential problems and corrective measures
- Review existing programs
- Select an approach.

Step 3: Develop an Integrated Program

- Develop a learning contract with employees and students
- Select training modules
- Tailor lesson plans to the students
- Schedule and coordinate activities.

Step 4: Implement the Program

- Prepare the environment
- Conduct media campaign
- Deliver instruction.

Step 5: Evaluate Top to Bottom

- Conduct learner assessment
- Conduct educator assessment
- Conduct support assessment.

Overcoming Common Problems in Training Delivery

For organizations that are initiating a training program and plan to use individuals who do not have much experience in providing training, the following information may be useful. Malcolm Knowles, author of the *Adult Learner*, explains that, although instructor-led training is still the most popular training method when compared to other options such as CD-ROM and learning, most beginning trainers are not well prepared to teach.

A study was conducted with novice and expert trainers to identify problem areas and solutions. The data noted 1,098 training delivery problems that novice trainers face. The problems were categorized into 12 areas within three basic categories:

- Those pertaining to the trainer
- Those describing how the trainer relates to the trainees
- Those pertaining to presentation techniques.

The major differences between novices and experts are knowledge and experience. Because experts have a broader knowledge base than novices, they solve problems in a dif-

ferent manner. Experts have more focus, recognize cues that allow them to recall chunks of information, and are better able to integrate and interconnect knowledge.

After careful analysis of the 1,098 problems, methods were proposed for handling them, and "Expert Solutions to the Twelve Most Common Training Delivery Problems of Novice Trainers" was developed. While the solutions provide useful tips, nothing replaces practical experience. The bottom line is that novice trainers require both knowledge and podium time. Employing competent trainers results in educated and motivated students.

Training is an important element of your overall security program assessment and implementation of a strong protection plan for your facility. It may be necessary to train participants before embarking on this effort. This chapter has given you a method for conducting this training.

Exhibit 1 to Management Training
Solutions to Training Problems

1. Fear
   - A. Be well prepared
   - B. Use icebreakers
   - C. Acknowledge the fear
2. Credibility
   - A. Do not apologize
   - B. Have the attitude of an expert
   - C. Share personal background
3. Personal Experiences
   - A. Report personal experiences
   - B. Report experiences of others
   - C. Use analogies, movies, or famous people
4. Difficult Learners
   - A. Confront problem learners
   - B. Circumvent dominating behavior
   - C. Organize small groups for timid learners
5. Participation
   - A. Ask open-ended questions
   - B. Plan small group activities
   - C. Invite participation
6. Timing
   - A. Plan well
   - B. Practice, practice, practice
7. Adjust Instruction
   - A. Know group needs
   - B. Request feedback
   - C. Redesign during breaks
8. Questions
   - A. Anticipate questions
   - B. Paraphrase learners' questions
   - C. "I don't know" is okay
   - D. Ask concise questions
9. Feedback
   - A. Solicit informal feedback
   - B. Conduct cumulative evaluations
10. Media, Materials, Facilities
    - Media
      - A. Know equipment
      - B. Have backups
      - C. Enlist assistance
    - Material
      - A. Be prepared

- Facilities
  - A. Visit beforehand
  - B. Arrive early

11. Openings and Closings
    - Openings
      - A. Develop an "openings file"
      - B. Memorize
      - C. Relax trainees
    - Closings
      - A. Summarize concisely
      - B. Thank participants
12. Dependence on Notes
    - A. Notes are necessary
    - B. Use cards
    - C. Use visuals
    - D. Practice

These suggestions will ensure a successful training program.

Exhibit 2 to Management Training

Sample Lesson Plan

Intent and Use

The sample lesson plan depicts the typical depth and level of instruction that managers should expect of their training staff. The lesson plan requires the designated instructor to possess antiterrorism knowledge at the intermediate level to explain terms, general concepts, terrorist organizational structure, and typical capabilities and tactics. Of equal importance is the need for instructors to have significant teaching skills, not just presentation skills, to lead students to an understanding and appreciation of their roles in an effective security program.

This sample lesson plan is designed to give you a methodology for planning a training class on a variety of issues related to your facility's security and ensuring that your agency, department, or company has a complete training program.

Antiterrorism Lesson 1

Introduction to Antiterrorism

OBJECTIVE: Identify basic terrorism/antiterrorism facts and terms.

Lesson: Using the elements of attention, motivation, and overview, introduce the subject of terrorism/antiterrorism.

Antiterrorism Exercise	
Introduce yourself and provide a cameo of your professional experience. Introduce activity. Have participants introduce each other.	Working in pairs, have participants introduce each other and find out their experience with antiterrorism. Also have them discuss what their goals are for the class and what they expect to do when they return to their workplace.
Lesson Topics	**Presentation Material/Methods**
1. Background ✹ World Trade Center, New York City – February 29, 1993 ✹ Alfred P. Murrah Federal Building, Oklahoma City – April 19, 1995 ✹ Khobar Towers, Dhahran, Saudi Arabia – June 25, 1996 ✹ Embassies in Dar es Salaam, Tanzania, Nairobi, Kenya – August 7, 1998 ✹ USS *Cole*, Aden, Yemen– October 13, 2000 ✹ World Trade Center, the Pentagon, and Pennsylvania (airplane crashes) – September 11, 2001	
2. Terrorism ✹ Is the use of force or violence against persons or property for purposes of intimidation, coercion, or ransom in violation of the criminal laws of the United States? ✹ Most terrorist incidents in the United States have been bombing attacks involving detonated and undetonated explosive devices, tear gas, and pipe or fire bombs ✹ The effects of terrorism can vary significantly from loss of life and injuries to property damage and disruption of services such as electricity, water supply, transportation, and communication	

Lesson Topics	Presentation Material/Methods
3. Categories of Terrorism in the United States ✸ *Domestic terrorism*—Involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction ✸ *International terrorism*—Involves groups or individuals whose terrorist activities are foreign-based or directed by countries or groups outside the United States or whose activities transcend national boundaries	
4. General Information About Terrorism ✸ Absolute protection against terrorism is impossible ✸ Terrorism can occur in peacetime or in conflict ✸ Terrorism often consists of acts to intimidate governments or societies to obtain objectives ✸ Terrorism is performed to meet political, religious, or ideological objectives ✸ Terrorism is or can be used to: — Overthrow governments or economic systems — Retaliate against U.S. foreign policy — Impede U.S. ability to wage war or build up for war ✸ High-risk targets include any place with a large concentration of U.S. personnel	
5. Characteristics of Terrorist Operations ✸ Carried out by specially trained and organized underground elements called cells ✸ Previous surveillance of target to exploit vulnerabilities ✸ Acts of terrorism are usually directed against specific targets in the general population and government ✸ Terrorist operations are characterized by violence, speed, and surprise	
6. Terrorist Goals ✸ Immediate goals — Obtain recognition for cause — Expose government's inability to protect citizens — Demonstrate power or threat credibility — Impact elections, free prisoners, obtain money or equipment, economic disruption ✸ Long-range goals — Cause dramatic changes in government — Turn the flow of events to their side — Gain political recognition	
7. Terrorists Characteristics ✸ *Crusaders*—Ideologically inspired hard-core individuals or groups. ✸ *Criminals*—People who commit terrorist acts for personal rather than ideological gain ✸ *Crazies*—Mentally ill people who commit terrorist acts during a period of mental disturbance	
8. Terrorist Methods ✸ *Bombs*—May be of any degree of sophistication—pipe, letter, package, car bomb — Placed to destroy property — Cause casualties and death ✸ *Ambush*—Attacks by an individual or small groups, using small arms to assassinate important persons in or outside of government ✸ *Armed attack*—Initiated with diversionary actions — Aimed at key personnel or critical resources — The objective is to cause disruption of mission and adverse publicity ✸ *Hostage seizures*—Undertaking to seize a specific: — Hostage for ransom or political bargaining purposes — Critical asset when personnel are present. Used for bargaining for publicity and political advantage ✸ *Sabotage*—Internal or external means used to destroy resources or weaken ability to counter terrorist activities	

Lesson Topics	Presentation Material/Methods
9. Bomb Recognition/Indicators ✹ Mail bomb — Heavy, soiled wrapper — Bulky, envelope — Crude handwriting with misspelled words — Excess postage — No return address — Protruding wires — Has a general address ✹ Pipe bomb — Constructed of metal or plastic — Capped at both ends — Wires may or may not be visible	
10. Leader Actions and Responsibilities ✹ Establish cordon and evacuate nonessential personnel. Cordon size determined locally ✹ No radio transmissions within 500 feet of the affected area ✹ Do not touch the object ✹ If the suspicious object or package is in a doorway, personnel should be advised not to exit and to seek shelter as far inside the building as possible ✹ Description—location, size, color, unusual appearance, wires, etc. ✹ Do not alter the environment where the object or package is located. Bombs may be detonated in one of the following four ways: — Mechanical—tripwire — Command—remote control — Electrical—mercury switch, thermal switch, photosensitive — Delay—fuse, mechanical, timer, chemical reaction	
11. Bomb Threat via Telephone (Use Bomb Threat Checklist)	
12. Personal Security Precautions ✹ Stay alert to activities around you ✹ Assume a low profile ✹ Be unpredictable, and recognize signs of surveillance. Vary your route and schedule ✹ Report suspicious activity ✹ Have prearranged simple verbal codes to alert family and coworkers of physical threat ✹ Terrorists select targets on foot and in vehicles to kidnap and or kill	
Application:	
Evaluation:	

Conclusion: Using elements of attention, motivation, and overview, conclude the subject of terrorism/antiterrorism.

Exhibit 3 to Management Training

Handout for Lesson Plan

This is a complementary handout to the lesson plan. Students should use this as a note-taking guide.

Antiterrorism Lesson 1

Introduction to Antiterrorism

OBJECTIVE: Identify basic terrorism/antiterrorism facts and terms.

Antiterrorism Exercise	
Working in pairs, introduce each other and find out about the other person's experience with antiterrorism and identify his or her goals for the class and what he or she expects to do when he or she returns home.	Introduce your partner.
Lesson Topics	**How Will I Use This Information?**
1. Background ✹ World Trade Center, New York City—February 29, 1993 ✹ Alfred P. Murrah Federal Building, Oklahoma City—April 19, 1995, ✹ Khobar Towers, Dhahran, Saudi Arabia —June 25, 1996 ✹ Embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya—August 7, 1998, ✹ USS *Cole*, Aden, Yemen—October 13, 2000 ✹ World Trade Center, the Pentagon, and Pennsylvania (aircraft crash)—September 11, 2001	
2. Terrorism ✹ Is the use of force or violence against persons or property in violation of the criminal laws of the United States for purposes of intimidation, coercion, or ransom? ✹ Most terrorist incidents in the United States have been bombing attacks involving detonated and undetonated explosive devices, tear gas, and pipe or fire bombs ✹ The effects of terrorism can vary significantly from loss of life and injuries to property damage and disruption of services such as electricity, water supply, transportation, and communication	
3. Categories of Terrorism in the United States ✹ *Domestic terrorism*—Involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction ✹ *International terrorism*—Involves groups or individuals whose terrorist activities are foreign-based or directed by countries or groups outside the United States or whose activities transcend national boundaries	
4. General Information About Terrorism ✹ Absolute protection against terrorism is impossible ✹ Terrorism can occur in peacetime or in conflict ✹ Terrorism often consists of acts to intimidate governments or societies to obtain objectives ✹ Terrorism is performed to meet political, religious, or ideological objectives. ✹ Terrorism is or can be used to: ✹ Overthrow governments or economic systems ✹ Retaliate against U.S. foreign policy ✹ Impede U.S. ability to wage war or build up for war ✹ High-risk targets include any place with a large concentration of U.S. personnel	

Lesson Topics	How Will I Use This Information
5. Characteristics of Terrorist Operations ✹ Carried out by specially trained and organized underground elements called cells ✹ Previous surveillance of target to exploit vulnerabilities ✹ Acts of terrorism are usually directed against specific targets in the general population and government ✹ Terrorist operations are characterized by violence, speed, and surprise	
6. Terrorist Goals ✹ Immediate goals — Obtain recognition for cause — Expose government's inability to protect citizens — Demonstrate power or threat credibility — Impact elections, free prisoners, obtain money or equipment, economic disruption ✹ Long-range goals — Cause dramatic changes in government — Turn the flow of events to their side — Gain political recognition	
7. Terrorists Characteristics ✹ *Crusaders*—Ideologically inspired hard-core individuals or groups ✹ *Criminals*—People who commit terrorist acts for personal rather than ideological gain ✹ *Crazies*—Mentally ill people who commit terrorist acts during a period of mental disturbance	
8. Terrorist Methods *Bombs*—May be of any degree of sophistication—pipe, letter, package, car bomb — Placed to destroy property — Cause casualties and death ✹ *Ambush*—Attacks by an individual or small groups, using small arms to assassinate important persons in or outside of government ✹ *Armed attack*—Initiated with diversionary actions — Aimed at key personnel or critical resources — The objective is to cause disruption of mission and adverse publicity ✹ *Hostage seizures*—Undertaking to seize a specific: — Hostage for ransom or political bargaining purposes — Critical asset when personnel are present. Used for bargaining for publicity and political advantage ✹ *Sabotage*—Internal or external means used destroy resources or to weaken ability to counter terrorist activities	
9. Bomb Recognition—Indicators ✹ Mail bomb — Heavy, soiled wrapper — Bulky, awkward envelope — Crude handwriting with misspelled words — Excess postage — No return address — Protruding wires — Has a general address ✹ Pipe bomb — Constructed of metal or plastic — Capped at both ends — Wires may or may not be visible	

Lesson Topics	How Will I Use This Information
10. Leader Actions and Responsibilities ✹ Establish cordon and evacuate nonessential personnel. Cordon size determined locally ✹ No radio transmissions within 500 feet of the affected area ✹ Do not touch the object ✹ If the suspicious object or package is in a doorway, personnel should be advised not to exit and to seek shelter as far inside the building as possible ✹ *Description*—location, size, color, unusual appearance, wires, etc. ✹ Do not alter the environment where the object or package is located. Bombs may be detonated in one of the following four ways: — *Mechanical*—tripwire — *Command*—remote control — *Electrical*—mercury switch, thermal switch, photosensitive — *Delay*—fuse, mechanical, timer, chemical reaction	
11. Bomb Threat via Telephone (Use Bomb Threat Checklist)	
12. Personal Security Precautions ✹ Stay alert to activities around you ✹ Assume a low profile ✹ Be unpredictable, and recognize signs of surveillance. Vary your route and schedule ✹ Report suspicious activity ✹ Have prearranged simple verbal codes to alert family and coworkers of physical threat ✹ Terrorists select targets on foot and in vehicles to kidnap and or kill	
Application:	
Evaluation:	

Describe what you will do differently as a result of this training:

What date do you expect to begin? _____

What date do you expect to finish? _____

Write the name and phone number of a classmate you will call to ask about progress toward his or her goal: _____

Exhibit 4 to Management Training

Sample Security Education Program

It is important to reinforce the security principles and programs that you have already initiated or plan to initiate for your agency or company. This sample program suggests ways to keep your organization highly aware of the security threat and encourages them to practice sound security at all times.

Objective

The objective of the security education and training program is to instill in all employees a sense of responsibility for the security of critical assets and to enable them to react quickly and correctly to threats directed at those assets. All employees must accept their share of security responsibility. It is incumbent upon all supervisors to give security awareness the full consideration it warrants and to emphasize its importance to subordinates.

Implementing the Program

Design the program so that personnel attain the skills they need to apply security techniques pertaining to their job. For example, an administrative specialist who does not work in an industrial area may not need the same depth of understanding as an employee of an oil refinery whose work place is within a restricted area. The program consists of Phase I, Orientation Training, and Phase II, Continuation Training. Appoint a security adviser to manage and implement the program.

Phase I. Orientation Training

This phase is directed toward security procedures and requirements particular to the work site and the job of each individual. It should be administered promptly after an individual arrives at the site. All employees should have a general knowledge of the following:

- Local threat conditions and how the threat applies to the individual
- Information from the Core Security Document (see Part II: Management Chapter 2, Security Policies) concerning restricted area entry and other pertinent specific security information
- Locations and designations of resources
- Orientation on entry control procedures, including verification of the right and the need to be in a restricted area
- Escort procedures for restricted areas
- The threat and how it applies to their area of responsibility.

Phase II. Continuation Training

This phase is ongoing and tailored to the individual's job. It is designed to keep everyone apprised of threats, security procedures, and mission changes affecting them. This phase should include a method for determining the effectiveness of the security program through detection exercises conducted on a recurring basis in restricted areas. Results can be provided to management for follow-up action.

- The security adviser will conduct continuation training by planning, conducting, and evaluating detection exercises in restricted areas. Design these exercises to determine the effectiveness of the security program in restricted areas. The SC must establish complete exercise guidelines and objectives to develop exercise scenarios. The SC will determine frequency of detection exercises based on local operational needs, security awareness,

and trends. Evaluate the number needed in each area based on the size of the area and the number of personnel assigned to the area on a regular basis.

- Develop an exercise grading scale for use during security education and training (SET) exercises. This grading scale must be approved by the SC and should be included in your security policies. As a minimum, assign a grade of pass or fail for each exercise conducted. More elaborate systems may be developed to give better insight into the outcome of the exercises. A scale with 3 or 5 levels (e.g., Unsatisfactory, Satisfactory, or Outstanding) may be adopted by the SC. The security adviser briefs the SC on the overall assessment of security awareness for the site based on the training and testing results.
- A plan or course of action will be developed and implemented if an exercise failure occurs. If a work center fails an SET exercise, conduct a reevaluation with a similar scenario within 30 to 60 days. Ensure that all personnel are aware of the reevaluation results and lessons learned.
- Track and log all SET exercises on a locally developed exercise log or as directed by the SC. Note the time, date, and location of all SET exercises. Send a formal report for any exercise resulting in a failure to the SC and supervisor of the work center affected. Conduct face-to-face briefings with supervisory personnel, telephone calls, or e-mail notifications. Include a brief summary of the scenario, personnel involved, and the outcome of the exercise. Maintain a log of exercises by calendar year. Maintain SET exercise results for 1 year after closeout.
- Develop a test bank of written questions. This will allow you to tailor tests for the work center being visited. Develop questions specific to restricted area security personnel. Develop additional questions that apply to nonsecurity personnel who do not work in restricted areas, but who require security awareness training. Use reinforcement questions.
- All departments whose personnel work with or around critical assets or in restricted areas will conduct Phase II, Continuation Training, as part of their ancillary training program. This training must be tailored to the duties of their work centers. The security adviser will work closely with each department to ensure that it has current training materials and tests to evaluate personnel. The security adviser must travel to the work center to speak with personnel before and after training to continue awareness training and validate the effectiveness of the training. Phase II training must include at a minimum the following:
  - Information on threats to resources located at the site
  - Security procedures for restricted areas
  - Written tests

A primary security education coordinator must be identified from each department. This person should have a close working relationship with the security adviser.

The security adviser should regularly review criminal statistical data for crime patterns. Subsequently, the trainer should:

- Recommend crime prevention strategies and provide analyzed crime data to organizational leaders unless critical events dictate otherwise.
- Develop and maintain a relationship with local law enforcement agencies, especially the RDSTF and with crime prevention officers.
- Consider participating in or hosting a local criminal activities group with police agencies. Consider exchanging information related to drug activity, gang information, and the local criminal threat. Brief pertinent information to the SC.
- Develop media campaigns to publicize the crime prevention program and crime problems.

Exhibit 5 to Management Training

Security Adviser Handbook

The security adviser will be a key member of your organization, responsible for managing your security programs. This sample handbook provides a guide for this official as well as recommended duties and tasks to ensure a successful antiterrorism and facility protection program.

Overview

This handbook establishes procedures for developing and organizing an effective security education and training program. It establishes procedures and requirements for the designated security adviser to implement Phase I, Orientation Training, and Phase II, Continuation Training. Requirements established in this handbook are directive in nature.

1. Introduction: As the security adviser, you are the key player in an effective security education and training program which has a direct impact on the security of company assets. You will work hand-in-hand with a large part of the employee population to ensure protection of valuable assets. Additionally, your reach extends outside the restricted area to the adjoining areas. Security awareness is paramount in providing appropriate protection for our resources.

2. Role of the Adviser: You are an educator, motivator, public relations representative, and, above all else, a professional who can be counted on for security guidance and assistance. You are a force multiplier, bringing support and security personnel together to obtain the overall state of security required to protect our assets. Duties are determined by the director or head of security to meet the following minimum requirements:

- *Phase I, Orientation Training:* Training conducted during indoctrination to the company
- *Phase II, Continuation Training:* Tailored to the individual job and encompasses security detection exercises in restricted areas
- *Program Administration:* Updates to the SC (including exercise ratings and trends).

3. Establishing the Security Education and Training Program: The security adviser's position is established under the authority of governing company policies and in accordance with published security and law enforcement jurisdictional authority. This is the single most important position in developing the security education and training of personnel assigned. Without an effective security education and training program, the security awareness of personnel working on company property will be degraded. You must communicate security policy and procedures, establish a relationship of trust with managers, and provide supervisors with support and guidance needed to educate and motivate employees.

- The head of security must appoint the security adviser in writing and inform all managers of the appointment.
- The security adviser's information must be publicized to employees through media campaigns.
- The security adviser must be included by the human resource department as part of the employee indoctrination program. Your involvement at this level is paramount!
  - Phase I, Orientation Training, must be accomplished during indoctrination training. Documentation of this training can be accomplished by maintaining sign-in sheets.

— Phase II, Continuation Training, must be accomplished continuously. This includes detection exercises conducted on a recurring basis in restricted areas. As the security adviser, you should be focused on detection exercises and continued awareness briefings to employees. You should work with managers and trainers to ensure that they have updated information.

4. Conducting the Security Education and Training Program: As the security adviser, you must be flexible and highly mobile. Your job should take you into work centers and restricted areas on a daily basis. Consider becoming a mobile adviser, setting up your office outside the normal security work center. You cannot effectively complete your responsibilities sitting at your desk day in and day out. You must gather and use available resources to conduct program initiatives. Consider the following examples for inclusion in the program (not all-inclusive):

- Video productions depicting local security conditions
- Computer briefings for staff meetings and work centers
- Bogus credentials for restricted area penetration exercises
- "Stolen" uniform items for use during exercise scenarios
- Handouts containing security education information
- Incentive programs sponsored by managers for security awareness actions.

Phase I, Orientation Training: Get involved with the human resource departments (HRD) employee indoctrination monitor and develop a briefing that will grab the attention of new employees. You must conduct this training as part of the agency's indoctrination program. It will include at a minimum the following:

- Local threat conditions and how the threat applies to the individual
- Information from the agency security instruction concerning restricted area entry and other pertinent security information
- Escort procedures for restricted areas
- Duress procedures to address hostage procedures (how to warn others if you are under duress)
- Locations and designations of critical resources.

The key is to get their attention! Include information on recent security incidents or events in your presentation. Talk about scenarios from actual events without divulging privileged information. Talk about the exercise scenarios you have demonstrated in work centers, citing good and bad examples. If company managers have established an incentive program related to company security, this would be a good time to inform new personnel how it works.

Document Phase I training. At a minimum, maintain a list of all personnel who attended the training sessions for a period of 1 year. Establish procedures to have personnel sign a sheet acknowledging completion of the training. Consider briefing the company SC on numbers trained.

Phase II, Continuation Training: This phase of training will be conducted in two parts.

- The employee's office conducts Part 1 as part of its ancillary training program. This training should be tailored to the specific duties of the work centers. For instance, training a crew of baggage handlers should include procedures to detect, detain, and report intruders found in the restricted area. The security adviser should work closely with each office to ensure that it has current training materials and tests to evaluate personnel. The security adviser should travel to the work centers to speak with personnel before and

after training to continue awareness training and validate the effectiveness of the office-level training. Phase II training must include at a minimum the following:

- — Information on threats to company resources
- — Security procedures for restricted areas (i.e., circulation and entry control)
- — Duress words and authentication procedures to warn others that you are in danger or to verify authority to carry out action or enter an area
- — Written knowledge tests (results should be forwarded to the security adviser on an annual basis)

- You will conduct Part 2 of continuation training. This will be completed by the following procedures:
  - — Visits to each restricted area work center twice per year (can be accomplished through roll call training or by briefings)
  - — Detection exercises to determine the effectiveness of the training program (designate them as security education and training exercises)
- Documentation of Phase II training will be accomplished on a locally devised form (computer database is acceptable). When tests are administered as part of the training, document the number tested, number of failures, and heavily missed (trend) items. Use the trend information to tailor future briefings and exercise scenarios for personnel assigned to the work center. Consider reporting this information to management.
- You will conduct continuation training separate from offices by planning, conducting, and evaluating detection exercises in restricted areas that support critical company resources. Design these exercises to determine the effectiveness of the security program. Management must establish complete exercise guidelines. The director of security will locally determine the number and frequency of detection exercises. Evaluate the number needed based on the size and number of restricted areas and the number of personnel assigned to these areas on a regular basis. Document the local determination in a memorandum and adjust as necessary. Conduct sufficient exercises to develop trends and report those trend data to management.
- SET exercises should be designed to test the security awareness of nonsecurity personnel assigned to restricted areas. Exercises to test the security awareness of security personnel should be coordinated with the security supervisor. You should be highly experienced at conducting exercises before initiating this program. Keep in mind that exercise objectives should never take precedence over the safety of personnel, equipment, or resources. Using actual perpetrators may be authorized; however, exercise perpetrators WILL NOT simulate any action which could be interpreted as hostile by support or security personnel. Perpetrators will explicitly follow all directions given by the exercise participants unless cause a safety hazard or violate the law. Consider implementing an exercise safety briefing (sample provided in **exhibit 6**).
- To plan effective and safe exercises, you must completely plan and execute SET exercises with a cradle-to-grave philosophy. Use the following guidelines when developing SET exercises:
- Planning phase:
  - — Schedule a time and location for the exercise
  - — Develop an exercise scenario with at least one objective
  - — Determine equipment, uniform, and perpetrator needs
- Implementation phase:
  - — Notify the control center
  - — Brief perpetrators on their responsibilities and safety guidelines

- Initiate the exercise (follow local authentication procedures)

- Execution phase:
  - Obtain a position where you can observe all actions of the perpetrators and exercise participants
  - Control the actions as needed (step in if problems arise or safety is in question)
  - Terminate the exercise when objectives are met or when it is clear that the objectives will not be met
  - Gather exercise participants and conduct a critique of the exercise make every effort to impart positive lessons even if the exercise is graded as a failure
  - Allow exercise participants to evaluate what they saw wrong
- After-action phase:
  - Obtain names of participants for an exercise report
  - Notify the attending control center of the termination
  - Debrief perpetrators and gather equipment
  - Complete an exercise report and send it to management for review
  - Compile trend information for formal reporting to management

Note: The use of noncompany employees in SET exercises should be discouraged. However, if company managers consider this necessary, it must be coordinated with the legal department.

- Develop an exercise grading scale for use during SET exercises. This grading scale must be approved by the director of security and should be included in the company security policies. At a minimum, assign a grade of pass or fail to each exercise conducted. More elaborate systems may be developed to give better insight into the outcome of the exercises. A scale with 3 or 5 levels (e.g., Unsatisfactory, Satisfactory, and Outstanding) may be adopted by the company.
- Exercise failure procedures must be developed to ensure that the correct lessons are learned from the exercises being conducted. If a work center fails a SET exercise, a reevaluation with similar circumstances must be conducted after 30 days, but no longer than 60 days from the date of the failure. Although the same personnel may not be involved during the reevaluation, the intent is that the exercise results and lessons learned will be shared by personnel throughout the company.
- Document your SET exercises as directed by the director of security. Consider a formal report for any exercise which resulted in a failure. Some form of notification to managers and exercise participants should be developed. Consider face-to-face briefings with supervisory personnel, telephone calls, or e-mail notifications. Track and log all exercises on a locally developed exercise log. Note the time, date, and location of the exercise. A brief summary of the scenario, personnel involved and the outcome of the exercise should be included. Maintain a log of exercises by calendar year and maintain SET exercise logs for 1 year after closeout.
- Develop a test bank of questions for written knowledge tests. This will allow you to tailor the tests for the work center being visited. Develop questions specific to restricted area security. Develop additional questions which apply to nonsecurity personnel who do not work in restricted areas, but who require security awareness training.
- Questions should be multiple choice or true/false. Do not design questions to trick or stump the participants. Written tests should be aimed at determining the level of comprehension from your training sessions. Consider taking tests with you when you visit work centers. Inform supervisory personnel that pretests are available and can be used

before training to identify training needs. Most supervisory personnel will appreciate your targeting the training to what they need rather than conducting a general training session that may waste time.

- Grade the tests on the spot and give immediate feedback to test takers. Give an overall summary of the items missed. For areas that were frequently missed, provide the group with the correct information immediately. Do not let personnel leave the training session with incorrect information.
- Document results of the tests. Individual documentation of test results is not required. Brief managers on overall test results. The director of security should determine the format for reporting this information.

5. Day-to-Day Security Adviser Activities: Because the security adviser typically is a full-time position, there are many day-to-day operations that can be accomplished when you are not conducting training.

- Entry control point checks: You can quickly spread the word on security awareness by interacting with employees. Consider asking a series of security education questions as you check the badges of those entering a restricted area. This is a great way to determine knowledge on duress words and entry control procedures. Once again, this is great information to report to security managers. It is also a good way to provide feedback to supervisors.
- You may require a vehicle for daily use. Rather than dedicating an otherwise usable patrol vehicle, consider using one of the following:
  - All-terrain vehicle
  - Bicycle
  - Golf cart
- **Table 1** suggests the DOs and the DON'Ts of conducting adviser operations.

DO:
Conduct face-to-face meetings with security managers and superintendents
Attend quarterly security manager's meetings
Attend staff meetings
Walk around and conduct face-to-face meetings in restricted areas
Review security incident logs weekly
Publish security education handouts and distribute them
DON'T:
Act like an inspector
Create security rules and regulations
Keep personnel from accomplishing mission-essential tasks
Be late for meetings
Allow personnel to downplay the security education and training program

Table 1. Security Adviser Duties

Note: The above list is not all-inclusive. The security adviser should be an extremely professional person, selected to perform these duties based on maturity level, experience, and proven performance.

The security adviser must be the security education and training expert for the entire company. Thorough knowledge of security policies governing the security of the company is mandatory. Additional knowledge on antiterrorism procedures, intrusion detection systems, training, and evaluations is critical to the proper execution of the adviser's duties.

Keep in mind that you are the lone representative of the director of security during many encounters on the company grounds. Your professional conduct and bearing must remain above reproach at all times. The effectiveness of your company's security awareness is highly dependent on your success.

Exhibit 6 to Management Training

Sample Security Exercise Safety Briefing

1. Introduce yourself and explain your role.
2. Relay pertinent communications information.
3 Identify the exercise control center.
4 Assign call signs to perpetrators if they have radios.
5. Confirm the presence of all exercise perpetrators.
6. Confirm the presence of equipment items needed
   - Uniforms
   - Bogus credentials
   - Radios
7. Give a detailed briefing on the exercise scenario.
8. Tell perpetrators the actions you want them to take.
9. Identify the work center or area where the exercise will be conducted.
10. Discuss the objectives of the scenario.
11. Give the perpetrator instructions on information gathering (names, unit, and actions taken or not taken by exercise participants).
12. Discuss the time limit of the exercise.
13. Specific times should be planned and adhered to.
14. Set exercises may be delayed pending real-world activities and continued as deemed necessary.
15. Discuss a plan of action if the perpetrator is not detected within the time limit.
16. Determine travel routes to be used.
17. Determine rally point.
18. Give detailed instructions on the action to take.
19. Perpetrators must obey instructions.
20. Perpetrators may not commit hostile acts.
21. Perpetrators will not use physical violence.
22. Conduct after-action review.

PART III: ASSESSMENTS

Chapter 1: Methodology

Introduction

The self-assessment methodology is designed for use by facility managers and security professionals to determine the risks to their facilities or sites. Managers must identify the levels of risk they face in protecting their assets, particularly their assigned facilities, in order to use the best practices and the most prudent approaches. This section addresses the means to analyze and assess the risks to facilities.

Understanding the term vulnerability is key to conducting an assessment of assigned resources. In antiterrorism, the Department of Defense (DoD) defines a vulnerability as "a situation or circumstance, if left unchanged, that may result in the loss of life or damage to mission-essential resources. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment." Two examples are:

- No (or inadequate)control at buildings or sites that are in the high-risk category
- No distance has been established at a designated high-risk facility to standoff from explosives.

Generally, managers should conduct an initial vulnerability assessment to be followed by annual reviews. These initial and annual assessments should identify vulnerabilities and mitigation options for enhanced protection of personnel and resources. Agencies should review lower-level antiterrorism (AT) programs at least once every 2 years to ensure unity of AT efforts throughout their regions. The higher agency assessment should assess AT plans and programs, intelligence processes, physical security, vulnerability and responses to threats (including weapons of mass destruction [WMD]), availability of resources, and local emergency response support. At a minimum, each agency should prioritize, track, and report to the appropriate agency the actions to be taken to address the vulnerabilities identified in their annual assessments.

A key to protecting assets is the determination of the criticality and vulnerability of facilities (buildings, communications systems, etc.). Once that has been established, managers and/or security professionals can apply a set of security protection measures (countermeasures) to mitigate vulnerabilities to the extent possible. Presented in Part IV: Encyclopedia, is a list of protective measures for each facility. This effort will not prevent a terrorist attack, but is designed to deter such activity, detect an imminent attack, and facilitate an effective response to such an attack.

The protective measures also are designed to mitigate the consequences of an attack and provide the agency or company "owner" an improved response and consequence management process.

Assets Inventory

The first step in the assessment process is to conduct an inventory of the assets for which the manager is responsible. In Chapter 2, below, the Florida Department of Law Enforcement (FDLE) provides a tool that managers and/or security professionals can use to identify and classify all assets and sites. This step is essential to the assessment process and we recommend it before application of the assessment methodologies listed below.

Vulnerability Assessment Process

Once you have committed to the vulnerability assessment project in principle, you can use this chapter to conduct your assessment. We designed this section to make the process as simple as possible. When you score your facilities or sites, you will have a vulnerability score based on this process to determine into which risk category your facility fits. Then you can select those security (protective) measures necessary to reduce your facility's risk and to have a facility that should experience minimal consequences as the result of a terrorist attack or event. For the purposes of your assessment, the facility risk categories are:

- High
- Medium
- Low

Combined with your facility's risk category is the threat level assigned by the U.S. Department of Homeland Security (DHS). In other words, you will use the security measures and your facility's risk score (level) and the threat level that originates from DHS. It will look similar to the diagram below:

Facility Risk Score	Elevated Threat: Significant Risk of Terrorist Attack	High Threat: High Risk of Terrorist Attack	Severe Threat: Severe Risk of Terrorist Attack
High	List of Measures	List of Measures	List of Measures
Medium	List of Measures	List of Measures	List of Measures
Low	List of Measures	List of Measures	List of Measures

Note: We are using the elevated threat as the minimum threat because the state of Florida has determined that this is the most realistic minimum threat level in which to operate. There are two lower threat levels, Low and Guarded. We are not providing security measures for these levels because it is prudent to maintain a level of security that can cope with the Elevated Threat level.

Once you have determined your facility's risk level and compared the three threat levels, you will be able to select suggested security measures from the major security protection categories. These measures will include options in key areas such as perimeter security, lighting, access control, parking lot security, maintaining a security officer force, having an awareness program for your employees and customers, and others. Again, the measures presented for implementation will be based on these two main factors:

- Your facility risk score
- Operating in the three DHS threat levels

For example, if your facility scores "medium" and you see the need to implement security measures for the elevated threat level, you will then select from a menu of options for:

- Medium risk level
- Elevated threat level

It is more than likely that you also will have security measures that should be implemented for the two higher threat categories. Therefore, it is possible you will need to implement additional security measures for:

- Medium risk level
- Elevated, High, and Severe threat levels

Following is a brief description of the process you will use to conduct the vulnerability assessment:

- Preparation Phase
  - Gather your vulnerability assessment team
  - Review the **Part I, Basics** in this Manual
  - Review the **Part II, Management** in this Manual
  - Review your current risk management plan
- Security Planning Phase
  - Obtain current intelligence on facility risk and vulnerability
  - Determine your facility (site or building) risk level
  - Conduct the vulnerability assessment later in this section (There are three options presented for you to do this.)
  - Review the Protective Measures Database matrix
  - Review your final plan
- Implementation Phase
  - Implement the matrix actions you have selected
  - Reassess your plan based on the threat
  - Make necessary adjustments to your plan

You should start with a "clean slate," as this vulnerability assessment is geared toward the current terrorist threat. But, you *should consider what security measures you have in place,* because many of your current security measures could assist in reducing the consequences of a terrorist attack. Armed with this information, you can conduct a vulnerability and risk assessment, based on a determined threat and obtain a score for your facility, site, building, or public venue. Based on that score and using the DHS advisory system color chart, you will select from the menu of choices the security measures you need to implement to *reduce your vulnerability to a terrorist attack to the lowest level possible.*

Vulnerability Assessment Purpose

A vulnerability assessment is defined as the process of identifying any weakness that can be exploited by an adversary to gain access to or information from an asset. Vulnerabilities can result from but are not limited to building characteristics, equipment properties, personal behavior, and operational practices.

The vulnerability assessment is designed with two purposes in mind:

1. It will provide the facility director or agency head with a current vulnerability profile. This provides information needed to determine what capability there should be regarding the improvement of the response capability for a terrorism/WMD incident. This assessment will provide information to the planning focus for further development of the overall regional risk. It may also provide information for modification of the region/facility's Emergency Operations/Response Plan.
2. It will provide information that can be used to refine, modify, and/or develop the facility or site planning scenario or focus of your response effort. For the public infrastructure, it also can provide the region or state with a cumulative set of risk data to assist in planning actions against terrorism.

Considerations

Following are two key considerations that should be taken into account before proceeding with the regional/facility vulnerability assessment process:

1. Use the concept of the most likely scenario when completing the vulnerability assessment for each assessment factor. Based on the facility's unique infrastructure and its attractiveness as a lucrative target, the most likely scenario may not necessarily be the worst case (nuclear attack for example), but represents the most probable kind of terrorism/WMD event that may occur in your area (hazardous materials [HAZMAT], toxic spill release, or a conventional bomb explosion).
2. Use the fact that an attack against your facility, site, system, or special event within your area of responsibility would likely result in death, injuries, or infrastructure damage or destruction that could overwhelm the area's emergency response capabilities, including any mutual aid agreements or assistance pacts.

Implementation

Step 1: Assembling the Team

Public Infrastructure. Because public facility sites and building managers know their infrastructure and systems better than anyone, they are capable of analyzing their own facilities. A facility's vulnerability assessment team should include:

- Appointed team leader or lead manager
- Public works (engineering, heating, ventilation, and air conditioning [HVAC], structural, design, maintenance)
- Public health services
- Emergency management
- Law enforcement
- Fire department
- Hazardous material team and emergency medical services
- Human resources
- Employee representative
- Public affairs or media relations
- Facility security managers

Private Infrastructure. These officials and employees will have the same level of qualifications as the public officials. The private infrastructure team should consist of:

- Appointed team leader or lead manager
- Facility security manager
- Facility engineering (maintenance, HVAC, structural, design)
- Public sector representatives*
  - Emergency management
  - Law enforcement
  - Fire department
  - HAZMAT team (private and public)
- Employee representative
- Human resources
- Corporate or company public affairs or media relations

*The availability of public sector agencies to assist in a private sector vulnerability analysis may be limited. An alternative is to use consultants from disciplines outside of the public sector.

Special Venues. The selection of these personnel uses the same reasoning as for public and private facilities and infrastructure.

- Appointed team leader or lead manager
- Facility security manager
- Facility engineering (maintenance, HVAC, structural, design)
- Public sector representatives* (see above)
  - Emergency management
  - Law enforcement
  - Fire department
  - HAZMAT team (private and public)
- Employee representative
- Human resources
- Corporate or company public affairs or media relations
- United States Secret Service (it can assist because of its role as appointed executive agent for "national security events" and for facilities that will host a national political convention or appearance by the president or vice president)
- Entertainment security coordinators

The multidisciplined planning team members must be selected with care to perform the assessment. They must have expertise in their respective areas and be able to work well with others. They must establish an overview of the jurisdiction as to who has what responsibilities and oversight for the process. The importance of this step cannot be overemphasized, as it will lead to the development of the remaining assessment and provide the facility with the information it needs to focus on strategy. The planning team has several steps to complete as it develops the vulnerability assessment.

Step 2: Identifying Potential Targets

It is impossible and probably not desirable to make all facilities secure to the point that they constrain access and adversely impact the economy of the owning agency or company. Public and private infrastructure facilities do not have unlimited funds, resources, or people to meet the impossible task of securing all facilities. Our approach is to maximize what capabilities you have and recommend practical and sensible steps to reduce your vulnerabilities. This step helps to identify targets that are most critical to the region.

- A potential target is defined as a public or private facility, or a special venue, including its support structure, building, or total system.
- The team should examine all portions of the facility, site, building, complex, or special venue and consider all the components to develop a comprehensive assessment.
- Consider how these components could be a target of a terrorist attack, and consider adjacent facilities and how an event there could affect your facility.
- Develop a complete list of potential targets within your facility in order of their criticality.
- If you have dozens of potential high risk targets, select at a minimum the top 10% of your facility assets for assessment and work your way down the list as time permits.

Step 3: Conduct an Individual Target Vulnerability Assessment

Use the following seven factors to assess vulnerability for each potential target:

1. Level of visibility addresses the awareness of the existence and visibility of the target
2. Criticality of the potential target site in terms of its importance to the corporation or agency and the protection of the population and maintaining a viable economy
3. The potential threat element's access to the potential target for entry and exit
4. The value of the target to terrorists based on their motivation (i.e., whether their attack is a political statement, whether the target is of symbolic importance, whether the target is a multinational corporation that could be perceived as a symbol of U.S. presence/influence, etc.).
5. Potential target threat of HAZMAT presence at the site or facility
6. The population affected by the potential threat (site or facility occupancy, public venue capacity, location to nearby populations)
7. The potential for collateral damage to other facilities in specified distance radius, ranging from 300 feet to 2 miles

Your planning team or specially trained team members can perform the above tasks. We suggest that a knowledgeable and authoritative representative from each class of facility to be evaluated be included in the assessment process. These individuals can provide expert advice and assist in obtaining the necessary cooperation for your effort.

It is important that your team accurately record the results of each assessment. Once the initial effort is completed, the results and any corrective actions taken must be reviewed annually and updated as the threat and other factors change. It will be important to stay focused, as some corrective actions may take years to complete.

We recommend that assessment reports for public facilities be protected as "For Official Use Only." For private facilities, the relevant documents should be marked with legally sufficient proprietary data. For the public infrastructure only, the FDLE should receive a copy of the assessment through your FDLE regional office.

In addition to the factors outlined, we recommend that you also consider the following issues when you conduct the vulnerability assessment:

1. Potential for death and injuries resulting from the use of classes of WMD including chemical, biological, nuclear, and radiological releases. One example to consider would be the potential impact on humans of a biological weapon and if it would be worse than an incendiary device (bomb, fire, and explosive) or weapon.
2. Potential impact of property loss and damage from the use of a particular type of WMD. Also, consider the cost of providing temporary replacement for facilities and property damaged or destroyed.
3. Impact on the interruption of your tourism industry, critical utilities (water, electricity, gas, telephone, etc.), critical infrastructure (roads, bridges, rail lines, etc.), and the recovery time and cost associated with the disaster.
4. Capabilities of your organizational emergency response personnel (if staffed), support of the public sector, and emergency response equipment (fire suppression, HAZMAT containment, first responder) immediately available on a day-to-day basis. Do not include resources available through mutual aid agreements, or from state or federal agencies, as they have dual commitments. Make sure that you know what you have available to handle the emergency, because you will be on your own while waiting for assistance.

5. Capabilities of external first responder and emergency management agencies, including their personnel, equipment, and capabilities. Evaluate the availability of this equipment, as it will be dispatched on a priority basis in the event of numerous calls for assistance.

Step 4: Determine the Public, Private, and Special Venue Facility Vulnerability

Compile individual target vulnerability assessment results on the individual target vulnerability summary. The ranking should indicate (from highest to lowest) the individual target assessments conducted for your region. For the private infrastructure, you will not be able to rank similar facilities from high to low, but you can list those within your own organization.

It may be possible for you to meet with similar private infrastructure groups to compare vulnerability assessment findings. However, some corporations may elect not to release such information because of competitive concerns.

For the public facilities, as approved by FDLE, the highest individual target vulnerability assessment of any potential target in the region is defined as the regional vulnerability rating.

Implementation Advice. Infrastructure vulnerability assessments should be conducted as soon as possible and, based on your findings and open recommendations, they should be reviewed regularly. Your assessment team must include properly trained, qualified, empowered, and dedicated individuals to maintain the integrity of this essential process.

Your vulnerability assessment effort, whether at the state or local level will require the complete support of the public. For the private sector, support will be needed from organization or corporation employees, customers, and shareholders; for the private infrastructure and for public venues, the patrons and the venue owners.

As noted in the Introduction, the responsible manager (agency director, owner or operator, or other leaders of the corporation or agency) should establish a multidisciplinary planning group to accomplish the vulnerability assessment and strategic development process.

In addition, we recommend forming an expert subgroup that has been trained in all aspects of the assessment to examine the potential threats. A recommendation of how to proceed is up to the region, as internal circumstances may direct one course of action versus another. The focus is on the region's or facility's ability to take care of its citizens. We recommend that the following personnel be appointed for this team:

- Site or facility manager or a knowledgeable and empowered representative
- Security director or knowledgeable representative
- Community outreach or private security coordinator from the local law enforcement agency
- Security and protection consultants as necessary

We also recommend that you seek assistance from the FBI, FDLE, or other law enforcement agencies.

Assessment Options

Three vulnerability assessment models are provided as tools for conducting assessments. Recognizing differing opinions, approaches, and time constraints of users, FDLE selected these options to allow managers to select the best tool for their circumstances. Each model has a different level of complexity, comprehensiveness, and accuracy for determining the appropriate risk level.

- *Option One: DOJ Assessment Model*—This assessment tool described in Chapter 3 is derived from the Department of Justice (DOJ) and is a succinct, abbreviated assessment tool for those who prefer not to use the comprehensive American Association of State Highway and Transportation Officials (AASHTO) model (Chapter 5) or the mid-range DoD assessment model. This DOJ option provides users with a simple vulnerability assessment tool using a rapid, less intuitive scoring mechanism. The AASHTO Guide provides objective empirical data, whereas the alternative DOJ tool is a tailored (shortened) version derived from DOJ's Office for Domestic Preparedness. The DOJ model allows users to complete a single-page document and obtain an approximate vulnerability rating. This product typically can be completed in 15 to 20 minutes.
- *Option Two: DoD Assessment Model*—Chapter 4 includes the DoD's vulnerability assessment model, referred to as MSHARPP (for Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity). This tool uses a slightly more refined and objective scoring methodology than does the DOJ model and requires roughly twice the time to complete the scoring process (30 to 40 minutes). This model pits specific threats against facility categories and expects scoring results to lead users to design protective measures based on the outcomes.
- *Option Three: AASHTO Model*—This comprehensive criticality and vulnerability assessment tool (see Chapter 5) was designed for the U.S. Department of Transportation (DOT). As the most complex and detailed of the three assessment methodologies, this tool provides the best and most complete analysis for determining appropriate risk levels. Although managers and security professionals may find initially that the AASHTO model is challenging to use, an investment of several hours to learn and use this tool will provide the most empirical, unbiased, and supportable assessment of risk.

Based solely on their needs, users should select the best assessment option for their circumstances and constraints. It is possible for users to forego all assessment options and simply select a risk level that they feel best represents their facility. However, using a completely subjective selection without any weighted scoring factors may undermine the best practice protective measures outlined later in this Manual.

This is perhaps the most important chapter of the preparation phase as it outlines the three recommended vulnerability assessment methods. All are designed to give you a *quantifiable* score based on objective data that you can provide to your senior managers to demonstrate the need for security upgrades. This chapter also is designed to give you enough information to decide which tool fits your needs best and to move to the next step in this process.

PART III: ASSESSMENTS

Chapter 2: FDLE Assessment Inventory Tool

The following FDLE Assessment Tool should be used as a facility security checklist to assess and highlight in-place security features. This document should be completed upon receipt in order to note security gaps and assist FDLE in better assessing the "health" of the state security program.

Statewide Comprehensive Facility Vulnerability Assessment Form

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Information Contained In This Report Is Confidential

Pursuant To Florida State Statutes 281.301 and F.S. 119.07(3)(ee); (CH 2002-67)

January 2003

Facility Name:	
Street Address:	
City	
State	
Zip Code	
County:	
Latitude (Center of Site):	
Longitude (Center of Site):	
Emergency Contact Person:	
24/7 Contact Telephone Number:	
Contact Facsimile Number:	
Contact Person Email Address:	
Policing Jurisdiction:	
Regulating Agency:	
Regulating Agency Telephone:	
Average Number of Employees on Site Daily:	
Average Number of Visitors on Site Daily:	
Is the Site occupied by Employees or Visitors	
Hours of Operation	
Primary Contact Name:	
Contact Person Position:	
Type of Construction:	
Date of Assessment:	

Survey/Assessment Conducted By:

Name	Agency	Assignment	Telephone

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Facility/Infrastructure Type (check only one primary category and one sub-category if provided)

- ☐ **Government Facility**
  - ☐ State
  - ☐ Federal
  - ☐ County
  - ☐ City/Local
- ☐ **Embassy/Consulate**
- ☐ **Military Facility**
  - ☐ Base
  - ☐ National Guard Armory
  - ☐ Bombing Range
- ☐ **Educational Facility**
  - ☐ College/University
  - ☐ High School
  - ☐ Middle School
  - ☐ Elementary School
- ☐ **Emergency Facility**
  - ☐ Hospital
  - ☐ Other Medical Facility
  - ☐ Fire Department
- ☐ **Law Enforcement**
  - ☐ Federal
  - ☐ State
  - ☐ County
  - ☐ Municipal
- ☐ **Correctional Facility**
- ☐ **Recreational Facility**
  - ☐ Stadium/Arena
  - ☐ Park
  - ☐ Amusement Park
  - ☐ Beach
  - ☐ Shopping Mall
- ☐ **Transportation Facility**
  - ☐ Airport
  - ☐ Airfield
  - ☐ Seaport
  - ☐ Bus Station
  - ☐ Railway
  - ☐ Truck Terminal
  - ☐ Interstate Highway
  - ☐ Bridge
  - ☐ Tunnel
  - ☐ Lock/Dam
  - ☐ FAA Navigation
- ☐ **NASA**
- ☐ **Business/Corporate Facility**
- ☐ **Industrial Complex**
- ☐ **Nuclear Plant**
- ☐ **Chemical Storage Facility**
  - ☐ Crude Oil Refinery
  - ☐ Oil Tank
  - ☐ Fuel Depot
- ☐ **Power Grid**
- ☐ **Reservoir/Water Supply**
- ☐ **Food Storage/Distribution Center**
- ☐ **Transmitter Facility**
  - ☐ Cable Network
  - ☐ Open Air Television Network
  - ☐ Radio Network
  - ☐ Network Service Provider
- ☐ **Phone Relay System**
- ☐ **Financial Institution**
- ☐ **Other (Please list)**

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Facility/Infrastructure Category (check all that apply)

☐ Telecommunications	☐ Water Supply Systems
☐ Electrical Power Systems	☐ Emergency Services
☐ Gas and Oil Production, Storage, Transportation	☐ Continuity of Government Services
☐ Banking/Finance	☐ Commerce
☐ Transportation	☐ Educational Facilities

Facility/Infrastructure Commodities (check all that apply):

☐ Phone Relay System	☐ Main Aquifer(s)
☐ Cable	☐ Water Holding Tanks
☐ Cell Phone Relay Towers(s)	☐ Airplanes
☐ Systems Supplying Power to 10,000+	☐ Buses
☐ Systems Supplying Power to Metropolitan Areas	☐ Distribution Vehicles
☐ Supply Electrical Power for Nuclear Plants	☐ Emergency Vehicles
☐ Gas Facilities Servicing 10,000 +	☐ Law Enforcement
☐ Oil Tanks	☐ Governor/State Officials
☐ Pipelines/Natural Gas Transmission Lines	☐ Key Government Officials
☐ Computer Mainframe(s)	☐ Ship(s)
☐ Centralized Information System(s)	☐ Medical Supplies
☐ Water Supply	☐ Agriculture
☐ Hazardous Materials	☐ Power Lines
☐ Transmitter(s)	☐ Other (Please List)

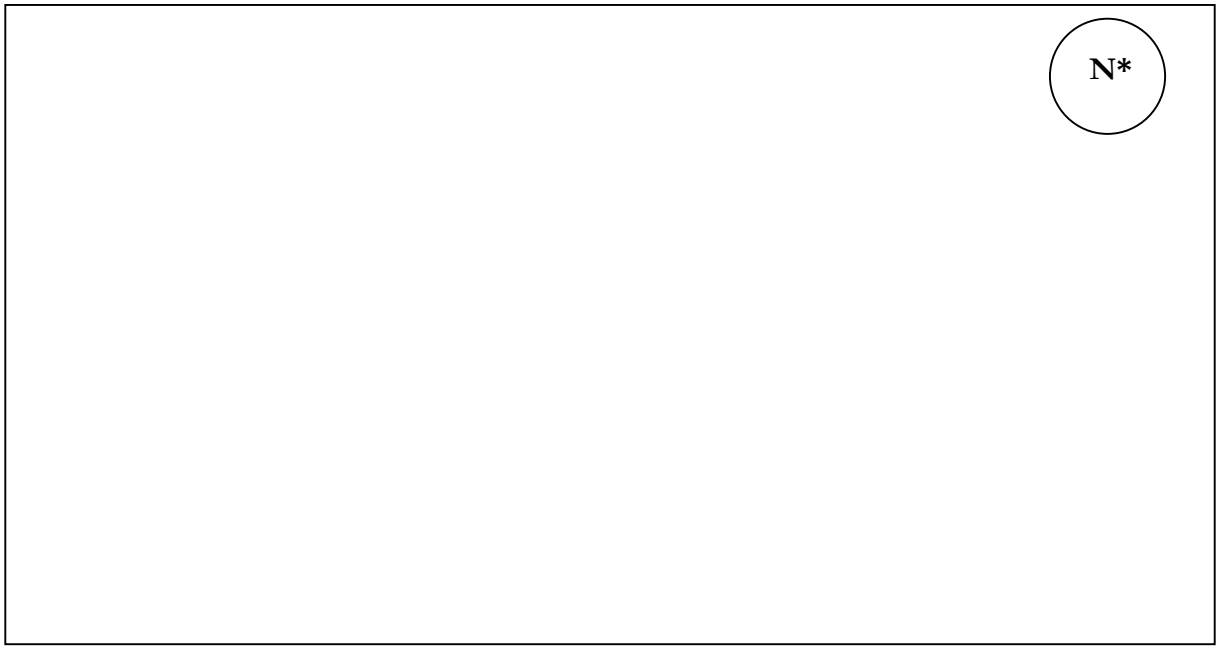
Facility/Infrastructure Impact (check one)

National	State	Regional	Local
☐	☐	☐	☐

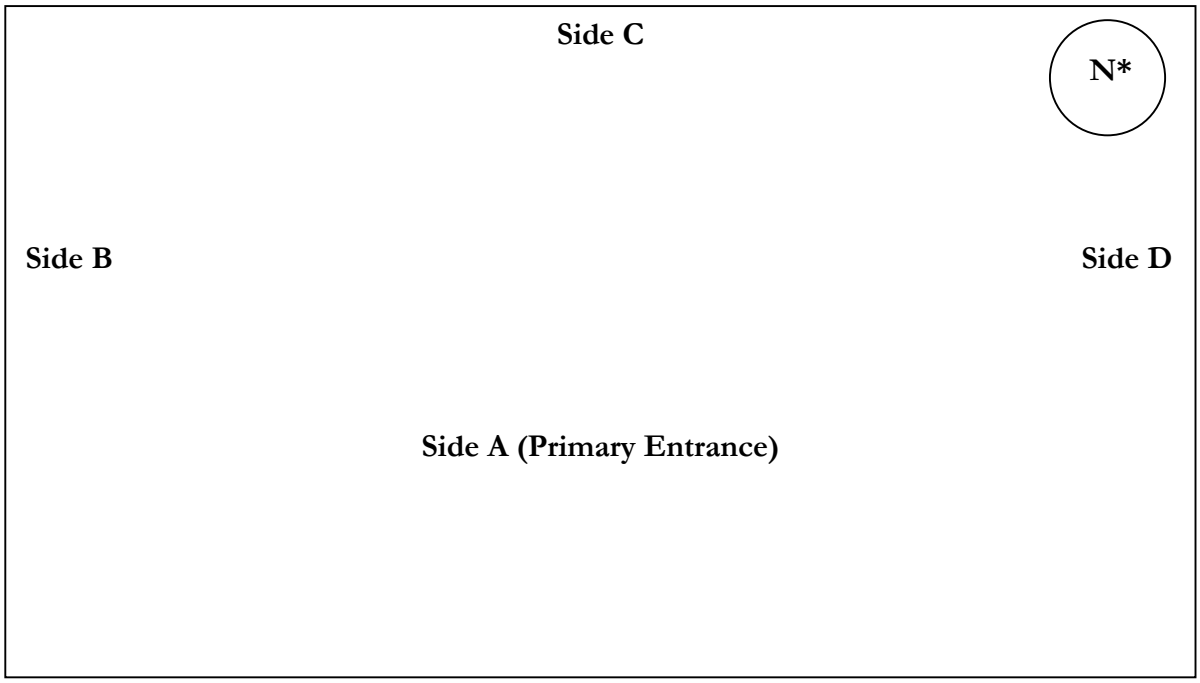
The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

PART I

To be completed by Facility Administrator or Security Personnel.



Property Diagram



Facility Diagram

*Insert North directional arrow in circle.

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION I. BUILDING INTERIOR

1. Doors

Type	Type Access Control	Alarmed(Y /N)	Observations

2. Fire protection

Sprinkler (Y/N)	Extinguishers (Y/N)	Stand Pipe (Y/N)	Halon (Y/N)

2a. Access to city main (Y/N)

Observations

3. Reception area

Secured Reception Area (Y/N)	Secured Receptionist Booth (Y/N)	Receptionist (Y/N)	On Site Security / PSO (Y/N)	Armed Security (Y/N)	Police (Y/N)

Observations

4. Interior closed circuit TV

Areas	Monitored (Y/N)	Recorded/BU (Y/N)	Analog (Y/N)	Digital (Y/N)

Observations

5. Location of Most Actively Used/High Occupancy Rooms

Location	Observations

5a. Safe Rooms or Concentrated Location for Valuables? (Y/N)

Location	Observations

5b. Designated Mail Handling Facility? (Y/N)

Location	Secured (Y/N)	Observations

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

6. Internal HVAC

Location	Secured (Y/N)	Observations

6a. Duct Systems

Location	Public Access (Y/N)	Secured (Y/N)	Observations

6b. HVAC Shut-Off

Location	Public Access (Y/N)	Secured (Y/N)	Observations

7. Elevators? (Y/N) If yes, how many?
On emergency generator? (Y/N)

7a. Accessibility of Mechanical Equipment or Elevator Machine Room

Description/Location	Observations

7b. Serviced by (Company)

Name of Company	Contact Telephone Number

8. Ceiling (Construction and Material)

Description	Observations

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

9. Floor/Floor Coverings (construction and material)

Description	Observations

10. Evacuation Routes/Fire Escapes

Side	Description	Observations
A		
B		
C		
D		
Other		

Section I. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION II. LIST OF NON-AGENCY TENANTS IN FACILITY

Company Name	Floor	Point of Contact	Telephone # - 24/7	# of Personnel within Facility

Section II. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION III. COMPUTER APPLICATIONS

1. How is Computer Technology Actively Utilized at the Facility?

Description	Observations

2. What kind and size of external connectivity exists?

Description	Observations

3. What Computer Operating Systems Are Used at the Facility (Windows 2000, Unix, etc)?

Description	Observations

4. What Computer Back-up Systems are utilized?

Description	Observations

5. Are the Computers Internally Networked? (Y/N)

Observations

6. Can Workers Log Into the Network Remotely? (Y/N)

Observations

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

7. Can Workers Log Into the System through the Internet? (Y/N)

Observations

Section III. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION IV. HAZARDOUS MATERIALS

1. Are Biological Hazardous Substances Used or Stored On-Site? (Y/N)

Description	Quantity on Hand	Storage Location	Describe Security

2. Are Nuclear / Radiological Substances used or stored on-site (Note: Not simply Weapons Grade)? (Y/N)

Description (Type & Level)	Quantity on Hand	Storage Location	Describe Security

3. Are Explosive/Incendiary Devices/Substances Stored or Used On-Site? (Y/N)

Description	Quantity on Hand	Storage Location	Describe Security

4. Are Chemical Substances Stored On-Site? (Y/N)

Description	Quantity on Hand	Storage Location	Describe Security

Section IV. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Section No.	Additional Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

PART II

To be completed by RDSTF of Designated Personnel.

SECTION I. OUTER PERIMETER

1. Neighborhood-Type (check all applicable)

Business ☐	Residential ☐	Rural ☐	Industrial ☐

2. Surrounding Structure Types (check all applicable)

Single-story ☐	Multi-story ☐	High-rise ☐

3. Adjoining Land and/or Buildings, Streets, Access to Freeways, Railroad Spurs, Bodies of Water

Side	Description
A	
B	
C	
D	

4. Fencing/Walls/Barricades

Side	Description	Observations
A		
B		
C		
D		

5. Parking Lot/Garages/Entrances/Exits

Side	# of Entries/ Exits	Access Controlled (Y/N)	Type of Access Control	Decal (Y/N)	Observations
A					
B					
C					
D					

5a. How close to Facility/Infrastructure can vehicles park?

5b. Is there a designated parking area for non-employees? (Y/N)

Business	

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

6. Are there out buildings and/or Storage Buildings, Dumpsters? (Y/N)

Side	Description	Locked/Secured (Y/N)
A		
B		
C		
D		

7. Freestanding Exterior Lighting (streetlights, floodlights, manual or automatic-when do they activate)

Side	Description	Observations
A		
B		
C		
D		

8. Visibility of Perimeter/Building/Site

Side	Description	Observations
A		
B		
C		
D		

9. Landscaping/Possible Concealment

Side	Description	Observations
A		
B		
C		
D		

10. Exterior freestanding closed circuit TV

Side	Y/N	Monitored (Y/N)	Taped/Backed Up (Y/N)
A			
B			
C			
D			

11. Signage/Way Finding

Side	Description	Observations
External to Perimeter		
Entrance Way		
Front Entrance		
Other Entrances		
Other Signage		

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

12. Observation into/from Building (Natural Surveillance/Plain View)

Side	Description	Observations
A		
B		
C		
D		

Section I. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION II. BUILDING EXTERIOR

1. Roof

Access from ground (Y/N)	Access from other buildings (Y/N)	Skylights or vents (Y/N)	Doors (Y/N)	Observations

2. Utility connections to building

Service	Location	Public Access (Y/N)	Secured (Y/N)	Location of Shut-Off	Observations
Phone					
Water					
Electrical					
Gas/Fuel					
Telecommunications					

3. Emergency power

Location	Fenced (Y/N)	Fuel Source	Self-start or manual	Service contract (Y/N)	Connections from Gen. to bldg. shielded/ secured (Y/N)

Observations

4. Doors (List every exterior door type: metal (m), glass (g), solid (s))

Side	Type	Type access control	Alarmed (Y/N)	Number of Doors / Observations

4a. Loading Dock (Y/N)

Location	Description	Observations

5. Windows (accessible)

Side	Operable (Y/N)	Alarmed (Y/N)	Barred (Y/N)	Treatment (Blinds, Curtains, Tinting)	Observations
A					
B					
C					
D					

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

6. Exterior wall lighting (Manual or automatic – when do they activate)

Side	Description	Observations
A		
B		
C		
D		

7. Exterior wall mounted closed circuit TV (Accessibility / height)

Side	Y/N	Monitored (Y/N)	Taped/Backed Up (Y/N)
A			
B			
C			
D			

8. Building Ventilation Intake

Location (include side and floor as appropriate)	Public Access (Y/N)	Secured (Y/N)	Observations

9. Underground Access and Facility? (Y/N)

Observations

Section II. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION III. SECURITY/ALARM SYSTEM

1. Type **Burglar** ☐ **Fire** ☐ **Panic** ☐

Central Station (Y/N)	Silent (Y/N)	Audible (Y/N)	Motion (Y/N)	Panic (Y/N)	Audio (Y/N)	Alarm Co. Name / Contact Person / Phone #

Observations

Name of Alarm Company	Contact Person	Phone #

2. Are There Private Security Personnel Assigned to the Facility/Infrastructure (Y/N) ☐

Name of Security Company	Contact Person	Phone #

3. Are There Law Enforcement Personnel Assigned to the Facility/Infrastructure (Y/N)

Name of L. E. Agency	Contact Person	Phone #

Section III. Comments

(Cellular back up, monitored or listening devices) (Average number of false alarms over the last six months) (Are regular tests provided) (Alarm response procedures) (Specificity of alarm, i.e., zone/sectors)

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

SECTION IV. POLICY/PROCEDURES

Is there a security plan in place? (Y/N)
If yes, obtain a copy of the plan.

Observations

1a. Is there a specified law enforcement component of the security plan? (Y/N)

Observations

1b. Do you have photo ID of employees? (Y/N)

Observations

1c. Are employee photo IDs required to be worn? (Y/N)

Observations

1d. Who manufactures/produces the badges or badge making equipment?

Name of Company	Contact Phone #

1e. Who controls the issuance of the badges?

Contact Person	Contact Phone #

1f. Are badges also used for doorway access control? (Y/N)

Observations

1g. What type of access control software system is in use?

Type	Observations

1h. Is access control software password protected for different users? (Y/N)

Observations

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

1i. Do procedures exist for activation/deactivation of access? (Y/N)

Observations

2. Is system in place to provide temporary ID cards to visitors/outside contractors/vendors/janitorial personnel in the facility? (Y/N)

Observations

2a. Is there a visitor log that reflects date, time, name, company, and vehicle information? (Y/N)

Observations

3. What system of key control is in place?

Findings	Observations

4. What person(s) outside of the agency have keys or codes to the facility?

Findings	Observations

4a. Who has master keys?

5. Do outside contractors/vendors/janitorial personnel check-in before providing service? (Y/N)

Observations

5a. Do they have a routine entry point and route of service? (Y/N)

Observations

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

6. Are Criminal Background Checks Provided on Outside Contractors/Outside Vendors/Janitorial Personnel? (Y/N)
National check ☐ State check ☐ Local check ☐

Observations

7. Are there re-opening/closing procedures in place to assure building security? (Y/N)

Observations

8. Does Facility Have a Lethal Cloud/Vapor Plume Distance Diagram or Emergency Contingency Plan/Procedures for Terrorist or Critical Incidents (including an evacuation plan and designated evacuation site)? (Y/N)

Observations

8a. Do Emergency Contingency Plan/Procedures specifically address protection f critical assets (e.g., water supply, ventilation equipment, electricity)? (Y/N)

Observations

9. Are the Employees trained in the Emergency Contingency Plans/Procedures? (Y/N)

Observations

9a. Are Emergency Evacuation Plans posted near Exits? (Y/N)

Observations

10. Are Emergency Plans/Procedures Routinely Practiced? (Y/N)

Observations

11. Are PSO/secretaries trained in Telephoned Bomb Threat Procedures? (Y/N)

Observations

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

12. Are PSO/Secretaries trained in Mail Handling Security Procedures? (Y/N)

Observations

13. Are there in place procedures which define proper response following inquiries about, or intrusions against, facility security design or procedures? (Y/N)

Observations

14. Is There an Active System in Place to Identify and Prevent Cyber Attacks? (Y/N)

Observations

15. Are Procedures in Place to Report All Cyber Attacks to the National Infrastructure Protection Center or the Regional Domestic Security Task Force? (Y/N)

Observations

Section IV. Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Digital Ground Photo of
Infrastructure/Facility

Aerial Photo of
Infrastructure/Facility
(if available)

Confidential – Law Enforcement Sensitive

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Section No.	Additional Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Section No.	Additional Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Section No.	Additional Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Section No.	Additional Comments

The purpose of this survey is to provide security observations. This report is only advisory and is not intended to identify all security weaknesses or to warrant the adequacy of all present and future security measures whether or not recommended.

Annex A. Hospitals

1.	Where are bulk oxygen and chemical tanks located?
	Are tanks accessible? (Y/N)
	Are fuel sources nearby? **(Y/N)**
	Power sources? **(Y/N)**

2.	Are personal oxygen tanks stored in accordance with OSHA standards? **(Y/N)**

3.	Are radiological materials stored on site? **(Y/N)**
	What is the level of the material?
	What is the half-life?
	Who has access?
	Is there an access roster? **(Y/N)**
	Are background checks performed on those with access? **(Y/N)**
	What level?

4.	Where is the pharmacy and satellite pharmacy (if applicable) located?
	Are the doors secured? **(Y/N)**
	Is electronic access employed? **(Y/N)**
	Is delivery of medications monitored from the receiving dock to the pharmacy? **(Y/N)**
	Is there a security window for disbursement of medications? **(Y/N)**
	Is video surveillance employed? **(Y/N)**

5.	Is there a helipad? **(Y/N)**
	Is it secured? **(Y/N)**
	Is the helipad under video surveillance? **(Y/N)**

6.	What type of monitoring is employed at the ER entrance?
	Are there guards? **(Y/N)** How many? Are they armed? **(Y/N)**

7.	Badge System
	What type of badge system is in place?
	Is the badge system controlled and enforced? **(Y/N)**
8.	Is access to the newborn and pediatric wards controlled?
	How?
	Is video surveillance employed? **(Y/N)**

9.	Mass Casualty Plan
	Is a plan in place? **(Y/N)**
	Who is the administrator?
	Is an emergency evacuation/shelter plan in place? **(Y/N)**
	Is there a lock down procedure in place to prevent a mass casualty/contamination on the facility? **(Y/N)**
	Is there an emergency decontamination plan for the facility, patients, staff, and outside mass casualties seeking assistance? **(Y/N)**

10.	Is liaison established with local enforcement agencies? **(Y/N)**

Annex B. Stadiums

1.	Security
	Does the security provide adequate coverage of key areas and entrances? (Y/N)
	Are background checks conducted on contract security employees? **(Y/N)**
	What level?
	Do security personnel receive threat indicator training? **(Y/N)**
	Are they trained in recognition of Bomb/Improvised Explosive Devices? **(Y/N)**
	What are the procedures if an explosive or chemical device is found?
	Are radio communications employed to link all security personnel? **(Y/N)**
	Does a line of communication exist between the local law enforcement and the stadium security to receive intelligence updates and the latest potential threat information? **(Y/N)**
	Does security check all doors after shutdown? **(Y/N)**
	Are roving patrols used before/during the game? **(Y/N)**
	Are guards at entrances/exit points when fans are present? **(Y/N)**
	Where are guards and law enforcement located throughout the stadium?
	Are counter-sniper assets used? **(Y/N)**
	Are undercover units utilized during the game? **(Y/N)** Roving? **(Y/N)**

2.	Canine units
	Does the stadium utilize canine patrols? **(Y/N)** How many?
	Are they utilized prior to the game and during? **(Y/N)**
	How many hours do they work?

3.	Tailgate area
	Are vehicles screened prior to entry to tailgate area? **(Y/N)**
	Are canine units (bomb detection) utilized in the area? **(Y/N)**
	Do undercover units patrol the area? **(Y/N)**

4	Emergency Medical Plan (EMP)
	Who is the EMP coordinator?
	What is the mass evacuation, mass decontamination, and mass triage plan?
	Have mutual aid agreements been signed between all local EMS, fire departments, and Local, State and Federal law enforcement agencies? **(Y/N)**
	Has an off-site command center been established before the game? **(Y/N)**

5.	Safety
	Who is the safety coordinator?
	Are plans posted regarding bomb threats, false alarms, evacuations, loss of utilities, and civil disorder? **(Y/N)**
	Are false alarms and threats documented? **(Y/N)**

6.	FAA
	Is the FAA contacted prior to the game to ensure a no fly zone over the stadium? **(Y/N)**
	Is there an early warning and notification system in effect? **(Y/N)**

7.	Inspections
	Are packages, backpacks and purses checked? **(Y/N)**
	Are metal detectors utilized? **(Y/N)**
	Is the stadium shut down 24 hours prior to game and inspected by canine units? **(Y/N)**
	Is security posted after shut down? **(Y/N)**
	Are trash containers emptied prior to and during the game? **(Y/N)**
	Are vehicles parked near the stadium inspected? **(Y/N)**
	Are trash trucks inspected before removing trash? **(Y/N)** Are they empty before they arrive? **(Y/N)**
	Are all doors to restricted areas secured and checked before the game? **(Y/N)**
	Does the stadium maintain a list of prohibited items at each entrance? **(Y/N)**

Annex C. Chemical Plants

1.	Risk Assessment and Prevention Strategies
	What are all key facility assets?
	Has a chemical hazard evaluation been performed? **(Y/N)**
	Has a process hazard analysis been performed? **(Y/N)**
	Has a consequence assessment been performed? **(Y/N)**
	Has a security assessment/ gap analysis been performed? **(Y/N)**
	Have rings of protection been developed? **(Y/N)**

2.	Management Issues
	Does the company's top management visibly support security efforts? **(Y/N)**
	Have clear security policies been developed and promulgated? **(Y/N)**
	Have partnerships with local, state, and federal law enforcement agencies, Other public safety agencies, and surrounding communities been established? **(Y/N)**
	Have relationships and procedures with other management functions to been clarified to provide a more coordinated response to security incidents? **(Y/N)**
	Is there a well-understood system for employees to report security incidents? **(Y/N)**
	Is there a system for collecting and analyzing reports of security incidents? **(Y/N)**
	Is there a security awareness program for employees and contractors? **(Y/N)**
	What is the procedure for referring suspicious incidents and breaches of company Policy to corporate counsel or corporate security management? **(Y/N)**
	What is the policy of referring all suspected illegal activity to law enforcement?
	What are the procedures for emergency response and crisis management?
	Is the site's security posture periodically reassessed (threats, vulnerabilities, risks, and countermeasures)? **(Y/N)**

3.	Physical Security
	Are appropriate access control measures in place, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of Gates and docks? **(Y/N)**
	Does the facility need security officers, on patrol or at fixed locations? **(Y/N)** If so, do they have written Post orders to direct their activity? **(Y/N)**
	Are crucial communications equipment and utilities appropriately protected? **(Y/N)**

4.	Employee and Contractor Security
	Have appropriate security practices been developed for voluntary and involuntary terminations Of employment? **(Y/N)**
	Are policies and established procedures been adopted to prevent and respond to workplace Violence? **(Y/N)**

5.	Information, Computer, and Network Security
	Have steps been taken (through the Operations Security, or OPSEC, process) to protect information that could be of used by our adversaries? **(Y/N)**
	Are procedures followed to reduce the likelihood that spoken information (in face-to-face conversations, phone calls, and radio communications) could be picked up by adversaries? **(Y/N)**
	Are procedures followed for protecting and destroying sensitive documents? **(Y/N)**
	What are the hardware, software, and procedural techniques for protecting Computers and networks?

6.	Safety
	Who is the safety coordinator?
	Are plans posted regarding bomb threats, false alarms, evacuations, loss of utilities, and civil disorder? **(Y/N)**
	Are false alarms and threats documented? **(Y/N)**
	Are computer transaction histories periodically analyzed to look for irregularities that might indicate security breaches? **(Y/N)**

Annex D. Airports

1. Badge System
What type of badge system is in place?
Is the badge system controlled and enforced? **(Y/N)**

2. Employee and Contractor Security
Have appropriate security practices been developed for voluntary and involuntary terminations of employment? **(Y/N)**
Are policies and established procedures been adopted to prevent and respond to workplace Violence? **(Y/N)**

3. Physical Security
Are appropriate access control measures in place, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of Gates and docks? **(Y/N)**
Does the facility need security officers, on patrol or at fixed locations? **(Y/N)** If so, do they have written Post orders to direct their activity? **(Y/N)**
Are crucial communications equipment and utilities appropriately protected? **(Y/N)**

4. Inspections
Are luggage, mail and freight shipments checked? **(Y/N)**
Are metal, radiological detectors utilized? **(Y/N)**
Are vehicles allowed unattended near the airport facility inspected? **(Y/N)**
Are parking garages electronically monitored?
Are vehicle license tags recorded?
Are all doors to restricted areas secured and checked throughout the day? **(Y/N)**

5. Safety
Who is the safety coordinator?
Are plans posted regarding bomb threats, false alarms, evacuations, loss of utilities, and civil disorder? **(Y/N)**
Are false alarms and threats documented? **(Y/N)**

Annex E. Ports

1.	Badge System
	What type of badge system is in place?
	Is the badge system controlled and enforced? **(Y/N)**

2.	Risk Assessment and Prevention Strategies
	What are all key facility assets?
	Has a chemical hazard evaluation been performed? **(Y/N)**
	Has a process hazard analysis been performed? **(Y/N)**
	Has a consequence assessment been performed? **(Y/N)**
	Has a security assessment/ gap analysis been performed? **(Y/N)**
	Have rings of protection been developed? **(Y/N)**
	Have relationships and procedures with other management functions to been clarified to provide a more coordinated response to security incidents? **(Y/N)**
	Is there a well-understood system for employees to report security incidents? **(Y/N)**
	Is there a system for collecting and analyzing reports of security incidents? **(Y/N)**
	Is there a security awareness program for employees and contractors? **(Y/N)**
	What is the procedure for referring suspicious incidents and breaches of company Policy to corporate counsel or corporate security management? **(Y/N)**
	What is the policy of referring all suspected illegal activity to law enforcement?
	What are the procedures for emergency response and crisis management?
	Is the site's security posture periodically reassessed (threats, vulnerabilities, risks, and countermeasures)? **(Y/N)**

3.	Where are bulk fuel and chemical tanks located?
	Are tanks accessible? **(Y/N)**
	Are fuel sources nearby? **(Y/N)**
	Power sources? **(Y/N)**

4.	Mass Casualty Plan
	Is a plan in place? **(Y/N)**
	Who is the administrator?
	Is an emergency evacuation/shelter plan in place? **(Y/N)**
	Is there a lock down procedure in place to prevent a mass casualty/contamination on the facility? **(Y/N)**
	Is there an emergency decontamination plan for the facility, patients, staff, and outside mass casualties seeking assistance? **(Y/N)**

5.	Employee and Contractor Security
	Have appropriate security practices been developed for voluntary and involuntary terminations Of employment? **(Y/N)**
	Are policies and established procedures been adopted to prevent and respond to workplace Violence? **(Y/N)**

6.	Physical Security
	Are appropriate access control measures in place, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of Gates and docks? **(Y/N)**
	Does the facility need security officers, on patrol or at fixed locations? **(Y/N)** If so, do they have written Post orders to direct their activity? **(Y/N)**
	Are crucial communications equipment and utilities appropriately protected? **(Y/N)**

7.	Inspections
	Are deliveries, inbound and outbound shipments checked? **(Y/N)**
	Are radiological detectors utilized? **(Y/N)**
	Are port personnel screened upon each trip onto port property? **(Y/N)**
	Are security posts operational 24 hours per day? **(Y/N)**
	Are vehicles allowed near on/off loading berths? **(Y/N)**
	Are all gates to restricted areas secured and checked throughout the day? **(Y/N)**

8.	Safety
	Who is the safety coordinator?
	Are plans posted regarding bomb threats, false alarms, evacuations, loss of utilities, and civil disorder? **(Y/N)**
	Are false alarms and threats documented? **(Y/N)**

Annex F. Schools

1.	Badge System
	What type of badge system is in place permanent/ part-time staff and teachers?
	Is the badge system controlled and enforced? **(Y/N)**

2.	General Security
	Does the security plan provide adequate coverage for key areas and entrances? **(Y/N)**
	Are background checks conducted on all staff and volunteer employees? **(Y/N)**
	What level (local, state, national)?
	If school police are utilized, do personnel receive threat indicator training? **(Y/N)**
	Are they trained in recognition of Bomb/Improvised Explosive Devices? **(Y/N)**
	Are plans in place, in the event an explosive or chemical device is found?
	Are parents informed where to pickup children in the event of an emergency?
	Are drills regularly conducted on evacuation plans?
	Are key staff positions able to communicate in the absence of hard-line telephone service? **(Y/N)**
	Does a line of communication exist between the local law enforcement and the school security to receive intelligence updates and the latest potential threat information? **(Y/N)**
	Are school resource or school police officers utilized as roving patrols on campus throughout the school day? **(Y/N)**
	Are security personnel at drop off and pickup points at the start and end of the school day? **(Y/N)**
	Where are security personnel located throughout the school day?
	Are appropriate access control measures in place, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of gates and docks? **(Y/N)**

3.	Employee / Student / Volunteer Security
	Have appropriate security practices been developed for voluntary and involuntary terminations Of employment? **(Y/N)**
	Are policies and established procedures been adopted to prevent and respond to School Violence? **(Y/N)**

4.	Inspections
	Are random checks done of packages, backpacks and lockers? **(Y/N)**
	Are metal detectors utilized? **(Y/N)**
	Are driver's education vehicles accounted for each day? **(Y/N)**
	Are parking areas monitored throughout the school day? **(Y/N)**
	Are all doors to restricted areas secured and checked each school day? **(Y/N)**

PART III: ASSESSMENTS

Chapter 3: DOJ Vulnerability Assessment Model

The Option One self-assessment entails completing the single-page worksheet provided below. This evaluation process can be completed in approximately 15 minutes. This DOJ model is based on scoring the following seven factors:

1. *Visibility*—How visible is the location without a dedicated search?
2. *Criticality*—How critical is the location to the operation of the daily activities of the facility?
3. *Value*—What is the value to potential terrorist element (PTE)? This factor evaluates the target's value in meeting the PTE's goals based on their motivations.
4. *Site population*—What is this location's maximum capacity during the course of the day?
5. *Collateral damage*—What can be expected in terms of damage outside the target area?
6. *Access*—What is the ease or difficulty of access to this location?
7. *Threat of hazard*—What is the potential for use of WMD materials in quantities that would expend internal response capabilities?

Steps

1. Duplicate the worksheet so a clean copy is available for later use.
2. Use one form for each facility.
3. Evaluate each of the seven areas listed, then enter the selected point value in the Summary Section.
4. Total the seven areas.
5. Use the Vulnerability Assessment Key to determine the risk level.
6. Enter the score and risk level at the top of the sheet and transcribe it to the designated facility protective measures matrix.

Complete the worksheet on the following page using the instructions provided above or those included in the bottom right corner of the worksheet. Upon completion of the worksheet, use the risk level outcome as the "data input key" necessary for use in the Protective Measures Database.

The DOJ model has been used successfully throughout government and is a relatively simple way to obtain a score for your facility and determine if it is high, medium, or low risk. It is relatively simple because it does not factor in all parameters that may be present in your facility—it is designed primarily to determine the potential casualty rate in the event of a WMD attack.

Exhibit 1 to Assessments DOJ Model

Individual Facility Vulnerability Worksheet

1. Level of visibility – Addresses the Awareness of Facility Existence and Visibility of Facility

Value

0=Invisible-classified location

1=Very low visibility – probably not aware of its existence

2=Low visibility- probably not well known existence

3=Visibility – existence is probably known

4=High visibility – existence well known

5=Very high visibility – existence is obvious

2. Criticality of target site to jurisdiction

Usefulness to population, economy, government, etc. deemed critical to the continuity of basic jurisdiction

Value

0=No usefulness
1=Minor usefulness
2=Moderate usefulness
3=Significant usefulness
4=Highly useful
5=Critical

3. Value of Facility to Potential Terrorist Elements (PTE) (evaluates target worth to serve PTE ends identified in threat assessment based on motivation)

Value

0=None
1=Very low
2=Low
3=Medium
4=High
5=Very high

4. Site Population Capacity (maximum number of individuals at any given time)

Value

0=0
1= 1-250
2= 251-500
3= 501-1000
4= 1001-5000
5= >5000

5. Potential for Collateral Mass Casualties (number ranges indicate inhabitants within a 1-mile radius of site)

Value

0= 0-100
1= 101-500
2= 501-1000
3= 1001-2000
4= 2001-5000
5= >5000

6. Potential Terrorist Element Access to Facility – evaluates the availability of ingress and egress by a PTE

Value

0=Fenced, guarded, protected air/consumable entry, controlled entrance by-pass only, no vehicle parking within 50 feet.

1=Fenced, guarded, protected air/consumable entry, controlled access of visitors and non-staff personnel, no vehicle parking within 50 feet.

2=Protected air/consumable entry, controlled access of visitors and non-staff personnel, no vehicle parking within 50 feet.

3=Controlled access of visitors, unprotected air/consumable entry, no unauthorized vehicle parking within 50 feet.

4=Open access to all personnel, unprotected air/consumable entry, no unauthorized vehicle parking within 50 feet.

5=Open access to all personnel, unprotected air/consumable entry, vehicle parking within 50 feet.

7. Target Threat of Hazard – assess the presence of WMD materials (BNICE) in quantities that would expend internal response capabilities if released.

Value

0= No WMD materials present

1= WMD materials present in moderate quantities, under positive control, and in secured locations.

2= WMD materials present in moderate quantities and controlled.

3= Major concentrations of WMD materials that have established control features and are secured in the site.

4= Major concentrations of WMD materials that have moderate control features.

5= Major concentrations of WMD materials that are accessible to non-staff personnel.

Summary

Score
_____1. Visibility
_____2. Criticality
_____3. Value
_____4. Site Population
_____5. Collateral Damage
_____6. Access
_____7. Threat of Hazard

_____TOTAL

Individual Facility Vulnerability **Assessment Key**

0-2 pt. = 1	Low Risk
3-5 pt. = 2	
6-8 pt. = 3	
9-11 pt. = 4	
12-14 pt. = 5	Medium Risk
15-17 pt. = 6	
18-20 pt. = 7	
21-23 pt. = 8	
24-26 pt. = 9	High Risk
27-29 pt. = 10	
30-32 pt. = 11	
33-35 pt. = 12	

Instructions for Worksheet

1. Duplicate this form.
2. Use one form for each facility.
3. Evaluate each of the seven areas listed. Enter selected point value in the Summary Section.
4. Total the seven areas
5. Use the VA Key to determine risk level.
6. Enter the score and risk level at the top of the sheet and transfer it to the designated facility protective measures matrix.

PART III: ASSESSMENTS

Chapter 4: DoD Vulnerability Assessment Model

The DoD uses several types of vulnerability assessment tools to determine asset risk levels. One of the more objective and uncomplicated tools DoD uses is the **MSHARPP** model, which is used to narrow the margin in determining the most plausible, lucrative terrorist targets. This tool uses a slightly more refined and objective scoring methodology than the DOJ model and requires roughly twice the time to complete the scoring process (30 to 40 minutes). This model pits specific threats against facility categories and expects scores to aid users in designing protective measures. Agencies can use this scoring methodology matrix to identify and prioritize their most compelling protection concerns. Each letter in the MSHARPP acronym represents a vulnerability consideration:

- **1. M**ission
- **2. S**ymbolism
- **3. H**istory
- **4. A**ccessibility
- **5. R**ecognizability
- **6. P**opulation
- **7. P**roximity

- ***Mission***—Mission focuses on the situations, activities, capabilities, and resources that are vulnerable to a terrorist attack. What is the importance of the area or assets, considering their functions, inherent nature, and monetary value? What are the ramifications of a terrorist attack, considering the psychological, economic, and sociological impacts? How long will it take to recover from an attack, considering the availability of resources, parts, expertise and manpower, and redundancies?
- ***Symbolism***—Does the target have a symbolic significance? Could it be perceived to represent government authority or U.S. colonialism (e.g., a company headquarters for an overseas operation or perhaps buildings where federal agencies are located)?
- ***History***—Do terrorist groups (particularly any local terrorist or extremist groups) have a history of attacking this type of target?
- ***Accessibility***—How easy is it to approach the target? Is it an open site or facility? Does the security force appear vigilant? Is a standoff distance or a fixed perimeter established? Can a person enter the target unchallenged? Can the target be attacked with a low chance of being thwarted?
- ***Recognizability***—Is the target easy to recognize? Can it be readily located and identified by a terrorist?
- ***Population***—What is the population relative to the populations of other potential targets in the area or region? A basic assumption is that the higher the population, the more attractive it is as a terrorist target.
- ***Proximity***—Is the target located near a residential area or is it near a highly populated area made up of apartment complexes, schools, or churches, which might make it a more attractive target to terrorists? Collateral damage may deter or encourage terrorists. A target located near another desirable facility may increase the attractiveness of that target.

The purpose of the MSHARPP model is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy (terrorists), and variables affecting the disposition (e.g., "attractiveness" or potential psychological effect on the community) of potential targets.

After developing a list of potential terrorist targets (e.g., buildings), use the MSHARPP selection factors to further refine your assessment by determining the most efficient, effective, and plausible method of attack and identifying vulnerabilities to that type of attack. After assigning the MSHARPP values (using the score scales below) for each target or component, the sum of the values indicates the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities. Using the acronym as a step-by-step guide, the process begins with evaluating the "Mission" (M).

1. Mission

Mission focuses on the situations, activities, capabilities, and resources at an agency or activity that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities necessary to accomplish the agency or company mission. When assessing points in this area, first review the following three components and determine whether an attack on mission components will cause degradation:

- *Importance*—measures the value of an area or assets located in the area, considering their functions, inherent nature, and monetary value.
- *Effect*—measures the ramifications of a terrorist incident in the area, considering the psychological, economic, and sociological impacts.
- *Recoverability*—the time required for the functions occurring at an area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.
- *Mission scores*—assign points to the target equipment, information, facilities (buildings), and/or operations or activities in this area using a scale of 1-5, with 5 being highest consequences, based on the degree of mission degradation should it be attacked by a terrorist.

Mission Criteria Scale

- **5 points:** An agency ***cannot continue*** to carry out its mission until the attacked asset is restored
- **4 points:** Ability to carry out a primary mission would be ***significantly impaired*** if this asset were successfully attacked
- **3 points:** ***Half*** of the mission capability would remain if the asset were successfully attacked
- **2 points:** The agency ***could*** continue to carry out its mission if this asset were attacked, but with some degradation in effectiveness
- **1 point:** Destroying or disrupting this asset would have ***no effect*** on the ability of the agency to accomplish its mission

2. Symbolism

Consider whether the target represents, or is perceived by the terrorist to represent, a symbol of a targeted group (e.g., democracy, Christianity, etc.).

Symbolism scores. Assess points in this area based on the symbolic value of the target to the enemy using a scale of 1-5, with 5 being worst.

Symbolism Criteria Scale
✹ **5 points**: High profile, direct symbol of target group or ideology
✹ **4 points**: Low profile, direct symbol of target group or ideology
✹ **3 points**: Low profile and/or obscure symbol of target group or ideology
✹ **2 points**: Asset is ***perceived to be vital*** to the mission
✹ **1 point**: Asset is ***not*** vital to the mission

3. History

Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities. Terrorist patterns often have indicated an organizational perseverance for attacking areas again after failed attempts.

History scores. Assess points in this area based on past targeting, including attacks on similar facilities and foiled attacks. Values of this category should rank on a scale of 3-5, with 5 being worst. Although the history score lists only three values, history has typically been a strong indicator of future attacks, and these numbers intentionally lean toward the high end of the scoring process.

History Criteria Scale
✹ **5 points**: ***Strong history*** of attacking this type of target
✹ **4 points**: History of attacking this type of target, but ***none in the immediate past***
✹ **3 points**: ***Little or no history*** of attacking this type of target

4. Accessibility

A target is accessible when a terrorist or terrorist group can reach it with sufficient personnel and equipment to accomplish its mission. Even a protected target can be accessible with the assistance of knowledgeable insiders (see definition of insider threat in the Glossary). The accessibility assessment entails identifying and studying critical paths that the terrorist must take to achieve its objectives and measuring those elements that aid or impede access. The enemy must not only be able to reach the target but also must remain there for an extended period. The four basic stages to consider when assessing accessibility are:

- Infiltration from the staging site to the target area
- Movement from the point of entry to the target or objective
- Movement to the target's critical element
- Exfiltration (getaway)

Accessibility scores. Assess points in this area based on ease of gaining unimpeded access to a facility with little or no warning to occupants, or limiting the impact of an attack on designated assets. Values of this category should rank on a scale of 3-5, with 5 being the most damaging.

Note: As with the history assessment, only three values are listed because accessibility is a key factor in denying terrorists the ability to attack specified targets; therefore, these numbers intentionally lean toward the high end of the scoring process.

Accessibility Criteria Scale
✹ **5 points**: ***Easily accessible***, standoff weapons can be employed
✹ **4 points**: Inside perimeter fence (if installed), ***climbing or lowering*** required
✹ **3 points**: Not accessible or ***accessible*** only with extreme difficulty

5. Recognizability

A target's recognizability is the degree to which it can be easily observed by terrorists under all weather conditions or can be easily viewed from a public access point without arousing suspicion. Weather has an obvious and significant impact on visibility (that of the surveillance systems used, yours and the enemy's). Rain, snow, and ground fog may obscure observation. Distance, light, and season must be considered. Other factors that influence recognizability include the size and complexity of the target and the technical sophistication and training of the enemy.

Recognizability scores. Assess points in this area based on the degree of being able to distinguish an asset as a target. Values of this category should rank on a scale of 2-5, with 5 being most damaging.

Note: Because only four factors are listed, the number "1" point value is not used.

Recognizability Criteria Scale
5 points: Target is ***clearly recognizable*** under all conditions and from a distance; requires little or no training for recognition
4 points: Target is easily recognizable and ***requires a small amount of terrorist training*** for recognition
3 points: Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition
2 points: Target ***cannot be recognized*** under any conditions—except by experts

6. Population

What is the population relative to other potential targets? Assuming that the intent of the attack is to kill or injure people, it follows that the more densely populated a site or building is, the more lucrative a target it makes (with all other factors being equal).

Population scores. Assess points in this area based upon the population density. Values of this category should rank on a scale of 1-5, with 5 being most damaging.

Population Criteria Scale
5 points: ***Densely populated***; prone to crowds
4 points: Relatively large numbers of people, but ***not in close proximity*** (i.e., spread out and hard to reach in a single attack)
3 points: The population is comprised of ***personnel deemed vital*** to the accomplishment of the agency's mission
2 points: Prone to ***small groups*** or individuals
1 point: Sparsely populated or ***unattended***

7. Proximity

Is the potential target located near other personnel, facilities, or resources that because of their intrinsic value or "protected" status and a fear of collateral damage afford it protection (e.g., near national monuments, protected religious symbols, etc., which terrorists find attractive as a target)?

It is important to consider whether the target is close to other likely targets. Just as the risk of inadvertent collateral damage may decrease the chances of attack, a "target rich" environment may increase the chances of attack.

Proximity scores. Assess points in this area based on the site's placement relative to other potential targets. Values of this category should rank on a scale of 1-5, with 5 being most damaging.

Note: As with the history and accessibility assessments, only three values are listed, because proximity is relatively simple to discern. However, these scores vary widely, depending on the factors assessed.

Proximity Criteria Scale

- **4-5 points**: Target is in ***close proximity***; serious injury/damage or death destruction of protected personnel/facilities likely
- **2-3 points**: Target is in close enough ***proximity*** to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction
- **1 point**: Target is ***isolated***; no chance of unwanted collateral damage to protected symbols or personnel

Application. After scoring each MSHARPP factor, the values should be transcribed into **figure 1**, the MSHARPP worksheet. Values from 1 to 5 are assigned to each factor based on the associated data for each target. "Five" represents the highest vulnerability or likelihood of attack and "1" the lowest. Accordingly, the higher the total score, the more vulnerable the target.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
									4,000 lb Truck Bomb
									220 lb Car Bomb
									Small Arms Attack
									7.62mm (Sniper)
									50 lb Satchel Charge
									Mortar
									Rocket Attack (RPG)
									Hand Grenade

Figure 1. MSHARPP Matrix

Begin by reviewing the threats listed in the right column. If these are not considered realistic, prevalent, or viable threats, modify the list accordingly. Next, list the target asset in the left column followed by the score for each of the noted factors from the explanations above. Combine (add) the scores and place the result in the "total" column. An example is provided in **figure 2**.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
Large Govt Agency	5	5	3	5	5	4	3	30	4,000 lb Truck Bomb
Large Govt Agency	4	5	3	5	5	3	2	27	220 lb Car Bomb
Large Govt Agency	3	5	3	5	5	3	2	26	Small Arms Attack
Large Govt Agency	2	5	3	5	5	2	2	24	7.62mm (Sniper)
Large Govt Agency	4	5	3	4	5	3	2	26	50 lb Satchel Charge
Large Govt Agency	4	5	3	5	5	3	2	27	Mortar
Large Govt Agency	4	5	3	5	5	2	2	26	Rocket Attack (RPG)
Large Govt Agency	3	5	3	4	5	2	2	24	Hand Grenade

Figure 2. MSHARPP Example Matrix (Single Facility)

The example shown in **figure 2** shows a single facility and the differences in scoring when facing different threats. The large government agency in this example represents a state administration facility.

The matrix in **figure 3** shows **various facilities** (noted as potential targets); the scores are based on the factors explained previously and potential threats (listed as weapons). This example captures the differences among multiple facilities facing differing threats.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
Large Govt Agency	5	5	3	5	5	4	3	30	4,000 lb Truck Bomb
College Dormitory	5	2	3	5	4	2	1	22	220 lb Car Bomb
Command Center	5	4	3	4	3	3	1	23	Small Arms Attack
Elementary School	2	4	4	5	5	5	1	26	7.62mm (Sniper)
Fuel Storage	4	4	3	4	3	1	1	20	50 lb Satchel Charge
Football Stadium	5	5	3	5	5	5	2	30	Mortar
State Capitol	5	5	4	3	5	4	1	27	Rocket Attack (RPG)
Electric Transformer	5	3	3	5	4	1	1	22	Hand Grenade

Figure 3. MSHARPP Example Matrix (Multiple Facilities)

Upon completion of the scoring process, review the risk matrix in **figure 4** to determine score ranges as they relate to risk. This risk "score" is used later when assigning mitigation strategies in the protective measures matrices.

MSHARPP Total Score	Risk Level
28–35 Points	High Risk
23–27 Points	Medium Risk
0–22 Points	Low Risk

Figure 4. Risk Matrix

The DoD model, as you can see, is more comprehensive than the DOJ model. This model has been used to determine the vulnerability or risk level of military and DoD facilities. Using seven factors, the "MSHARPP" matrix, determine your facility (building or site) risk score. Much the same as the DOJ model, it will give you quantifiable scores for high-, medium-, and low-risk facilities.

PART III: ASSESSMENTS

Chapter 5: AASHTO Model

Background

Although designed for surface transportation system analysis, the AASHTO methodology can be used to assess all classifications and types of both public and private sector critical infrastructure and other use categories. The Guide can be and has been used by state departments of transportation to:

- Assess the vulnerabilities of their physical assets, such as bridges, tunnels, roadways, and inspection and traffic operation facilities.
- Develop possible countermeasures to deter, detect, or delay the consequences of terrorist acts to such assets. Within separate protective measures matrices there is **a wide range of options for implementing mitigating options.**
- Estimate the capital and operating costs of such countermeasures.
- Improve security operational planning for better protection against future acts of terrorism. Provided at the end of this section is **a basic outline for a security protection plan.**

This AASHTO method can be used by senior state and local government officials and their security staff involved in the initial planning stage of the vulnerability assessment process, mid-level managers charged with developing the assessment plans and procedures, and field personnel who will conduct the assessments of government or other organization critical assets.

A Team Effort

In commencing the assessment, we recommend that the organization form and manage a multidisciplinary team whose members have a sound working knowledge of the key assets (including sites, facilities, equipment, and personnel). This will include knowledge of the organization's mission, critical assets, policies, plans, and procedures. This Guide identifies the types of resources typically required by a team to conduct a vulnerability assessment and describes the three major phases of the process—pre-assessment, assessment, and post-assessment.

This Guide provides managers with a road map and six steps for conducting a vulnerability assessment of the organization's critical facilities.

These six steps provide a straightforward method for examining critical assets and identifying cost-effective countermeasures to guard against terrorism. For each step, the objective is clearly stated, the practice of that step by other state and federal agencies is referenced, a detailed approach is described, and illustrative examples are provided.

Scope of the Assessment Methodology

This Guide is designed to allow facility managers, mid-level and senior government, or organization officials to "score" or rate their facility or infrastructure in an objective manner using a proven mathematical formula. Using the attributes and scoring system, managers can rate their vulnerability and criticality in clear terms and can rank them by priority for improvements. This Guide will address all areas of the state and local facilities and the private sector critical infrastructure.

Key asset vulnerabilities generally are categorized as follows:

- People

- Facilities (Property)
- Equipment (Resources)
- Criticality to:
  - Continuity of government (federal, state, local, or special district) (i.e., how your assets support the continuity of government)
  - Continuity of your operations (economic, command and control, safety of life, education, and public venues)
  - Quality of life (health, public safety, education, public works, energy, research labs, and transportation)
  - Information technology assurance

Assumptions

This vulnerability analysis combines a subjective analysis by the facility owner or user aided by security experts and a quantitative or scientific method to best assess or score a facility's vulnerabilities. It is not overly complex in scientific calculations, but is designed to go beyond the judgment of knowledgeable and experienced individuals.

One key assumption is that we no longer operate in a traditional threat environment. Today's threat is "asymmetric," or one in which terrorists use nontraditional and relatively low-cost weaponry (such as improved explosive devices and airplanes as WMD) to inflict catastrophic damage on large populations and property, instilling fear and panic or threatening to do so; and causing similar fear or panic or a loss of confidence in our ability to live "normal" lives within the United States.

Vulnerability to the asymmetric threat is more difficult to assess because we cannot predict with much certainty the time and place of an attack. However, we can make assumptions of terrorist capabilities based on previous acts and assess the consequences or resulting damage in terms of lives, property, and economic value.

In response to these threats, some of the best countermeasures may be in the areas of access control, surveillance, monitoring, standoff barriers, and procedural and practical measures of deterrence, awareness, and response tactics.

It is important that users of the vulnerability assessment guide presented have sufficient knowledge (or have readily available experts) of their facilities and structures. This knowledge will enable them to make the best use of this Guide.

This Guide will help users to divide the assessments into components in which informed judgments can be made and then "rolled up" to form a list of assets, threats, and countermeasures. This list provides decision makers with rankings for their infrastructures and for senior leaders of the necessary information for investment or capital budget purposes.

How to Use the AASHTO Model

This Guide is designed for state, local, and district levels of governments and other public or private organizations or agencies. It offers a general method that applies to all forms of infrastructure. Individual security managers will have to determine within their classification of facility or infrastructure the most critical assets and the less important ones. The Guide provides general attributes to consider in determining priority orders.

If an agency or organization has a vulnerability assessment structure, this Guide will assist in validating its method or provide methods for improvement or change.

General Approach

Figure 1 outlines the six steps used in conducting a vulnerability assessment.

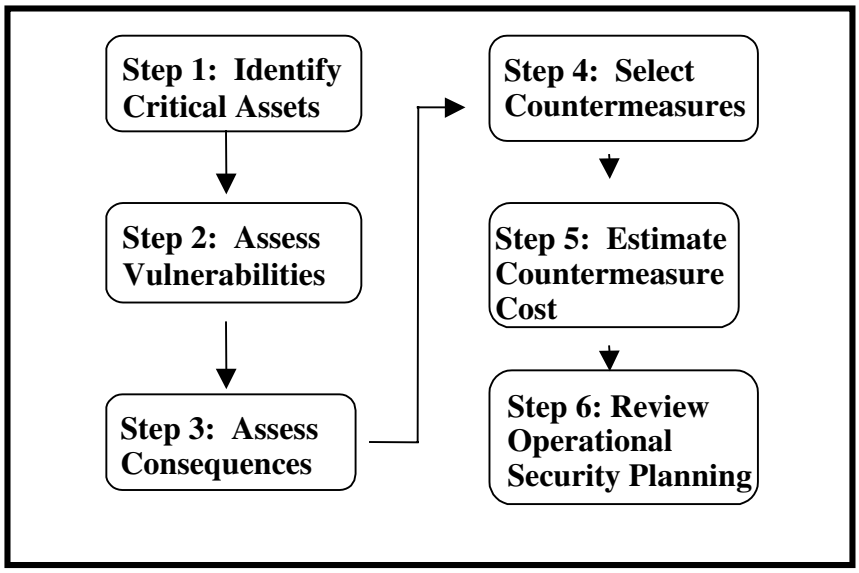


Figure 1. Six Steps for Conducting a Vulnerability Assessment

Team Composition

Team members from the agency, department, or organization should represent important department functions such as:

- Law enforcement—local, state, and (if possible) federal
- RDSTF representative
- Agency or department general management
- Agency or department security director or police chief
- Facilities engineering
- Design and planning
- Budget and fiscal
- Communications
- Safety
- Human resources
- Purchasing
- Maintenance

The team should obtain information on the threat from sources such as the Florida Office of Domestic Security and FDLE, and from county and local law enforcement officials. In most cases, these departments will provide threat data to other sworn officials within the jurisdiction, but some information regarding the threat may be general because sensitive intelligence data are not released outside of official law enforcement agencies.

The threat will likely be expressed in terms of likelihood of occurrence, because generally the timing and place of a terrorist event cannot be accurately predicted. The assessment is primarily designed to demonstrate the vulnerabilities of infrastructure assets and assist in determining the consequences of a terrorist attack or event at that facility.

To the extent possible, it is important to request public safety agencies (i.e., fire, police, first responders, HAZMAT and environmental protection) to assist in the threat and consequences assessment. However, these agencies may be limited in their ability to provide in-depth assistance because of demands on their time and limited resources. It is important to coordinate efforts and review findings with the applicable jurisdiction's state and local law enforcement officials whenever possible.

Department or organization managers of key assets should modify team membership as necessary to obtain a comprehensive input on the vulnerability assessment process.

Pre-Assessment Trial Run

If the department or organization has never conducted a vulnerability assessment (and to ensure that the team is well prepared to conduct the assessment), training exercises should be held before beginning the assessment. These training sessions may include a combination of classroom presentation and a tabletop exercise in which you select an agency facility or other key asset to evaluate. This exercise will help the team to reach agreement on terms, overall methodology and scoring process.

A tabletop exercise should simulate an actual vulnerability assessment, giving team members an opportunity to work through each of the steps and ask questions before they begin an actual assessment.

A team leader's responsibilities include:

- Providing technical direction and management of the team members
- Maintaining overall responsibility for team performance
- Ensuring access to technical and managerial resources
- Initiating quality control on all team activities
- Developing and monitoring schedule and cost control
- Maintaining communications with senior management

The composition of the team, number of members assigned, and level of experience and training will have a direct effect on the outcome and timetable of the vulnerability assessment. The team is responsible for selecting and assigning values to factors that determine the prioritization of the critical assets and identification of the most vulnerable assets.

Forming the Vulnerability Assessment Team

Team 1: Organization or Department Threat Working Group: Includes law enforcement, department managers, security managers, and public consultants, with input from federal, state, and local law enforcement agencies.

- Bring known threat to vulnerability assessment process (explained in the Security Policies section)
- Which determines the likelihood and assessment.

Team 2: Vulnerability Assessment Group: Includes design engineers, security specialists, and operating personnel familiar with the type or classification of facility

- Determines the vulnerability of the facility which then results in a criticality score
- Will determine the impact and assessment

Team 2 works through the vulnerability assessment process to evaluate critical assets within the department, facility, or critical infrastructure (CI) asset. Note that each organization or department CI asset will require different skills, knowledge, and experience.

Team 3: Mitigation Strategies Group: Includes department or organization security professionals/consultants, site managers, engineers, and others to suggest methods to reduce the likelihood of attack or reduce the impact if an attack occurs

- Formed to score assigned class of facilities
- Rates similar facilities in each class (telecommunications, public utilities, transportation, etc.) to determine criticality score and prioritization for mitigation
- Will determine the criticality and assessment score

Figure 2 represents the likely range of critical assets.

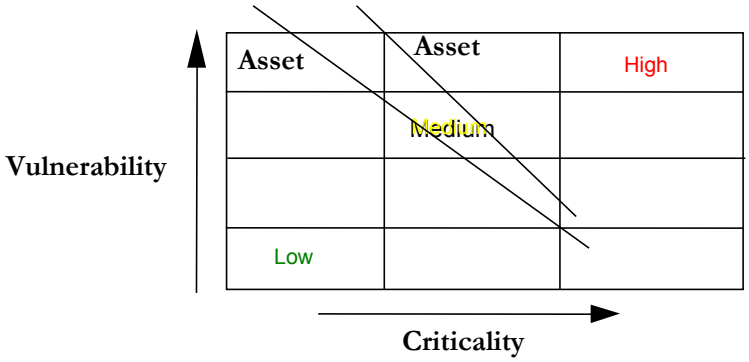


Figure 2. Possible Score Results (illustrative)

Required Resources and Level of Commitment

Support from senior management of the agency or organization sites and facilities being assessed is critical to a successful effort, especially as it affects the team's access to necessary resources and information. The following lists the types of resources typically required by a team to conduct a vulnerability assessment. Whenever possible, the data sources should be identified to help the team collect the information needed to conduct the assessment.

Resource List

- Organization, agency, or department asset data
  - Facility location and inventory list
  - HAZMAT information system
- Threat data related to key facilities
  - From previous efforts in this process (if any)
  - FDLE
  - Division of Emergency Management Agency
  - DHS
  - Appropriate federal, state, and local law enforcement/public safety agencies
  - Public consultants
  - Corporate security professionals
- Vulnerability data derived from this assessment process
- Consequence data
- Countermeasures data
- Cost data
- Policies, plans, and procedures
- Personnel (interviews)
- Geographic information systems (maps and drawings)

Getting Started

Because of the organization of this project, the vulnerability assessment in this chapter will be supported by an initial review of critical assets and a preliminary scoring of at least one component of critical infrastructure assets.

- *Phase I, Pre-Assessment*—The department, organization, or agency should assemble the assessment team. It is important to conduct team training exercises, contact appropriate external organizations, plan and schedule the vulnerability assessment process, and collect the required resources.
- *Phase II, Threat Assessment*—The department, organization, or agency CI assets to be assessed may already have a general threat and understands the likely scenarios and anticipated consequences.

  Armed with this information, the team will embark on the next task—the assessment phase—by using the above data, physically examining critical assets, interviewing personnel, assessing the data, conducting a scoring process using this Guide, and forwarding their scores to another group (if desired) to develop or make recommendations on the countermeasures.
- *Phase III, Post-Assessment (the final phase)*—The organization, department, or agency, working with either the same or a new team of professionals, develops a strategy for implementing protective measures (countermeasures). Details and processes for Phase III are contained in the matrices associated with this Manual.

Step 1—Asset Identification

Objective. For the state of Florida, the FDLE, Office of Domestic Security, has categorized state or local agency, publicly owned, or leased facilities as assets that must be assessed for criticality and vulnerability.

Approach. The state of Florida and local governments may use the following three-step approach to either validate an existing list or develop an initial list of critical assets.

1a. Create an All-inclusive List of Critical Assets. The FDLE, Office of Domestic Security, has already developed a list of all state and local government-owned or leased public facilities that are to be assessed for criticality. Essentially this step has been completed, but agency managers may add to the list. We do not recommend deleting any facilities without approval from senior management. Refer to the ***Introduction*** section chapters for a list of public, private, and special venue facilities.

1b. Establish and Assign Values to the Critical Asset Factors. Critical asset factors are the criteria used to identify and prioritize critical assets. Collectively, these factors are an indication of the conditions, concerns, consequences, and capabilities that might cause

government to label an asset "critical." The factors and associated values shown in **table 1** serve as a guide for scoring and ranking.

Critical Asset Factor	Max Value	Description
Deter/Defend Factors		
A) Ability to Provide Protection	1	Is there a system of measures to protect the asset?
B) Relative Vulnerability to Attack	2	Is the asset relatively vulnerable to an attack? (Judge on visibility, location, importance to the owning agency and the State of Florida)
Loss and Damage Consequences		
C) Casualty Risk	5	Is there the possibility of major loss of life/injury resulting from an attack on the asset?
D) Environmental Impact	1	Will an attack on the asset have a significant (expressed in terms of years) ecological impact of altering the environment (express in radius of to 3-5 miles or further
E) Replacement Cost	3	Will significant replacement cost (the current cost of replacing the asset with a new one of equal value) be incurred if the asset is attacked? Is replacement critical to the agency?
F) Replacement/Down Time	3	Will the attack on the asset cause significant replacement/down time?
Consequences to Public Services		
G) Emergency Response Function	5	Will the agency require an emergency response and will the action or activity of emergency response be affected?
H) Government Continuity	5	Is the asset necessary for maintaining local or state continuity of government?
I) Military Importance	5	Is the asset important to the overall security of the state and nation?
Consequences to the General Public		
J) Available Alternate	4	Is there a substitute that is designated to take the place of the asset, if necessary, to perform or provide the same level of service to the owning agency and the public?
K) Communication Dependency	1	Is the owning agency or the state dependent on the asset for communication?
L) Economic Impact	5	Will damage to the asset significantly impact the economy of the owning agency, region or state?
M) Functional Importance	2	Is there an overall value of the asset performing or staying operational?
N) Symbolic Importance	1	Does the asset have symbolic importance?

Table 1. Maximum Score (AASHTO Method) of Critical Asset Factors and Values

The samples listed in **table 2** are derived primarily from work done in the state of Texas, but are relevant to Florida as well, and are augmented by factors derived from the work of other states and federal agencies. The state of Florida and its local government agencies may choose to use this list as it is or adjust and augment the list based on their own needs.

Before beginning the assessment, the vulnerability assessment review team should agree on the list of factors and their individual values. Once the factors and values have been determined, this list must remain constant throughout the assessment. If the factor values and asset scores are not carefully examined for uniformity and consistency, multiple teams assigning critical asset factors and scores could result in inconsistencies in the prioritization of critical assets. If after beginning the assessment process, the team adjusts the critical asset factors or their respective values, the team may need to reassess some assets to ensure consistency.

The assigned factor values are based on the importance of the factor in labeling the asset as critical. The values assigned to factors range from "extremely important" (value of 5) to "less important" (value of 1).

	Critical Asset Factor														
CRITICAL ASSET (Examples Only)	**A 1**	**B 2**	**C 5**	**D 1**	**E 3**	**F 3**	**G 5**	**H 5**	**I 5**	**J 4**	**K 1**	**L 5**	**M 2**	**N 1**	**TOTAL SCORE (X)**
Asset 1 Miami Dade Central Public Safety Center															
Asset 2 Miami Dade FD Station 1															
Asset 3 Miami Dade FD Station 3															
Asset 4 Miami Dade FD Station 4															
Asset 5 Miami Dade FD Maintenance Building															
Asset 6 Miami Dade Fire Training Academy															

Table 2. Sample Score Sheet for Public Safety Asset—Miami Dade Metro Public Safety (Fire Department) Facilities

Note: The assignment of these factor values to assets is binary. If the critical asset factor applies to the asset being evaluated, the asset receives the value assigned to that factor. However, if the factor does not apply, the asset is assigned a value of 0 for that factor.

The state of Florida may set the values in terms of dollars, as one example, that distinguish between different levels. For example, if Florida chooses to distinguish between "medium" and "major" economic impact, the team might assign the factor "medium economic impact" a value of 3 and the factor "major economic impact" a value of 5. (Note: The state can set economic impact figures for the values 0 through 5 as well, such as <$50,000 as 0 and correspondingly >$100,000 as 5.)

Note: Because every asset is assessed for every factor (**table 2**) adding more factors increases the number of judgments required. The Texas model shown in **figure 2** has 14 factors to consider (A through N).

1c. Prioritize the All-Inclusive List of Critical Assets. In this step, the assessment team assigns priorities to the assets or facilities being evaluated or assessed. The letters A through N in **table 2** correspond with the critical asset factors listed in **table 1**. For each asset, the applicable critical asset factor values are entered. The sum of these values (x) represents the total score for the asset being evaluated. These scores are ordered from highest to lowest. The total score for the most critical facilities (assets) are used later in Step 3. The maximum possible criticality value (C_{max}) for each agency or facility will vary depending on the values assigned to critical asset factors in **table 1**.

The total score calculated in this step (x) will be used in calculating the criticality coordinate of each asset (x) in Step 3 as follows:

Criticality coordinate (X) = $(x/C_{max})*100$

Although the AASHTO Guide cautions against having too many critical assets, this project requires that all publicly owned or leased facilities (state and local governments, including special districts) be provided a vulnerability assessment in order to implement security best practices.

	Critical Asset Factor														
CRITICAL ASSET (Examples Only)	**A 1**	**B 2**	**C 5**	**D 1**	**E 3**	**F 3**	**G 5**	**H 5**	**I 5**	**J 4**	**K 1**	**L 5**	**M 2**	**N 1**	**TOTAL SCORE (X) 43**
Asset 1 Miami Dade Central Public Safety Center	1	2	4	1	2	3	5	5	4	3	1	4	2	1	38
Asset 2 Miami Dade FD Station 1	1	2	3	1	2	2	4	3	2	3	3	2	2	1	31
Asset 3 Miami Dade FD Station 2	1	2	2	1	1	2	3	3	1	1	2	2	2	1`	24
Asset 4 Miami Dade FD Station 3	1	2	2	1	1	2	3	2	1	1	1	1	1	1	20
Asset 5 Miami Dade FD Maintenance Building	1	2	1	1	1	2	3	2	1	1	1	1	1	1	19
Asset 6 Miami Dade Fire Training Academy	1	2	1	1	1	1	1	1	1	1	1	1	1	1	15

Table 3. Hypothetical Example of Completed "Score Sheet" of Miami Dade Public Safety (Fire Stations)

Explanation for the Scores Given Each Asset for the Miami Dade Fire Stations:

Asset 1—Primary Miami Dade public safety center has high visibility, is essential to government continuity of operations, and probably houses essential first responder equipment for high-rise buildings and technical rescue.

Asset 2—Miami Dade Fire Station 1 is an essential facility, probably stands alone and houses essential equipment, but is not a hub for command and control of the fire department.

Asset 3—Miami Dade Fire Station 2 would probably be suburban rather than urban and service area may consist of fewer high-rise and unique buildings.

Asset 4—Miami Dade Fire Station 3 (and others). These facilities probably serve a suburban to rural area, mostly family dwellings and retail/warehousing. Equipment could be housed in temporary facilities and probably would have redundant response capability (i.e., could be used to help other areas or fire stations).

Asset 5—Miami Dade Fire Department maintenance facility, although important to the operation of the fire department, if lost could relocate or subcontract general repairs to its equipment.

Asset 6—Miami Dade Fire Academy consists mostly of academic facilities—activities could probably be relocated to another academic facility or the Academy could temporarily use other agency exercise and drill facilities (fire training/tower).

Step 2—Vulnerability Assessment

Objective. A vulnerability assessment is designed to systematically identify and evaluate critical assets in terms of their susceptibility to terrorist attacks and the consequences of such attacks on the assets. The process below, as developed for state departments of transportation, identifies exposures and weaknesses that can be exploited by terrorists.

Approach

2a. Characterize the Threat. The state of Florida has determined that the "normal" threat posture is considered "Elevated" or color code "Yellow." This means that senior domestic security, intelligence, and law enforcement officials in Florida, supported by the governor and the state legislature, have established the threat baseline as a starting point in order to apply recommended protective measures (security best practices).

Earlier in this Manual, we provided background information on how the Homeland Security Threat Advisory System functions. Use of this threat warning system and knowledge of potential threats should enable managers to consider plausible attack scenarios against various assets. Developing a list of types of threats is crucial to moving forward and implementing protective measures to mitigate those threats.

2b. Assign Vulnerability Factors to the Critical Assets. This Guide uses the vulnerability factors in **table 4** to analyze the potential vulnerabilities of critical assets.

Vulnerability Factor	Definition
Visibility and attendance	Awareness of the existence of the asset and the number of people typically present
Access to the asset	Availability of an asset to ingress and egress by a potential threat element
Site-specific hazards	Presence of materials with biological, nuclear, incendiary, chemical, or explosive properties in quantities that would expend initial response capabilities if compromised
Off-site hazards	Potential for damage due to the relative proximity of other threat targets (e.g., facilities or material storage tanks)

Table 4. Vulnerability Factor Definitions

Each vulnerability factor is comprised of two sub-elements. These sub-elements will be used to calculate the vulnerability factor in the next section.

For the sub-elements shown in **table 5**, values ranging from extremely important (5) to less important (1) are assigned. **Table 6** indicates typical values assigned for the vulnerability factor sub-elements.

Note: The scores assigned to the assets should reflect judgments made based on analyses regarding the existence and capabilities of real or potential threats to the assets as discussed in Sub-step 2a above.

Vulnerability Factor	First Sub-element	Second Sub-element
Visibility and attendance	Level of Recognition (A)	Attendance/Users (B)
Access to the asset	Access Proximity (C)	Security Level (D)
Site-specific hazards	Receptor Impacts (E)	Volume (F)
Off-site hazards	Proximity (G)	Category (H)

Table 5. Vulnerability Factor Sub-Elements

Note: To determine the standards for "D" Security Level, in **table 6**, protected access is defined as structural and/or electronic security measures such as fencing, intrusion detection alarms, cameras, or locks. Controlled access is defined as entry validated by personnel such as armed or unarmed guards. Response force signifies that personnel are available to respond to either protected or controlled access violations.

Vulnerability Factor and Default Value			Definition
Visibility and Attendance	LEVEL OF RECOGNITION (A)	1	Largely invisible in the community
		2	Visible by the community
		3	Visible statewide
		4	Visible nationwide
		5	Visible worldwide
	ATTENDANCE/ USERS (B)	1	Fewer than 10
		2	10 to 100 (major incident per Federal Emergency Management Agency [FEMA])
		3	100 to 1000
		4	1,000 to 3,000
		5	Greater than 3,000 (catastrophic incident per FEMA)
Access to the Asset	ACCESS PROXIMITY (C)	1	Asset with no vehicle traffic and no parking within 50 feet
		2	Asset with no unauthorized vehicle traffic and no parking within 50 feet
		3	Asset with vehicle traffic but no unauthorized vehicle parking within 50 feet
		4	Asset with vehicle traffic but no unauthorized vehicle parking within 50 feet
		5	Asset with open access for vehicle traffic and parking within 50 feet
	SECURITY LEVEL (D)	1	Controlled and protected security access with a response force available
		2	Controlled and protected security access without a response force
		3	Controlled security access but not protected
		4	Protected but not controlled security access
		5	Unprotected and uncontrolled security access
Site-Specific Hazards	RECEPTOR IMPACTS (E)	1	No environmental or human receptor effects
		2	Acute or chronic toxic effects to environmental receptors
		3	Acute and chronic effects to environmental receptors
		4	Acute or chronic effects to environmental and human receptors
		5	Acute and chronic effects to environmental and human receptors
	VOLUME (F)	1	No materials present
		2	Small quantities of a single material present
		3	Small quantities of multiple materials present
		4	Large quantities of a single material present
		5	Large quantities of multiple materials present
Off-Site Hazards	PROXIMITY (G)	1	Small or no hazards nearby (within 300 feet)
		2	Medium hazard is over 1,000 feet away
		3	Medium hazard is over 500 feet away
		4	Large hazard is within 2,000 feet for potential damage
		5	Large hazard is within 1,000 feet for potential damage
Off-Site Hazards	CATEGORY (H)	1	No facilities or hazards are present that could damage the facility
		2	Small hazards (e.g., transportation workshop) are present that could damage the facility
		3	Medium hazards (e.g., state administration building) are present that could damage the facility
		4	Multiple medium hazards (e.g., national monument and state university) are present that could damage the facility
		5	Large hazards (e.g., multistory federal building or oil refinery) are present that could significantly damage the facility

Table 6. Vulnerability Factor Default Values and Definitions

2c. Score the Vulnerability Factor for Each Asset. In this step, the following formula is used to calculate the vulnerability factor (y) (note that the criticality factor [x] was done in Step 1c) for each asset. In the formula used, the sub-elements are multiplied by each other—for visibility and attendance (A*B); for access to the asset (C*D); for site-specific hazards (E*F); and off-site hazards (G*H). The four resulting numbers are then added.

Vulnerability factor (y) = (A*B) + (C*D) + (E*F) + (G*H)

According to **table 6**, for any asset that is being scored, the lowest attainable criticality factor score is 3 and the highest attainable score is 100.

The vulnerability factor (y) will be used to calculate the vulnerability coordinate (Y) in the next step as follows:

Vulnerability coordinate (Y) = 100

Asset	Vulnerability Factors *Multiply Each of the Two Factors (AxB, CxD, ExF, GxH). Then Add the Four Resulting Numbers (AB + CD + EF + GH = Y)*															
	A 1-5	x	B 1-5	+	C 1-5	x	D 1-5	+	E 1-5	X	F 1-5	+	G 1-5	X	H 1-5	Total (100 Pts Max)
Asset 1 Miami Dade Public Safety Center	2	X	2	+	5	X	5	+	3	x	3	+	3	x	3	47
Asset 2 Miami Dade FD Station 1	2	x	1	+	5	x	5	+	2	x	3	+	2	x	2	37
Asset 3 Miami Dade FD Station 2	2	x	1	+	5	x	5	+	2	x	3	+	2	x	2	37
Asset 4 Miami Dade FD Station 3	2	x	1	+	5	x	5	+	2	x	3	+	1	x	1	34
Asset 5 Miami Dade FD Maintenance Facility	1	x	1	+	5	x	4	+	2	x	3	+	1	x	1	28
Asset 6 Fire Training Academy	1	x	2	+	5	x	4	+	2	x	3	+	1	x	1	29

Table 7. Sample Vulnerability Factor Scoring

The order (highest to lowest) in terms of overall vulnerability (using the scores in **table 8**), will be:

- *Asset #1 (Public Safety Center)*—scored 41 as the highest vulnerability
- *Assets #2 and 3 (Stations 1 and 2)*—scored 37 and are the second highest in terms of vulnerabilities
- *Asset #4 (Station 3)*—scored 34 on the vulnerability scale
- *Asset #6 (Fire Training Academy)*—scored 29 in terms of vulnerability
- *Asset #5 (Maintenance Facility)*—is the least vulnerable facility according to this score sheet

Asset	Criticality		Vulnerability		Quadrant
	(x) (43 Max)	(X)	(y) (100 Max)	(Y)	
Asset 1 Miami-Dade Central Public Safety Center	38	88	47	47	I
Asset 2 Miami Dade FD Station 1	31	72	37	37	I
Asset 3 Miami Dade FD Station 2	24	56	37	37	I
Asset 4 Miami Dade FD Station 3	20	47	34	34	I
Asset 5 Miami Dade Fire Department Maintenance Building	19	44	28	28	II
Asset 6 Miami Dade Fire Training Academy	15	35	29	29	II

Table 8. Example Criticality and Vulnerability Coordinates and Related Quadrants for Sample Miami Dade Public Safety Facility—Fire Department

Step 3—Consequence Assessment

Objective. The consequence assessment helps to identify assets that, if attacked, would produce the greatest risks for undesirable outcomes given a specific set of circumstances and conditions. This assessment is based on an integrated analysis of the data collected on all assets owned or leased by state and local governments in Florida, realistic and credible threats, and known or identified vulnerabilities.

Approach

3a. Plot Asset Criticality Versus Vulnerability. In this step, criticality (X) and vulnerability (Y) coordinates are calculated for each asset. The X and Y coordinates define a point for each asset in one of the four quadrants in the Criticality and Vulnerability Matrix of **figure 3**. The criticality coordinate (X) is calculated using the procedure described in Step 1 (**table 2**). The vulnerability coordinate (Y) is calculated using the procedure described in Step 2 (**table 7**). X and Y coordinates plot the criticality and vulnerability for each critical asset:

X = Criticality = (x/Cmax) *100

Y= Vulnerability= (y) * 100

Where X and Y are the raw values of criticality and vulnerability for each asset and C_{max} is the maximum possible criticality value (C_{max} = 43 for the default values given in Step 1). **Figure 3** depicts the values given for vulnerability and criticality to determine your facility's ranges.

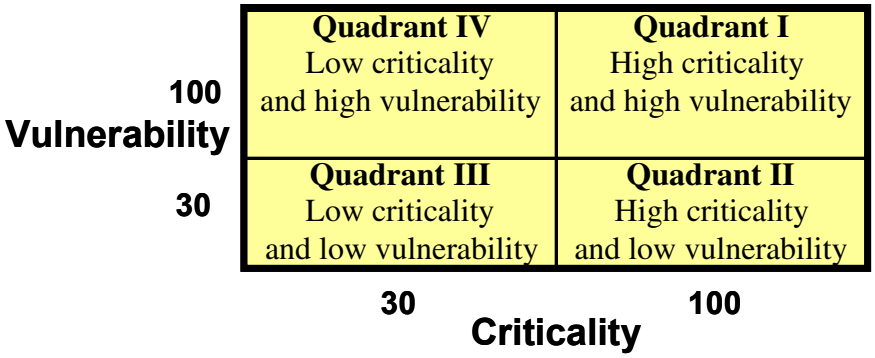


Figure 3. Criticality and Vulnerability Matrix

Figure 3 helps prioritize scored assets by the greatest level of consequences based on the critical asset factors and vulnerabilities evaluated previously (the Miami Dade Fire Department Assets 1 through 6). Quadrant 1 identifies the assets with the highest criticality and vulnerability for implementing protective measures. Low criticality scores range from 1-30. High criticality scores range from 31-100. Low vulnerability scores range from 1-30. High vulnerability scores range from 31-100.

Illustrative Example. Using Asset 1, the Miami Dade Public Safety Facility, as an example, the X and Y coordinates for this asset were calculated as follows:

X= (38/43) * 100 = 88

Y= (47) * 100 = 47

These coordinates (88, 47) place the Public Safety Facility in Quadrant I, or high criticality and high vulnerability.

Note that for this example, the Quadrant I assets include assets 1 through 4. The assets that fall into Quadrant I reflect the perceived vulnerabilities and characteristics of the asset to the agency, as captured by the vulnerability assessment, and the importance of the asset to

the agency (in terms of the critical asset factors). Also, note that some assets are critical to the government agency that owns or leases the facility (asset) but are judged to be less vulnerable, possibly because redundant facilities, minimal consequences, or their physical characteristics make them less susceptible to terrorist attacks.

3b. Consider Consequences for Quadrant I Critical Assets. The basic tenet of the AASHTO Guide is that the highest security measures should apply to those facilities or assets that fall within Quadrant I—the most critical and the most vulnerable. The state of Florida and its local government agencies can use these rankings to prioritize their efforts within each asset or facility class.

Assets that fall into Quadrant I are critical to the state or region and judged to be vulnerable to the identified threats. The consequences of attacks on those assets depend on the nature of the attack and the impact of the loss of the asset to the state or government agency. Consequences can range from loss of life and property to loss of part of the government's infrastructure critical to supporting economic activity, military deployment (or deployment of emergency response agencies), or the ability to respond effectively to other emergencies (e.g., loss of a critical fire station and its equipment).

A careful look at the criticality (X) and vulnerability (Y) coordinates of each asset in Quadrant I will reveal important information for the consequence assessment of the asset. In the case of the central Miami Dade Public Safety Center, the asset's X score of 88 out of 100 (numerical score of 38 divided by 43 = 88) was based on the scores it received in three areas described in **table 1**: Category C: Casualty Risk, Category G: Emergency Response Function, and Category H: Government Continuity. Based on the factor scores, which are fairly high in just those three areas, in which a maximum score of 5 points is allowed, the Public Safety Center resulting score was in the range of 88/100.

The Y score (vulnerability) of 47 of 100 places it in Quadrant I. The facility had a medium level of recognition, but allowed access to the asset and had off-site hazards that affected the outcome.

If you take into account that perhaps the Public Safety Center also houses the main police station, a high security jail, and federal prisoner detention center, it might score higher on the criticality scale and could score a little higher on the vulnerability scale, especially if it has an underground garage and poor controls over parking in and around the facility.

This Guide urges the assessment team to concentrate on the assets in the upper right corner (Quadrant I–High Criticality and High Vulnerability) for applying countermeasures.

The team can now apply a set of countermeasures, using the encyclopedia (Part IV) and the protective measures facility matrices (database), tailored for facilities based on their quadrant score. Again, facilities within Quadrant I would likely have the highest priority for security measures and would likely require that the highest level of security be applied (minus what is already in place).

Place All Facilities into One of Three Risk Categories. Once the criticality and vulnerability scores have been established, determine how those scores relate to the three risk categories of high, medium and low. The following scores were established for these categories so agencies can make decisions concerning implementing security measures:

- **High:** The facility has a criticality score of between 67 and 100 and a vulnerability score of between 67 and 100
- **Medium:** The facility has a criticality score of between 34 and 67 and a vulnerability score of between 34 and 67

- **Low:** The facility has a criticality score of between 0 and 33 and a vulnerability score of between 0 and 33.

Note: Although the original AASHTO guidance (developed for the DOT) uses four quadrants to rate facilities on criticality and vulnerability, we are using the scale of high, medium, and low to simplify the process for users.

Using the high, medium, and low categories, managers should apply the highest security measures to those facilities in the highest range for assets that score between 67 and 100. The next category, medium, will have fewer security measures to apply, and, the third category, low, will have the fewest security measures.

Assets that fall into the high category have been judged to be critical to both the agency and the state or region and vulnerable to the identified threats. The consequences of attacks on those assets depend on the nature of the attack and the impact of the loss of the asset to the organization, state, and nation.

Step 4—Protective Measures

Objective. This section provides a general guideline for protecting assets from the threats and vulnerabilities assessed previously.

Approach

4a. Identify Potential Protective Measures. Developing countermeasures to protect all assets depends on an effective partnership with all of the stakeholders of a facility or site. It is particularly important for security professionals to work closely with engineers and general managers so that everyone understands the basic approach the team will take in identifying protective systems and methods. Engineers and designers must understand the issues involved with ensuring that anything they design or propose is compatible with security operations and does not unduly restrict the essential daily operation of the facility or site. The best way to ensure a viable security solution is through teamwork.

Countermeasures are developed as a result of general and specific design strategies. They commonly take the form of site work, building/structure, detection, and procedural elements:

- Site work elements include the areas surrounding a facility or asset. They can include perimeter barriers, landforms, and standoff distances.
- Building and structure elements are protective measures directly associated with facilities and structures. They include walls, doors, windows, and roofs.
- Detection elements detect such things as intruders, weapons, or explosives. They include closed-circuit television (CCTV), and motion detectors, alarms and weapon and explosive detectors, as well as chemical and biological weapon detection technologies. They also can include a security force or improved security awareness and practices by the building or site occupants.
- Procedural elements are protective measures required by regulations, policies, or plans. They provide the foundation for developing the other three elements.

Table 9 identifies countermeasures considered applicable to protecting Florida's government-owned or leased sites and facilities (assets) and the functionality these countermeasures provide in terms of deterrence, detection, and defense. The terms defined below are consistent with the highly regarded *U.S. Army Field Manual 3-19-30-Physical Security*. Certain countermeasures such as surveillance systems must be incorporated into the operation of your facility or site security system.

- *Deterrence*—A potential aggressor who perceives a risk of being caught may be deterred from attacking an asset (site or facility). The effectiveness of deterrence varies with the aggressor's sophistication, the asset's attractiveness, and the aggressor's objective (aim for high publicity with mass casualties, damage to prevent use of the facility for long-term or economic consequences).
- *Detection*—Detection senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a response force (often through an assessment step) which in turn notifies a security force or police department. A valid detection system must provide all three of these capabilities to be effective.
- *Response*—Response measures protect an asset from aggression by delaying or preventing an aggressor's movement toward the asset or by shielding the asset from weapons and explosives. Defensive measures delay aggressors from gaining access by using tools in a forced entry, prevent an aggressor's movement toward an asset, and protect the asset from the effects of tools, weapons, and explosives.

Potential Countermeasures	Deter	Detect	Respond
Increase inspection efforts aimed at identifying potential explosive devices as well as increased or suspicious potential criminal activity	✓		
Institute full-time surveillance at the most critical assets where alternative facilities are limited or have not been identified	✓	✓	
Eliminate parking under any of the most critical facilities, or have 100% access control into the underground facility	✓		
Institute a standoff barrier plan using planters, wrought iron fencing, or earth berms for high-risk facilities	✓	✓	
Protect ventilation intakes with screening or mesh to prevent introduction of chemical and biological agents	✓		
Install and protect emergency ventilation shut-off systems and install sensors	✓	✓	
Install Mylar or similar protective film over windows within potential blast protection zone	✓		
Implement 100% entry and access control to the facility with trained security force or receptionist	✓	✓	✓
Implement 100% access control to surface parking lots with trained security force present at entry points	✓	✓	✓
Develop and implement an agencywide security awareness and motivation program for all employees	✓	✓	
To improve entry and access control, issue identification badges for use with automated access control system	✓	✓	
Install CCTV for critical entry points and spots not easily observed	✓	✓	
Install secondary verification system to the access control system (biometrics)	✓	✓	
Assign security patrols or contract with local police for on-site security response force	✓	✓	✓
Install perimeter lighting to enhance visibility for routine patrol coverage and response to calls for service around site or facility	✓	✓	
Install motion detection on perimeter fence; tie to CCTV and total access control systems	✓	✓	

Table 9. Potential Countermeasures

4b. Map Countermeasures to Assets (Sites and Facilities) Based on Their Criticality and Vulnerability Score. Based on the decision of the agency or department responsible for the site or facility, the team should use the information from Step 3a and the countermeasures presented in **table 9** (along with any additional measures the team wishes to add) and map the Quadrant I or most critical facilities and tailor the remaining facilities or sites based on their criticality and vulnerability scores. The process of selecting from a menu of choices is designed to tailor the security measures to the risk. The list shown in **figure 4** provides an example:

Consider using the following for critical bridges:

- Eliminate parking areas beneath the bridge
- Restrict entry and exit routes from adjacent areas
- Provide additional lighting
- Limit/monitor access to plans of existing bridges
- Install motion sensors or other active sensors
- Install surveillance cameras
- Apprise local law enforcement officials of critical bridges
- Provide column protection
- Provide pass-through in concrete median barriers
- Install advance warning system

Figure 4. Example: Potential Countermeasures for Bridges

4c. Assess Protective Measure Effectiveness. The effectiveness of countermeasures is measured subjectively by assessing how well the application reduces either the potential for or consequences of attacks on assets given specific threats and vulnerabilities. Using the previous quadrant scores, rescore Steps 1 and 2 to determine whether the proposed protective measures shift (change) the consequences (Step 3) into a lower quadrant (in **figure 4**). If so, Step 5 should be followed to estimate the capital, operating, and maintenance costs for the countermeasure as part of a cost-benefit analysis. If the consequences remain the same, consider selecting another countermeasure or set of countermeasures to reduce the threats and vulnerabilities to high-priority critical assets.

Example. **Table 10** illustrates the results from Step 4.

	Critical Asset Category				Countermeasures Function		
Countermeasure	**Infrastructure (Resources)**	**Facilities (Property)**	**Equipment (Information)**	**Personnel (People)**	**Deter**	**Detect**	**Respond**
Increase inspection efforts aimed at identifying potential explosive devices as well as increased or suspicious potential criminal activity	✓	✓	✓	✓	✓		
Institute full-time surveillance at the most critical assets where alternative facilities are limited or have not been identified	✓	✓			✓	✓	
Eliminate parking under any of the most critical facilities or have 100% access control into the underground facility.	✓	✓			✓		
Institute a standoff barrier plan using planters, wrought iron fencing, or earth berms for high-risk facilities	✓	✓			✓	✓	
Protect ventilation intakes with screening or mesh to prevent introduction of chemical and biological agents		✓		✓	✓		
Install and protect emergency ventilation shutoff systems and install sensors		✓		✓	✓	✓	
Install Mylar or similar protective film over windows within potential blast protection zone		✓		✓	✓		
Implement 100% entry and access control to the facility with trained security force or receptionist		✓		✓	✓	✓	✓
Implement 100% access control to surface parking lots with trained security force present at entry points		✓		✓	✓	✓	✓

Table 10. Illustrated Example, Applying Countermeasures to Critical (Quadrant I) Asset Categories

Countermeasure	Critical Asset Category				Countermeasures Function		
	Infrastructure (Resources)	Facilities (Property)	Equipment (Information)	Personnel (People)	Deter	Detect	Respond
Develop and implement an agencywide security awareness and motivation program for personnel	✓	✓	✓	✓	✓	✓	
To improve entry and access control, issue identification badges for use with automated access control system	✓	✓	✓	✓	✓	✓	
Install CCTV for critical entry points and spots not easily observed		✓		✓	✓	✓	
Install secondary verification system to the access control system (biometrics)		✓		✓	✓	✓	
Assign security patrols or contract with local police for on-site security response force	✓	✓	✓	✓	✓	✓	✓
Install perimeter lighting to enhance visibility for routine patrol coverage and response to calls for service around site or facility	✓	✓			✓	✓	
Install motion detection on perimeter fence; tie to CCTV and total access control systems	✓	✓			✓	✓	

Table 10. Illustrated Example, Applying Countermeasures to Critical (Quadrant I) Asset Categories (continued)

Step 5—Cost Estimation

Objective. In this step, general guidelines are provided to calculate the range of costs for implementing the selected countermeasures.

Approach

5a. Create Protective Measure "Packages." The protective measures (not an inclusive list) identified in Step 4 are intended to deter or detect a potential or real attack or to help defend Florida assets in the event an attack is underway. In some cases, the countermeasure will be an action taken to deny access to an asset through physical features or enforcement strategies; in other cases, countermeasures will render the attack harmless or mitigate damages. In many cases, combinations of countermeasures will be needed to achieve the desired vulnerability reduction. The first step in cost estimation is to "package" countermeasures in ways that make sense operationally and from a vulnerability reduction perspective. In some cases, a single measure will apply to multiple assets (sites and facilities) (e.g., video surveillance may cover multiple sites and facilities on a university campus or a government office complex). In others, multiple countermeasures will be applied to a single asset (e.g., the vulnerability of a main public safety complex or justice center may be reduced by applying electronic sensors, barriers, access control, and an on-site armed response force).

This countermeasure packaging step should help Florida and its local governments analyze procedural, equipment, technological, and design options for reducing vulnerability. Once viable packages are identified, their unit costs should be determined using standard life-cycle costing methods.

5b. Determine Acquisition, Operation, and Maintenance Costs of Proposed Countermeasures. The capital investment and annual operation and maintenance costs for countermeasures for state and local government agencies in Florida vary widely. It is beyond the scope of this

Guide to provide a detailed description of life-cycle cost estimating. **Table 11** provides a tool for assigning preliminary costs to each countermeasure listed in this Guide.

Sample Countermeasure Relative Cost Range			
Risk Level	**Capital Investment**	**Annual Operating Cost**	**Annual Maintenance Cost**
L	<$100,000	<$50,000	<$25,000
M	$100,000 to $500,000	$50,000 to $250,000	$25,000K to $100,000
H	>$500,000	>$250,000	>$100,000

Note: The figures above apply to a single site or facility.

Table 11. Countermeasure Relative Cost Range

Note: If you add countermeasures, you can assign a cost as well. These costs are described as high (H), medium (M), or low (L). The relative ranges associated with high, medium, and low costs are subjective and depend on many variables. Sample values are provided in **table 11** as a general guide to categorizing the countermeasure costs. These values are applied to the countermeasures shown in **table 12**.

	Countermeasure Function			Estimated Relative Cost High/Medium/Low		
Countermeasure	**Deter**	**Detect**	**Respond**	**Capital**	**Operating**	**Maintenance**
Increase inspection efforts aimed at identifying potential explosive devices as well as increased or suspicious potential criminal activity	✓	✓	✓	M	M	L
Institute full-time surveillance at the most critical assets where alternative facilities are limited or have not been identified	✓	✓		M	M	M
Eliminate parking under any of the most critical facilities, or have 100% access control into the underground facility	✓	✓		M	L	L
Institute a standoff barrier plan using planters, wrought iron fencing, or earth berms for high-risk facilities	✓	✓		M	L	L
Protect ventilation intakes with screening or mesh to prevent introduction of chemical and biological agents		✓		L	L	L
Install and protect emergency ventilation shutoff systems and install sensors		✓		H	L	L
Install Mylar or similar protective film over windows within potential blast protection zone		✓		H	L	L
Implement 100% entry and access control to the facility with trained security force or receptionist		✓		H	M	M
Implement 100% access control to surface parking lots with trained security force present at entry points		✓		M	H	L
Develop and implement an agencywide security awareness and motivation program for all personnel	✓	✓	✓	L	M	L
To improve entry and access control, issue identification badges for use with automated access control system	✓	✓	✓	M	M	L
Install CCTV for critical entry points and spots not easily observed		✓		H	M	M
Install secondary verification system to the access control system (biometrics)		✓		H	M	M
Assign security patrols or contract with local police for on-site security response force	✓	✓	✓	H	M	L
Install perimeter lighting to enhance visibility for routine patrol coverage and response to calls for service around site or facility	✓	✓		M	M	L
Install motion detection on perimeter fence; tie to CCTV and total access control systems	✓	✓		H	M	M

Table 12. Estimated Countermeasure Costs

Example: Countermeasure Cost Estimates

Consider these cost estimates on countermeasures related to fencing, cameras, and floodlights.

- Two CCTV cameras with floodlights and 200 feet of 10 ft. high fence: $23,500
- Fencing off access roads to bridges, installing gates, and placing two cameras: $25,000
- Ten cameras with floodlights, gates, and 600 feet of fence: $80,000
- Three cameras with floodlights, gates, and 600 feet of fence: $50,000

5c. Apply Costs to Assets. This step is the simple application of the unit cost of the countermeasure packages to the critical assets. Florida and its state and local government bodies have already grouped their facilities and sites by category and type and can extend the unit price for appropriate countermeasure packages (e.g., intrusion detection, perimeter sensors, surveillance measures) selected for reducing the vulnerability of a particular facility or site. This unit cost could then be applied to similar facilities with the same attributes or features within the same classifications (quadrants) of vulnerability and criticality. This overall cost estimate should provide data to the owning agency as to the costs for countermeasures. It provides a reasonable estimate so the agency can formulate a spending plan or budget request. A similar process applies to other asset types (other metropolitan area fire stations, for example) where other countermeasure packages may be applied.

As demonstrated with **tables 13** and **14**, we can see the likely countermeasures for the highest category (vulnerability and criticality), which in this example is Asset #1—the Miami Dade Metro Public Safety Building, which was scored as a fairly high critical facility with somewhat high vulnerabilities versus Asset #6, the Miami Dade Metro Fire Department training academy, which was rated with fairly low criticality and vulnerability scores. The countermeasure list for Asset #6, as expected, smaller than the list for Asset #1.

	Countermeasure Function			Estimated Relative Cost High/Medium/Low		
Countermeasure Description for Miami Dade Metro Public Safety Building Asset #1	Deter	Detect	Respond	Capital	Operating	Maintenance
Increase inspection efforts aimed at identifying potential explosive devices as well as increased or suspicious potential criminal activity	✓	✓	✓	M	M	L
Institute full-time surveillance at the most critical assets where alternative facilities are limited or have not been identified	✓	✓		M	M	M
Eliminate parking under any of the most critical facilities, or have 100% access control into the underground facility	✓	✓		M	L	L
Institute a standoff barrier plan using planters, wrought iron fencing, or earth berms for high-risk facilities	✓	✓		M	L	L
Protect ventilation intakes with screening or mesh to prevent introduction of chemical and biological agents		✓		L	L	L
Install and protect emergency ventilation shutoff systems and install sensors		✓		H	L	L
Install Mylar or similar protective film over windows within potential blast protection zone		✓		H	L	L
Implement 100% entry and access control to the facility with trained security force or receptionist		✓		H	M	M
Implement 100% access control to surface parking lots with trained security force present at entry points		✓		M	H	L

Table 13. Example of Countermeasure Costs

Countermeasure Description for Miami Dade Metro Public Safety Building Asset #1	Countermeasure Function			Estimated Relative Cost High/Medium/Low		
	Deter	Detect	Respond	Capital	Operating	Maintenance
Develop and implement an agencywide security awareness and motivation program for all personnel	✓	✓	✓	L	M	L
To improve entry and access control, issue identification badges for use with automated access control system	✓	✓	✓	M	M	L
Install CCTV for critical entry points and spots not easily observed		✓		H	M	M
Install secondary verification system to the access control system (biometrics)		✓		H	M	M
Assign security patrols or contract with local police for on-site security response force	✓	✓	✓	H	M	L
Install perimeter lighting to enhance visibility for routine patrol coverage and response to calls for service around site or facility	✓	✓		M	M	L
Install motion detection on perimeter fence; tie to CCTV and total access control systems	✓	✓		H	M	M

Table 13. Example of Countermeasure Costs (continued)

Countermeasure Description for Miami Dade Fire Department Academy Asset #6	Countermeasure Function			Estimated Relative Cost		
	Deter	Detect	Respond	Capital	Operating	Maintenance
Eliminate parking within 300 feet of the facility	✓	✓	✓	L	L	L
Institute a standoff barrier plan using planters or wrought iron fencing	✓	✓		M	L	L
Protect ventilation intakes with screening or mesh to prevent introduction of chemical and biological agents		✓		L	L	L
Implement 100% entry and access control to the facility with trained security force or receptionist		✓		H	M	M
Develop and implement an agencywide security awareness and motivation program for all personnel	✓	✓	✓	L	M	L
To improve entry and access control, issue identification badges for use with automated access control system	✓	✓	✓	M	M	L
Install perimeter lighting to enhance visibility for routine patrol coverage and response to calls for service around site or facility	✓	✓		M	M	L

Table 14. Example of Countermeasure Costs

Step 6—Security Operational Planning

Objective. This step will improve the security of critical assets by guarding against potential consequences from acts of WMD terrorism through security operational planning.

Approach. Security operational planning is necessary to ensure implementation of necessary protection measures, both physical and procedural, that are designed to:

- Safeguard personnel
- Prevent unauthorized access to infrastructure, facilities, equipment, and personnel
- Safeguard against espionage, sabotage, damage, and theft

Throughout the Manual, there are extensive security operational planning recommendations. These recommendations are designed to complement the AASHTO Guide and ensure that Florida and its state and local governments take all necessary steps to reduce the state's vulnerability to acts of terrorism through programs for physical protection and necessary procedural changes to the state's homeland security program.

Because Florida has already established emergency response plans, for the scope and purpose of this project we recommend that after performing the vulnerability assessments, appropriate state and local officials ensure their emergency response plans by including the findings and reflect the current terrorist threat and anticipated consequences of terrorist attacks.

6a. Initiate Training and Exercise Activities. Good policies, plans, and program development are the beginnings of preparedness. Implementing awareness, training, and qualification programs as part of security operational planning helps to determine organizational (Florida's state and local government agencies) effectiveness in dealing with crises. Experience and data show that training and exercise activities are practical and efficient ways to prepare for crises. They test critical resistance, identify procedural difficulties, and provide a plan for corrective actions to improve crisis and consequence management response capabilities, without the penalties that might be incurred in a real crisis. Training and exercise activities also provide a unique learning opportunity for synchronizing and integrating cross-functional and intergovernmental emergency responses.

Without a common level of awareness, training, and standards, Florida and all of its first responders from many different agencies, organizations, and jurisdictions may have difficulty functioning together when confronted by a serious terrorist incident. Florida is experienced in coping with natural disasters and can build on its existing emergency system to plan for terrorist event responses.

Elements of a training and exercise program for WMD terrorism include:

- *Awareness*—Understanding the functions of security operational planning in terms of the full range of threats and vulnerabilities faced by an organization
- *Training*—Implementing and adjusting the security operational plan and developing skills critical to WMD preparedness and response, as well as rehearsing emergency response and all agency personnel in their assigned roles—testing whether their response expectations are appropriate. Training also can identify lessons learned, improved standards for performance, and additional resources. Both table top and practical exercises are extremely valuable. Leveraging experience from an actual event, evaluating the response, and creating a lessons learned database for future response training is another valuable training method.
- *Standards*—Identifying which members of an organization (agency) have met the required or desired level of training and planning for recurring training on perishable skills.

Conclusion

While it is lengthy and detailed, especially when compared to the DOJ and DoD assessment models, the SAIC-designed AASHTO model provides an empirical, objective means of scoring the vulnerability and criticality of given assets. This model also provides a detailed methodology to carry forward into implementation. A step-by-step checklist is provided as an exhibit for walking through the entire process.

The AASHTO model and the contents of this chapter go well beyond the DOJ, DoD and FDLE models and provide a complete end-to-end vulnerability assessment

methodology, as well as solutions and recommended strategies and some cost analyses. AASHTO is a recognized process that has been used by departments of transportation in Texas, Missouri, Maryland, and other states. The primary feature of AASHTO when compared to DOJ, DoD, and FDLE is that it considers more parameters and risks, but its application will be more complex and take longer to administer.

Exhibit 1: AASHTO Model

AASHTO Checklist for Conducting Your Vulnerability Assessment		
Step	**Responsible Office**	**Action Required**
1. Assess the threat	U.S. Department of Homeland Security, FDLE Regional Domestic Security Task Force (RDSTF), Corporate Security Director	Use "elevated" for baseline threat—"significant risk of terrorist attacks"
2. Determine if your facility or critical infrastructure meets state and national definitions	Critical Infrastructure Assurance Office (CIAO) U.S. DHS, FDLE RDSTF, Corporate security director	See the list of facility categories in the Introduction section
3. Form your assessment team	Corporate leadership Corporate security Facilities managers Budget and fiscal communications Safety Human resources Purchasing Maintenance Local law enforcement (on an availability basis) FDLE RDSTF (on an availability basis)	Meet with your group to review the Vulnerability Assessment Guide
4. Develop a list of assets	Corporate leadership Corporate security Facilities managers Budget and fiscal communications Safety Human resources Purchasing Maintenance	Using this volume and the FDLE and/or Domestic Intelligence Office list, develop a list of all components and facilities that comprise your agency's critical assets. List by location, size, mission, costs, economic value and impact of a loss, and criticality to the government and public
5. Review the AASHTO Guide	Corporate leadership Corporate security Facilities managers Budget and fiscal communications Safety Human resources Purchasing Maintenance	For express method: review the methodology in this section
6. Conduct a pre-assessment trial run	Select members of the vulnerability assessment team	Use one set of your facilities to conduct a trial run of calculating criticality
7. Review results of the pre-assessment trial run	Select members of the vulnerability assessment team	Review results, and obtain agreement or revise as necessary to reflect your agency's needs. Keep overall score process the same
8. Conduct a criticality assessment of all of your assets	Select members of the vulnerability assessment team	Calculate the criticality score for each asset Use tables in this section to determine the numerical value for each facility
9. Assign values for your assets	Select members of the vulnerability assessment team	The values are derived from using the formulae in tables in this section. Keep these values for the next step in the vulnerability assessment process

AASHTO Checklist for Conducting Your Vulnerability Assessment		
Step	**Responsible Office**	**Action Required**
10. Prioritize the all-inclusive list of critical assets	Select members of the vulnerability assessment team	Keep these values for the next step in the vulnerability process
11. Assign vulnerability factors to the critical assets	Select members of the vulnerability assessment team	Tables in this section explain how the vulnerability definitions are determined
12. Score the vulnerability factors for each asset	Select members of the vulnerability assessment team	Use the same assets you scored for the criticality step Review tables to determine how the vulnerability factors are calculated
13. Prioritize the all-inclusive list of critical assets	Select members of the vulnerability assessment team	These scores will be used along with the criticality score to list all of your critical assets into three categories
14. Determine consequences of a terrorist attack	Select members of the vulnerability assessment team	Determine criticality consequences first For each asset's score, divide by 43; you will then get a figure between 1 and 100 List these assets in the order of these scores Determine vulnerability consequences second For each asset's score, divide by 75; you will then get a figure between 1 and 100 List these assets in the order of these scores
15. Rank order your critical assets	Select members of the vulnerability assessment team	Use this scale: 67-100 High 34-66 Medium 0-33 Low Do not combine scores; it is likely your criticality and vulnerability will fall within the same range If the criticality score is in the high range and the vulnerability score is in the low range, we recommend that you designate this asset as "medium"
16. Determine countermeasures	Select members of the vulnerability assessment team	Use the list of countermeasures in each risk category: high, medium, low. For the three threat levels Elevated, High, and Severe
17. Develop countermeasures implementation plan	Select members of the vulnerability assessment team	Develop prioritization plan Determine capital budget requirements Establish installation and operations plan

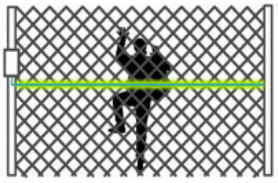
PART IV: ENCYCLOPEDIA

Chapter 1: External Building Security

Introduction

This section provides suggested methods for improving the physical security of the building, site, or facility. These measures can be implemented by the public sector, private sector, and for special venues. Use the information in this chapter to gain in-depth knowledge of security best practices, policies, and procedural recommendations. Proven methods are provided to enhance security at buildings or sites to protect people, facilities, and equipment. This chapter addresses security measures best suited for the boundary of a site or facility.

Barrier Systems



The function of a barrier system is to restrict, deny, delay, or channel the flow of pedestrian or vehicular traffic to a site. Barriers are not impenetrable but increase the probability of detecting persons or vehicles attempting to gain unauthorized access onto a site or dissuading them from attempting access. They offer a time delay to allow your security force or employees to detect and possibly assess illegal intrusion or trespassing.

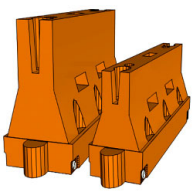
Facility managers must determine whether a permanent or temporary barrier system is needed during increased threat levels. Managers need a mechanism for detecting an intruder. Cameras, alarm sensors, or guards can be used, and some type of reaction force must be available to respond to the intruder. Depending on the criticality score of your facility and the availability of local police, you may need a well-trained security force to detain intruders until the police can arrive.

A barrier system consisting of man-made obstacles (such as fencing and gates) integrated with natural obstacles (such as wooded areas, creeks, ditches, marshy areas, rough ground, and rocks) can make most of a site perimeter inaccessible to vehicles. Other areas may require reinforcement, which should be tied into the natural terrain to discourage or make vehicle travel difficult.

Whichever barrier system is used, it must be integrated with other security measures, such as lighting, perimeter sensors, and surveillance plans.

Man-Made Barriers

Barriers such as decorative retaining walls, boulders, trees, thick evergreen bushes, short walls, berms or ditches, and concrete planters can be both aesthetically pleasing and effective. For example, pyracantha, a shrub with sharply pointed limbs, is very effective at discouraging foot traffic through unauthorized areas.



Other effective but perhaps less attractive techniques can be used on either a temporary or permanent basis. These could include Jersey (sometimes called "K" rail) barriers, concrete walls, bollards (concrete-filled steel pipes set vertically in concrete), cable barriers or cable reinforcement of fencing, large rocks, tree trunks, etc. Wrought-iron stanchions filled with concrete or bollards with decorative trees planted in them are other options.

Fences

Numerous types of fence are available. Chain-link fences are generally used for site perimeters and are normally 7 feet high. During increased threat levels or for critical operations, perimeter fencing can be reinforced with cables or 18-inch outriggers (arms) angling outward with barbed wire attached to deter climbing.

Fence fabric should be at least 9-gauge wire with 2-inch square mesh. Mounting hardware and fabric ties (of the same strength of the fabric) should be attached on the inside to prevent easy removal.

Razor wire can be installed above the barbed wire outriggers if additional security is desired. Steel posts can be set in concrete and bottom rails or tension wires can be installed at the base of the fabric. A trench at the base of the fence can be filled with concrete to prevent tunneling.

Standard chain-link fencing can easily be climbed. A trained individual can even climb fencing reinforced with barbed wire. If a perimeter requires a more formidable barrier than that afforded by typical chain link fabric, a tighter weave and heavier wire products can be used. These fences (often referred to as "super fences") come in large panels and are often 10 to 12 feet high. The tight mesh (1/4- to 1/2-inch separation) is resistant to bolt cutters and climbing. The smaller openings prevent a person from getting a finger hold in the mesh.

If no perimeter fencing exists, portable fencing can be erected during periods of increased threat levels. It can also be used as a supplemental barrier or to delineate limited-access areas. Normally, such fencing is chain-link fabric erected on a steel pipe frame. The frame should be well anchored to the ground. To be most effective, fencing must be observed by security staff.

Obstructive fencing is a solid fence that can be used to interdict the line of sight of a sniper and a standoff weapon projectile. Locate these fences inside the perimeter fencing so that a hole through which a projectile could be launched cannot be cut. Such fences can be solid wood, masonry, concrete, or other solid material that will cause the detonation of a rocket-propelled grenade. Fences should be high enough to obstruct the view of the facility from 500 meters.

A more expensive but attractive alternative to chain-link fencing is wrought-iron fencing topped with spikes or arrowheads. These fences have become popular around public housing units to prevent or slow down vehicle and pedestrian traffic.

Gates

One simple, inexpensive means to increased security is a gate. Either retractable or removable gates can be used to limit vehicle and pedestrian entry onto a site. Gate barriers must be fully integrated into the perimeter barrier system; otherwise terrorists may simply circumvent the gate and drive through the perimeter fence. This measure is appropriate for vehicle-borne bombs.

Gate barriers should be located in front of security forces (if posted) to afford reaction time and personal protection. A variety of retractable barriers exist, including sliding gates (often reinforced by steel beams), sliding beam, pop-up bollards, drum-type barrier, tire spikes, and removable bridges over anti-vehicle ditches.

Retractable barrier systems may be portable and can be placed during periods of increased threat levels and later removed. The selection and application of gate barriers depends on the size and speed of the anticipated terrorist vehicle. Speed bumps or a serpentine entrance can reduce vehicle speed.

For large high-security facilities such as airports, power plants, and refineries, consider removing unused gates and replace the opening with permanent fence fabric. It is also possible to render the approach road useless by breaking up the asphalt or installing barricades. Be sure to properly mark such a closed road and put reflective tape on the barricades. An unused gate is attractive to an intruder with a vehicle.

Clear Zones

Clear zones provide a strip of land normally at least 30 feet around the building or your security zone (fence) that allows no obstruction more than 4 inches high. Trash receptacles, dumpsters, ashtrays, bushes, and any other object that could obscure a small bomb or provide cover for an intruder must be eliminated.

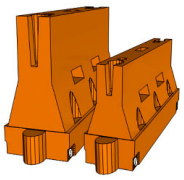
Clear zones offer an unobstructed view, making it easier to detect intruders and unauthorized vehicles that may contain explosives. Consider the use of clear zones during increased threat levels and at critical infrastructure or operation locations.

During low threat conditions or at low-risk facilities, creation of clear zones along sidewalks or pathways may be sufficient. During increased threat levels the removal of shrubs and trees adjacent to the site may be necessary.

When using perimeter cameras, a 30-foot clear zone is critical to give the cameras a clear field of view.

Explosive Standoff Zones

To protect facilities from explosive threats, it is usually necessary to increase the distance between vehicles and the facility. Explosive standoff zones are commonly used during heightened security conditions when vehicle bombs could be a threat.



It is rare that an adequate standoff zone will not adversely impact the flow of traffic or parking. At low threat levels, it may be adequate to simply delineate a standoff zone as large as possible without adversely impacting driveways, roads, or parking. For heightened threat levels, the appropriate standoff distance should be based on the anticipated size of the explosive. The distance is also affected by building construction and the existence of blast walls.

For low threat levels, folding barricades and caution tape may be adequate to delineate standoff zones. During increased threat levels, substantial barricades should be used to deny vehicles access into the standoff area. It may be advisable to close roads surrounding certain facilities in order to maintain adequate distances. This can be accomplished using Jersey barriers, concrete planters, or other forms of barricades.

As threat levels increase, it may be necessary to restrict parking. In an urban environment, it may be necessary to eliminate parking along a street adjacent to a high-risk facility. (For additional information, refer to the section on Parking.)

The military standard for minimum standoff distance is:

- 82 feet for a low threat level and low-risk building of standard (frame) construction
- More than 300 feet at a medium (moderate) threat level
- More than 400 feet for a high threat level

The use of blast walls, masonry construction, and other factors can mitigate the distance required. Such an analysis should be performed by a qualified engineer.

Inspections (Vehicles)

During increased threat levels at critical infrastructure sites, facility managers should inspect vehicles before the vehicles are allowed to enter the site. Vehicle inspections should be conducted in conjunction with a retractable vehicle barrier (refer to Barrier section) to limit an attempt by a vehicle forcing entry. More thorough inspections should be implemented for higher threat conditions and at higher risk facilities. Under-vehicle inspection systems such as inspection mirrors or light and cameras offer additional means of enhanced security. (Also refer to the Security Policies section.)

The number of inspections should be adjusted based on the threat level. Inspections can be random or they can be mandatory for all vehicles. Depending on threat levels, inspection of vehicle trunks or interiors may be sufficient. Undercarriage inspections may be included to detect weapons or explosives.

Large vehicles require more time to inspect, so consider directing them to an alternative entrance.

Lights

Perimeter lighting is a functional part of a facility's overall security plan and provides an additional level of protection for personnel and property. Lighting can be a significant deterrent to potential intruders and can allow for advance detection of unauthorized individuals. Facility managers should review their lighting criteria to ensure that they meet current operational objectives and illumination standards, and are compliant with local established guidelines.

Permanent lighting should be installed at all facility entrance points and should adequately illuminate the site perimeter, pathways, and parking areas. Lighting can be pole-mounted, building-mounted, or area lights, floodlights, and spotlights.

Lighting can be activated by sensors or timers or by manual operation. General site illumination should be used during increased threat levels.

Lighting activated by motion or other sensors can be an effective method of intrusion detection and deterrence. It can be especially effective in alerting surveillance personnel of an intrusion.

Portable area lighting, usually powered by generators, should be used to illuminate areas in which permanent lighting is insufficient. Where no perimeter lighting exists, portable lighting can be added during periods of increased threat levels.

If exterior closed-circuit television (CCTV) cameras are being used, facility managers should ensure that perimeter lighting levels are adequate to provide clear and undistorted monitoring. Some cameras claim to be effective at .1 foot candle. Normal illumination for a parking lot is .5 foot candle.

Facility managers should also ensure that they have a lighting maintenance plan and procedures to provide emergency power for lighting systems in the event of a power failure.

Parking

A facility parking plan can significantly decrease the threat of a moving or stationary vehicle bomb. Parking restrictions must be based on the threat level, type of facility, and other security concerns.

Parking policies must be based on the standoff distance between vehicles, the building, and other critical areas, such as a power substation or gas pipelines. Security measures such as lighting and surveillance should be integrated with parking plans.

The facility manager must assess the vulnerability to an attack and the protection afforded by the facility's construction. During increased threat levels, vehicles should not be permitted to park adjacent to a protected area or building unless stringent vehicle inspections have been conducted and/or a blast wall is in place.

You must consider parking for disabled employees and visitors. If it is necessary to restrict parking, you may consider these options:

- Provide parking nearby and offer a shuttle service
- Develop a gated parking area with card access for authorized disabled placard holders
- For disabled visitors, post appropriate signs directing them to parking and shuttle service
- If you cannot afford a fenced and access-controlled parking area for the disabled, issue a company-unique decal or placard that authorizes close-in parking.

Restricting Parking

During increased threat levels, portions of parking lots and some driveways may need to be barricaded. Parking controls may include restricting employee-owned vehicles or commercial vehicles to a designated standoff distance from the building.

Management may consider requiring vehicle registration to park in certain areas, a parking pass, or similar security measures.

It is recommended that parking not be allowed within the standoff zones. Management may consider restricting parking to vehicles such as emergency vehicles, company vehicles, or selected employees. In these cases, barriers and security officers will be necessary to verify vehicle occupants and enforce compliance.

Ensure that the needs of disabled employees and visitors are addressed in your restricted parking plan.

Alternative Parking Areas

During increased threat levels, alternative provisions for parking should be considered. Parking on leased, remote lots is an option. Shuttles can transport employees to the building.

Parking Access

Access to parking areas can be controlled by a staffed security post (on site or by remote CCTV surveillance) or, in critical operating areas, by technical means such as card access or personal identification number (PIN).

Card access and/or PIN systems often use a low-security arm system as a barrier. Such a system will not deter dedicated adversaries and should be augmented with additional barrier controls during periods of increased threat levels. Management may consider replacing this type of system with more stringent security measures for critical or high-risk facilities. Such measures include reinforced retractable gates (with or without a ground track), solid or mesh garage doors, and retractable tire defeat systems or in-ground security barriers.

Access Considerations

During periods of increased threat levels, a balance must be struck between convenience to visitors and the security of the facility. Visitors (non-employees, maintenance staff, etc.) should be required to park in a designated area and may be issued visitor parking passes as an additional security measure. Depending on the criticality of the location, visitors may be prohibited from parking on the immediate property.

Signs designating parking places for critical personnel should be removed during heightened threat conditions.

A log of visitor parking passes (including name, organization, license plate number, and person being visited) should be maintained for at least 90 days. This process should include adequate procedures to ensure that passes are not removed from the vehicle and used by unauthorized individuals to gain entrance to the facility. Positive identification of individuals should be made at the facility entrance prior to allowing vehicle access. Passes should be collected at the end of the visit.

Company Vehicle Parking

Company vehicles or school buses may require additional protective measures, especially those marked with a logo, name, or special license plate. These vehicles may be segregated and parked in a fenced and locked parking area or in a controlled area of a parking lot or garage where they can be monitored by CCTV—possibly motion-activated—or observed by security officers.

Lighting Parking Areas

Adequate lighting should be provided for parking areas. Special attention should be given to the protection of emergency response vehicles because they may present a higher risk than other company vehicles.

Underground or Elevated Parking

Access into and within underground or elevated parking garages should be controlled or prohibited during increased threat levels. Public parking in a garage underneath an occupied building should be prohibited during increased threat levels.

If access to these areas is controlled electronically (gates or control arms), facility managers should take appropriate measures to ensure that "piggybacking" does not occur by allowing only one vehicle to enter at a time. During high threat-level periods, security officers should be posted to screen all vehicles and pedestrians entering the parking area. It may also be appropriate to close these parking areas.

Security & Access Control

Parking can also be restricted to those people with a critical need to enter and only after identification is verified. During increased threat levels, unknown or unauthorized vehicles should not be permitted to remain parked in these areas and should be removed. Signs should be posted to alert operators that vehicles are subject to removal if illegally parked or conditions warrant.

Suspicious Vehicles

Local law enforcement authorities, supplemented by trained explosives professionals, should be notified immediately when suspicious vehicles are identified. Vehicles should not be approached and the area should be cordoned off. A vehicle bomb is a typical terrorist tactic; however, smaller, portable explosive devices may also be attached to vehicles.

What is a suspicious vehicle?

- An unexpected rental truck that arrives and/or has been left unattended in the parking area or near the building. A 1.5-ton rental truck can carry at least 5,000 pounds of explosives, as demonstrated by the Murrah Federal Building bombing in Oklahoma City. Anyone with a credit card and a driver's license has access to a rental truck
- A delivery vehicle that arrives at the wrong location and is not expected
- An unmarked "box" or commercial van that is not expected
- A clearly unauthorized or unusual truck that arrives and parks, such as a fuel truck near a theme park or stadium
- A driver parks a car and then runs from it.

Signs

To deter potential threats and establish legal recourse, signs should always be visible.

During increased threat levels, signs that divulge sensitive information should be removed. For example, signs that identify the location of senior officials' offices, emergency evacuation assembly areas (employees should know where these are), and signs indicating parking for individuals such as the chairman, director, or manager.

While it is important to have clearly marked signs for visitors and the public, consider alternatives such as having all visitors report to a central point and being escorted to their location.

Use symbols for fire and safety of life if you have hazardous materials stored or you are required by the fire code to have placards for chemicals and explosives. Experts will recognize these symbols, but an adversary may not.

Tunnels

Tunnels and utility manholes can provide unauthorized access to a site. Covers on sanitary and storm sewers, and telephone and electrical manholes may be vulnerable and should be evaluated and secured if warranted. For conduits that run under buildings or may be deemed a threat to the site, manhole covers should be removed and replaced with lockable types. An alternative is to tack weld the cover to the frame. For secured manholes, managers must maintain surveillance to identify tampering or attempts at unauthorized access.

The military standard is that any opening larger than 96 square inches should be covered with welded bars or a grate/grille.

Utilities

Utilities such as electricity, natural gas, water, and telecommunications require heightened attention in the facility protection plan. Managers should prepare a utility protection plan to protect backup generators and their fuel supplies. Exterior utility access and backup generators should be enclosed in aesthetically appealing (when practical) walls or fencing, with access controlled by the facility manager in addition to the security force. The following safety considerations should be incorporated into utility protection strategies:

- Provide surveillance of vulnerable utility points for both interior and exterior utilities. Post security officers at key utility points when the threat dictates.
- Control access to vulnerable points such as control panels, meters, fuel tanks, etc.
- Restrict vehicular traffic into or adjacent to utilities.
- Use stringent visitor control procedures for maintenance personnel who arrive to service utility systems (e.g., someone who claims to be representing the electric or telephone company).
- Use positive identification, callback procedures, and pre-arrangement of service calls as a protective screening measure.
- Escort service technicians and/or installers whenever practical.
- Ensure adequate emergency backup power arrangements and test the backup system.

Uninterrupted Power Supply (UPS)

Maintaining electrical power can be critical at facilities such as hospitals, treatment plants, and industrial plants. Facilities such as office buildings may have a lower need to

maintain power, but may require at least a minimal power supply. Normally, fire and building codes require at least emergency lighting with a battery backup for emergency evacuation of publicly occupied buildings.

The Environmental Protection Agency (EPA) requires treatment plants to have an alternative source of power, from either a generator or a second electrical feed from a different power circuit. This may also be standard for industrial plants with processes that can cause significant damage if abruptly terminated by a power outage.

Hospitals are required to have emergency generators. During increased threat levels these facilities should plan and contract for additional generators in case multiple electrical feeds or the main transmission power lines become disabled.

The military, particularly the state's Army National Guard, may be a source of generators in an emergency. Arrangements should be made in advance for this contingency. Certain vital systems, such as 24-hour computer network operations, may contain data to which remote users require continuous access and that cannot withstand interruptions. High-risk facilities should also consider the use of UPS to provide immediate lighting.

Another option is to rent a generator, but have a priority reservation because a widespread power outage will quickly drain local sources of generators.

PART IV: ENCYCLOPEDIA

Chapter 2: Internal Building Controls

Introduction

This chapter explains security methods or tools for improving the physical security of your building. It addresses security measures for controlling building entry and techniques for use inside the building. These measures can be implemented by the public sector, private sector, and for special venues. Additionally, several physical security tools are explained.

Access Control

Proper access control starts at the facility entrance, where employees should be required to display their identification badge. All non-employees should be required to sign in and out of the building and be sponsored by a company employee. An additional level of visitor control is to require all visitors to be escorted by an employee during their visit.

Consideration should be given to designating access to controlled areas and reducing the number of building entrances. Minimizing or closing entrances reduces vulnerability as well as the number of security personnel necessary to verify employees and process visitors. Management should survey the amount of pedestrian traffic to avoid congestion. Closed building entrances should be locked inside and alarmed, but provide immediate exit in an emergency.

During increased threat levels it may be necessary to increase a facility's access control. Depending on the criticality of the location, contractors, temporary employees, and visitors may be required to produce an official document (driver's license, passport, etc.) with photograph before being issued a badge.

Managers assigned to critical operating facilities may require two forms of identification. This process often includes retaining the official document at the entrance point and returning it at the conclusion of the visit. This method ensures the visitor will be properly identified and processed into and out of the facility and the visitor badge returned.

Managers may also consider conducting identification checks at the entrance to the building and inspecting all persons and hand-carried items as they enter. Inspections can be conducted using screening devices (hand wand) or a "pat-down."

During increased threat levels, managers should post security officers at entry points. They may also consider closing the facility if the threat warrants.

Entrapment areas are used to control the movement of individuals into restricted or critical areas. Two doorways usually separate an entrapment area. Once an authorized individual enters, the first door closes behind him or her, "entrapping" him or her in the space between the two doorways. Once the first door has closed, the second door can then be opened, using an access card or other means of entry, to allow access to the critical area. This method of access control is commonly used in conjunction with an electronic card access system and eliminates the possibility of someone following closely behind an authorized person to gain entry.

In another method, a vehicle may be driven through a gate and, once it stops, the gate closes behind it, entrapping the vehicle and person in the enclosed area.

Entrapment areas can also use mechanical turnstiles or gates to isolate entry to one individual at a time. In addition to electronic access by users, a security officer or member of the facility staff may operate the entrapment area gate electronically or manually.

Maintenance staff members often have unescorted and uncontrolled access into facilities. Managers should take appropriate actions to control maintenance staff access into and throughout the facility.

Maintenance personnel should be required to use a designated entrance, and a list of these personnel should be maintained at the entrance and continually updated. Only those individuals on the list should be granted access.

Maintenance personnel are commonly provided keys or electronic access cards to perform their jobs. Typically these keys allow unrestricted access into critical areas and locked offices. Facility managers should consider restricting access to critical areas to times when employees are present to supervise the maintenance personnel.

Depending on the facility and during increased threat levels, management should consider escort procedures, time restrictions, and limiting the issuance of access cards or keys. Management may decide to limit or suspend functions that are not critical to the operation of the facility.

Depending on the criticality of the location, facility management should consider conducting background and criminal-record checks on maintenance personnel. They could also require maintenance personnel to sign nondisclosure agreements.

Facility managers should consider scheduling specific times when workers are permitted access and closely control their activities. Also consider escorts or frequent checks, including after-hours checks of these personnel. Employees should leave small trash receptacles outside of locked offices for collection, therefore limiting janitorial access to common work areas.

Additional Access Control Measures Incorporating Badges

Some facilities may have an electronic card access control system. Employees use access cards (usually card swipe or proximity activated) to gain entrance. These systems provide management with an audit trail and the flexibility to grant individual access by date, time, location, etc. System administrators can quickly delete cards that have expired or are reported lost. Access card systems and their configurations depend on the type of facility and the level of access control required.

The system should include methods to prevent unauthorized individuals from entering the facility by piggybacking or following behind an authorized individual when a door is open.

Consideration should be given to the amount and type of information printed on an access card that doubles as an identification badge. Return procedures for lost or stolen cards should not identify the location so that if the badge is lost it cannot be used by an unauthorized individual.

Some integrated access control systems display a photograph of the holder on a monitor at the security/reception desk when the card is used. This allows the security officer or receptionist to verify an individual at the point of entry.

In critical infrastructure or where access requires additional levels of security, facility managers should consider integrating a PIN into the card access system. The PIN feature requires the holder to use his or her card and enter a corresponding PIN to gain access.

Background Checks

To protect facilities and critical infrastructure, it is customary to conduct background checks on individuals whose job is related to the continued operation of a facility. Background and fingerprint checks verify employment records, education, credit, or criminal history, etc. It may be possible to obtain background check information through a law enforcement agency, using the National Criminal Information Center (NCIC), after required agreements are established with the Florida Department of Law Enforcement (FDLE) Regional Domestic Security Task Force (RDSTF). Additionally, private companies offer a range of background check services. The costs generally depend on the depth of information requested and range from fairly inexpensive for a simple credit or criminal history scan to expensive (thousands of dollars) for an in-depth personal history investigation.

Badges

A badge program provides management with a method of identifying individuals and controlling admission into and access throughout a facility. Identification badges quickly distinguish employees from non-employees through distinctive markings or when they are part of an automated access control system and can be used to restrict or deny access to critical areas. Because there are several types and methods of badging criteria, facility managers wishing to establish an identification badge system should research badging issuance and administrative criteria to include standards, issuing controls, accountability, replacement procedures, etc.

The following are examples of badging criteria:

- *Permanent badges*—Used for regular full-time employees requiring daily access.
- *Visitor badges*—For visitors, should be visibly different from all other badges. They are intended to be used for short-term access, usually for 1 day (for meeting attendance, etc.). Self-voiding or time-limited badges should also be considered.
- *Long-term temporary badges*—Issued to individuals whose job function may require them to be on site for a predetermined period of time, such as maintenance staff, contractors, temporary employees, etc.
- *Restricted badges*—Should be a distinctive form of identification intended to limit the wearer's ability to move freely throughout the facility or to selective areas (restricted to a certain floor, loading dock, mailroom, etc.). This badge may also display the words, "ESCORT REQUIRED."
- *Exchange badges*—Used in critical facilities or for stringent visitor processing. Employees or visitors provide a credential (usually a driver's license) in exchange for another credential from the security force in order to gain access to a designated restricted area.

- *Distinctive badges*—Color-coded badges can be used to identify work functions, (e.g., blue badge for maintenance, red badge for food service, green badge for cleaning personnel, etc.).

All badges should be displayed above the wearer's waist.

Building Security Checks

Security officers or other personnel who perform roving patrols should use a systematic method of security checks to ensure the integrity of the facility. Facility management should develop written instructions outlining responsibilities, especially during increased threat level periods.

Facility management should adopt a plan for each location that includes use of security personnel to conduct routine inspections of all property and buildings. It should include a thorough search of all areas of the building and site comprising sensitive item storage areas, common areas, building access points, doors, windows, etc. An employee security awareness program should be implemented.

Facility managers or security officers should check skylights, sewer grates, or hatches that could provide access to a building or area. Hatches should be secured with padlocks and alarmed, or welded shut (if access is not required). Secured hatches must be checked on a routine basis for signs of tampering or unauthorized access.

Before leaving the facility, employees should routinely survey their workstations and surrounding areas to ensure that nothing suspicious has been introduced. Additionally, all maintenance and utility rooms, closets, and other potential hiding places should be checked. All windows, hatches, and doors must be secured. Employees should ensure that all sensitive or classified material is properly secured.

During heightened states of security, managers should conduct periodic building checks (daily, hourly, etc.) of the interior and exterior for suspicious packages or persons. Random checks should be conducted daily or weekly.

Facility inspections should be conducted by trained security officers or employee volunteers. Inspection efforts should be coordinated with local emergency response forces and, if feasible, conducted together.

Procedures should be implemented for documenting inspection strategies and for recording and reporting findings.

Managers should emphasize individual safety precautions during training scenarios and actual events.

Separate inspection procedures should be established for situations in which employees and other building occupants would be advised of an inspection and those in which they are not advised.

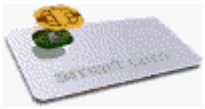
Controlled Area (Access)

Facility managers should identify and designate controlled or restricted access to sensitive operating areas within the facility. Job descriptions and the "need to enter" should determine access into these areas. Examples of critical or sensitive areas are: utility, telephone, and wire rooms, network operations centers (NOC), hazardous materials (HAZMAT) storage areas, weapons storage areas, executive suites, executive parking, special project areas, laboratories, security offices (including control centers), alarm and fire control panels, communications circuits, heating, ventilation, and air conditioning (HVAC) systems,

explosives/flammables storage areas, high-value-item or drug storage areas, warehouses and loading docks, etc.

A zone access plan can be implemented at an increased threat level by allowing open access to a facility, but zone-restricted access to specific portions of the building (permanently or temporarily) when warranted by security concerns. Consideration should be given to installing CCTV, intrusion detection systems, turnstiles, and remotely activated doors at access points.

Techniques to restrict access include limited distribution of keys, mechanical or electronic cipher locks, card access control (with or without PINs), and biometrics. These techniques can be combined for additional security during normal operations or increased threat levels.



Electronic access control cards and cipher locks are a convenient way to restrict individual access into critical or sensitive areas. Access cards can be programmed to activate selected doors or access points by day or specified time periods.

Access to executive suites or floors should be controlled and limited to those who have a legitimate business need to enter the area. Access can be controlled by an electronic card access system with an optional level of security incorporating a PIN.

Alternative ways of accessing the executive area should be considered, such as personnel and freight elevators and stairways. These should be reviewed to ensure controlled access.

Reception areas incorporating remotely activated entrance doors (e.g., requirement to be buzzed in by a receptionist) can be used to control access. Another option during increased threat levels is to post a security officer at the entrance door.

Consideration should also be given to a separate entrance/exit for executive areas, or alternate exit routes in the event of an emergency.

Deliveries

Facility management should have a procedure for receiving and processing deliveries that includes the type of delivery, delivery carrier, addressee, package contents, and shipment verification, inspection, etc. During increased threat levels, critical infrastructure or certain facilities may require additional levels of protection.

At low threat levels, it may be adequate to have each office receive deliveries. However, personnel who receive deliveries should be trained to identify suspect parcels and how to handle them.

During increased threat levels, managers should consider establishing a pre-notification process for deliveries, requiring the delivery company to notify the recipient of a forthcoming delivery. The recipient should call the delivery company (on a pre-determined list of approved telephone numbers) to verify that the caller and delivery is legitimate. Once verified, the shipment contents should be inspected.

A method of screening for explosive devices should be identified for each threat level. At low levels, visual detection may be adequate. At higher levels, the use of explosive detection equipment such as an x-ray machine, vapor analyzer, or explosive detection dogs is recommended.

Deliveries may need to be accepted only at a central loading dock for inspection outside the facility and immediately upon delivery. If a separate gate is designated for trucks, risk can be minimized by requiring that deliveries be inspected there.

Only critical supplies or equipment necessary for the continued operation of the facility should be delivered during high threat levels.

When threat levels increase, employees should be advised to limit requests for services from delivery personnel. Facility management may consider suspending deliveries until the threat subsides. An explosion-proof container may be needed at the delivery point.

Managers should develop procedures for scheduling the screening of deliveries, including U.S. mail, express parcels, building supplies, fuel, etc. You can arrange and coordinate your most common deliveries—FedEx, UPS, Emery, and Airborne, for example—and see if they will agree to become "trusted" shippers (i.e., they will have a regular, authorized backup driver who can be issued a pass that allows the delivery vehicle access).

Consideration for accepting only critical supplies or equipment necessary for the continued operation of the facility should be made during high threat levels.

Employees (both at home and work) should be constantly alert for unexpected package deliveries. They should also be aware of individuals disguised as maintenance workers or food or parcel delivery personnel, and should verify and inspect all deliveries to ensure they appear safe. Suspicious deliveries should be immediately reported to local law enforcement authorities.

Food Vulnerability

Food or food sources are not usually thought of as terrorist targets. Personnel in the food industry must be keenly alert to suspicious activity or personnel where food is being prepared or stocks are being maintained. Moreover, the inspection and evaluation of food items must be given a critical review by members of the Public Health department.

If food is identified as a suspected threat, the Public Health department will need assistance to increase the number of inspections. Medical facilities must be ready to respond to large numbers of patients and maintain the capability to advise leaders on how to contain and eradicate illnesses. Officials must be alerted early in order to attack diseases, and if a threat is identified must be capable of securing and storing a significant supply of food known to be uncontaminated.

Inspections (Personnel)

Personnel inspections are commonly used to prevent dangerous or prohibited items from entering a facility. During low threat levels, managers may decide to conduct random inspections or none at all.

As the threat increases, more stringent inspection procedures may be warranted. Prior to establishing inspection procedures, detailed policies and procedures should be developed and reviewed by legal department representatives. Employees must be made aware of the

policy and preferably sign an awareness statement regarding inspections as a condition to access the facility, with strong consideration given to critical infrastructure or operations facilities.

Facility managers should post appropriate warning signs at facility entrance points indicating that all persons and property are subject to inspection.

Security officers require training on proper techniques and methods of conducting inspections and legal stipulations of inspection and seizure guidelines. Personnel entering critical facilities or areas may be inspected with hand-held magnetometers or patted down, and their hand-carried belongings may be examined.

Management must ensure that security officers and/or designated employees who supplement inspection procedures have been adequately trained in inspection techniques and procedures. Procedures should be established in the event that questionable items are found.

Procedures should specify that in the event a pat-down is required (based on credible evidence) male security officers inspect males and female security officers inspect females.

Law enforcement officials should be contacted immediately if suspicious or dangerous items are discovered. The individual or item(s) should be immediately segregated to protect personnel from potential danger.

Random inspections may be used, particularly at increased threat levels, as a means to help prevent weapons or other dangerous items from being brought into a facility. The two primary types of inspections are manual inspections conducted by security or—preferably—law enforcement officials, and technical inspections using such devices as magnetometers or x-ray scanners. Technology is currently available for vapor trace detection of explosive residue and full-body scanning, but these are generally limited to extremely high-risk situations.

Locks

Facility managers should determine the type of lock based on the amount of protection required.

Managers should be aware of life safety considerations to protect employees for existing locks and for installing new door locks. Installation must conform to the provisions of the National Fire Protection Association (NFPA) Life Safety Code and comply with more stringent codes where they apply. Locks should also comply with UL® listings, BOCA®, UBC®, SBC®, and IBC® building code requirements.

Below are examples of various locks:

- *High security padlocks*—These locks are extremely heavy and require special keys. The interior of the lock is covered by a steel sleeve that ensures the lock is not bypassed.
- *Electronically controlled locks*—These door locks allow an individual, such as a receptionist, to control access into a facility by remotely unlocking a door with an electronic switching mechanism, allowing a person to enter. The individual granting entry should be able to observe the person before allowing him or her entrance.
- *Pin tumbler padlocks*—These locks are commonly used on storage cabinets and are often referred to as padlocks. They are constructed so that a key or a combination wheel must depress a pin in the key insert slot before they unlock.

1575 - 1200 lbs. Gates

- *Magnetic lock*—Electromagnetic door locks are commonly used in conjunction with card access systems. Electric strike locks may operate fail-safe or fail-secure. A fail-safe electric strike lock requires power to remain locked. A fail-secure electric strike is the most common type of magnetic lock. It remains locked from the outside, even without power. A doorknob or lever on the lock allows for safe exit. Managers must ensure that federal, state, and local building department regulations as well as fire and life safety code requirements are maintained. Ensure that locks are UL® listed, and meet NFPA Life Safety Code 101®, BOCA®, UBC®, SBC®, and IBC® building code requirements.
- *Coded locks*—Coded locks are usually installed to control access into small areas such as file or storage rooms. They require the user to enter a series of numbers to unlock the door. The inherent concern with this type of lock is that the code is susceptible to unauthorized detection if not safeguarded from disclosure by the user. It also requires adequate administrative controls to ensure the code is changed on a regular basis.

Key Accountability

Facility managers need to ensure that they develop a stringent administrative key control procedure that restricts key access.

A full-time employee should be assigned as a key control manager. In the event the key control manager is unavailable, a second employee should be assigned as a backup.

The issuance of keys, spare cylinders, and padlocks should be strictly controlled.

The accountability of master or change keys should be maintained and they should only be issued to regular full-time employees.

The key control manager should develop a master list identifying the key number and corresponding lock. Issued keys should be documented on a key control log after verifying access privileges from appropriate supervisors.

All unissued keys should be stored in a locked metal cabinet, file cabinet, or key safe accessible only to the key control manager or his or her designate.

Keys should be inventoried each time the cabinet is opened, or at least weekly if they are not used frequently.

Locking cylinders should be changed when a key is reported lost or stolen.

The key control manager must ensure that individuals no longer requiring key access to a location return keys immediately.

Mail Security

Employees who process and receive mail from the United States Postal Service or other sources should be trained in identifying suspicious parcels and how to handle them. They should be provided with written and visual guidelines for identifying and handling these packages. Posters detailing the identification and handling of suspicious items should be displayed.

Package screening machines (x-ray) and portable explosive screening devices can be used to screen incoming mail. These devices can be very expensive and are not affordable for many facilities; however, for high-risk facilities they should be strongly considered. Sound policies and in-depth procedures must be developed prior to implementing use of x-ray

machines and other screening devices. A variety of sources provide similar precautionary information concerning protection from letter or mail bombs (including biological threats).

- *X-ray devices*—may be used to identify weapons, bombs, or other dangerous items individuals may bring into a facility. The use of the x-ray technology is precautionary in the lower threat levels, but may become necessary as threat levels increase, especially when critical facilities are involved. Adequate training of the x-ray machine operator is critical to properly identify questionable items. Portable x-ray machines can be used during increased levels of security.
- *Magnetometers (metal detectors)* are commonly used at building or site entrances. Facility management should determine the need for these devices. Hand-held metal detectors are very effective to isolate searches of a specific area on a person and locate items constructed of porous metal, such as guns. Managers may elect to use these devices periodically or randomly at entry points depending on the criticality of the location. Operators must be properly trained and familiar with detection criteria to use these devices.
- *Vapor trace analyzers* are used to detect traces of explosive residue. Individuals who handle explosive devices often leave explosives residue on their hands or clothing, which is then transferred to other articles such as laptops or briefcases. System operators can test suspected areas and receive near instantaneous readings. While these systems are costly, they are reliable and readily available. Main entry points of critical facilities and mailroom operations may consider using vapor trace analyzers.

Employees should not accept express mail packages on behalf of other employees unless they are certain the package is expected.

An alternative mailroom location should be designated for use during periods of very high threat levels, in order to segregate the item until responding emergency personnel can examine it. The alternative mailroom may need to be outside the main structure.

A method of screening mail for explosive devices should be identified for each threat condition. At low levels, visual detection may be adequate. At higher levels, the use of explosive detection equipment such as an x-ray machine, vapor trace analyzer, or explosive detection dogs may be necessary.

An explosion-proof container may be needed in some facilities.

Visitor Control

Depending on the facility and threat level, managers need to establish a policy for processing visitors. This could include the requirement that visitors have controlled access into and throughout a facility. Uncontrolled access allows the potential for damage or destruction of property.

Visitor control measures include the following:

- All visitors should be processed at one entrance point to the facility.

- Visitors can be required to follow a prenotification process before traveling to the facility. This process requires a visitor to call and arrange a visit with a sponsoring employee who would process the visitor and possibly escort them during their visit.
- Visitors should sign in and out on the building admissions register, sponsored by an employee, and be issued a distinctive visitor's badge.
- *Verification*—Facility and departmental managers determine the necessity for visitors and or employees to enter restricted or sensitive areas (e.g., tape library, data rooms, power facilities, etc.). Entrance should be based on need. Unrestricted access may lead to the compromise of proprietary information or the destruction, damage, or theft of critical equipment. Prior to allowing a contractor access into a restricted area, verify and positively identify the contractor by conducting telephone or background checks to substantiate their need to enter the facility. Managers should not deviate from this policy because it is often the most critical and overlooked access control violation.
- During increased threat levels and when prenotification procedures are not in effect, visitors may need to be escorted by an employee while on company property.
- Facility managers should determine the need to additionally identify and control visitor access during increased threat levels by requiring them to produce an official document (driver's license, passport, etc.) which exhibits the holder's photograph to verify their identity before being issued a badge (managers assigned to critical operating facilities may require two forms of identification). This process often includes the individual's driver's license (or other official document), which can be retained at the entrance point and returned at the conclusion of the visit. This procedure ensures visitors are properly processed at the point of entry and the visitor badge is returned.
- During increased threat levels or at critical operating facilities, managers may determine the identity of a prospective visitor in advance by calling a predesignated telephone number to verify the need for the visit. After verifications are completed, visitors should be briefed on security policy and must remain with assigned escorts at all times.

PART IV: ENCYCLOPEDIA

Chapter 3: Emergency Services

Introduction

This chapter provides explanations of procedures for emergency services coordination or development of emergency planning documents. Managers should consider these techniques before there is an actual emergency situation. These measures can be implemented by the public sector, private sector, and for special venues.

Building Plans

If a terrorist incident occurs, emergency response officials may need access to facility plans and blueprints. Officials may need to shut down power and/or water and require communication lines for external telephones.

Emergency services officials, including local police and sheriff departments, fire and emergency medical service providers, and HAZMAT teams, should have up-to-date copies of building and floor plans with site maps. Maps should be current and indicate street names, dead-end streets, access points, buildings, power stations, entrances, and fenced areas.

Plans and blueprints may be transferred to computer media (e.g., diskette or CD) and provided to emergency responders well in advance of an incident. They should also be restricted to persons who have a "need to know" and secured from unauthorized access.

Chemical, Biological, Radiological, and Nuclear Explosive (CBRNE) Plan

Emergency response activities involving weapons of mass destruction (WMD) should be included in all response plans. Periodically review CBRNE response and recovery action plans with local government agencies. As terrorist threats increase or an incident unfolds, immediately review the plans on CBRNE and activate the predeveloped action plan. If the facility has a CBRNE team, brief them on the status of the threat, incidents, or any intelligence which may apply and use other added measures as necessary. Periodically review CBRNE response and recovery action plans with involved agencies.

Critical Employees

During increased threat levels, only employees who have been identified as critical for maintaining the continued operation of the facility should report to work. Facility management should maintain communication procedures to advise non-essential employees to remain away from the workplace.

Critical employees should be selected by job function and may need to be trained for different types of emergencies.

A roster of critical employees should be maintained and updated regularly to ensure an adequate work force has been retained to respond.

Personnel should understand their role and need for availability. Because of the threat condition, critical employees may be trained in actions to help counter the terrorist threat.

Managers should establish criteria and procedures for retaining critical personnel at the facility in the event of an emergency. Provisions such as food, water, and sleeping arrangements should be included in planning efforts. In some instances, arrangements may be made for critical workers to stay in hotels located near the work site.

- Managers should maintain reliable and practical contact procedures for critical personnel who may be involved in or respond to an emergency or disaster situation.

- The recall system should be tested and updated periodically to ensure that members or alternates are available on a 24-hour-a-day, 7-day-a-week basis.
- The recall plan should incorporate redundant forms of communication (wireless telephone, radio, etc.) in the event the main mode of communications becomes inoperative.
- Recall personnel should establish realistic plans allowing them to respond to the workplace. They may be provided with distinctive identification to ensure they are allowed access to the site if protected by security personnel.

Evacuation Plans

A facility manager is responsible for ensuring that building (and campus) evacuation plans remain current. Evacuation diagrams should be posted in a user-friendly format at appropriate locations throughout the facility. Evacuation drills should be performed on a regular basis.

As part of the building manager's emergency evacuation plan, rally points should be established for building occupants in the event an evacuation becomes necessary. Rally points should be carefully selected considering personal safety, vehicular traffic flow, and the need for emergency personnel to respond and enter the building, potential types of emergencies, standoff distance, and weather factors.

Building emergency evacuation teams should be established and evacuation training provided. Publicize the location of fire escapes, emergency doors, exits, and stairwells.

Managers should establish a method to ensure that all personnel are accounted for in the event of an emergency requiring evacuation of the facility. This includes personnel who are in the facility and those who would be expected to be in the facility (i.e., ensure that employees who are on vacation or business trips are identified so they are not flagged as "missing"). Visitors and other non-employees should also be accounted for.

Response and Recovery

The state Division of Emergency Management or Federal Emergency Management Agency (FEMA) formulates plans for disasters like floods, hurricanes, tornadoes, etc. Additional response plans for terrorist incidents include requests for federal assistance or assistance from the Federal Bureau of Investigation (FBI) Hostage Rescue Team, etc. Facility managers should be familiar with these response and recovery methods.

- Depending on the operation, managers should assess their facility and determine what emergency or safety personal protection equipment is required. Several items of personal protective equipment can be provided to critical personnel and/or pre-positioned for their use (such as an escape-pack breathing apparatus for chlorine rooms of water plants).
- Other protective items may be appropriate for placement where personnel may be exposed to airborne contamination. Chemical antidotes may need to be stocked, such as atropine injectors for nerve agents. Anti-ballistic vests can be used to protect against a sniper. Armor in these vests must be chosen based on the ballistic threat anticipated.

Response Teams

Facility managers should establish policies and procedures for coordinating with emergency personnel and appropriate public agencies in the event of a terrorist incident. The procedures should include designated roles for corporate management, security and safety personnel, public relations, medical, facilities, and human resources staff.

Types of response teams include the following:

- *Expert Response*—Managers should identify appropriate first responders and other experts or officials who can assist in the event of an emergency. If possible, advance coordination with these agencies should be conducted relevant to facility emergency plans. Information should be shared with Security Control Center operators and other employees responsible for security of the facility or involved in disaster management for the organization.
- *Explosives Response Team*—In the event of a bomb threat or if an explosive device is found or suspected, managers should have identified local law enforcement officials who can respond with an explosives response team. This may include an internal team of security or volunteer professionals. If so, this procedure should be coordinated with and approved by local law enforcement. The internal response team can assist with employee education, evacuation, information collection, and incident management. Some organizations identify and train employees as "floor wardens" or similar roles.
- *Disaster Response Force*—Identify individuals, generally security officers, disaster response professionals, or safety coordinators, to compose a team to assist in investigating disasters and preserving suspected crime scenes.
- *Hostage Response Team*—Managers should establish policies and procedures for a hostage situation within the facility. Coordination with responding law enforcement agencies should be conducted in advance of an actual incident. Include roles and responsibilities for security officers, management, public relations, and individual employees.
- *WMD Teams*—Establish policies and procedures for a possible WMD incident affecting facilities and personnel. Develop policies for team response and include roles and responsibilities for security officers, safety officials, management, public relations, and individual employees.

Information should be readily available for officials responding to the situation, including facility layouts, operation, estimated number of occupants, concentration areas for occupants, hazardous or dangerous materials, weapons stored in the facility, unique or special equipment/operations within the facility, major evacuation routes, location of key personnel, and the location of utility shut-offs/controls (including HVAC).

Identify the proper first responder agency to call and review procedures with that agency before an incident occurs. Coordinate the plan, if feasible, with neighboring facilities and organizations, as well as responsible public agencies.

If appropriate, at least two facility staff members should be trained on WMD response. Training is generally available through federal sources.

Security Office (Control Center)

The security control center (SCC) is the nerve center for emergency operations and is separate from normal day-to-day operations. Facility managers should consider activating a contingency command center 12 or more hours before a major event such as a parade, political rally, public ceremony, convention, etc. The operation of this center is vital immediately following a terrorist attack or incident. The command center should operate with established written guidelines. Both this center and the SCC should have the communications equipment necessary to maintain liaison with local, state, and federal agencies.

- Facility managers should establish a policy for a separate and secure room identified and used as an SCC as part of a facility's overall security protection plan.
- The SCC is usually the central control point for all security alarm lines, CCTV cameras and monitors, HVAC and UPS systems, fire and smoke monitoring and control systems, building emergency notification systems, emergency service response and coordination, and key control functions. Any other critical facility functions determined by the facility manager should be contained within the SCC.
- The SCC should operate 24 hours a day and is usually staffed by on-site security officers under the direction and control of a full-time management employee, exceptions include short-term special events.
- Personnel assigned to the SCC should be trained on alarm monitoring and response procedures and coordination efforts with local EMS departments.
- Access to the SCC should be restricted to persons on a need-to-know basis.

PART IV: ENCYCLOPEDIA

Chapter 4: Communications

Introduction

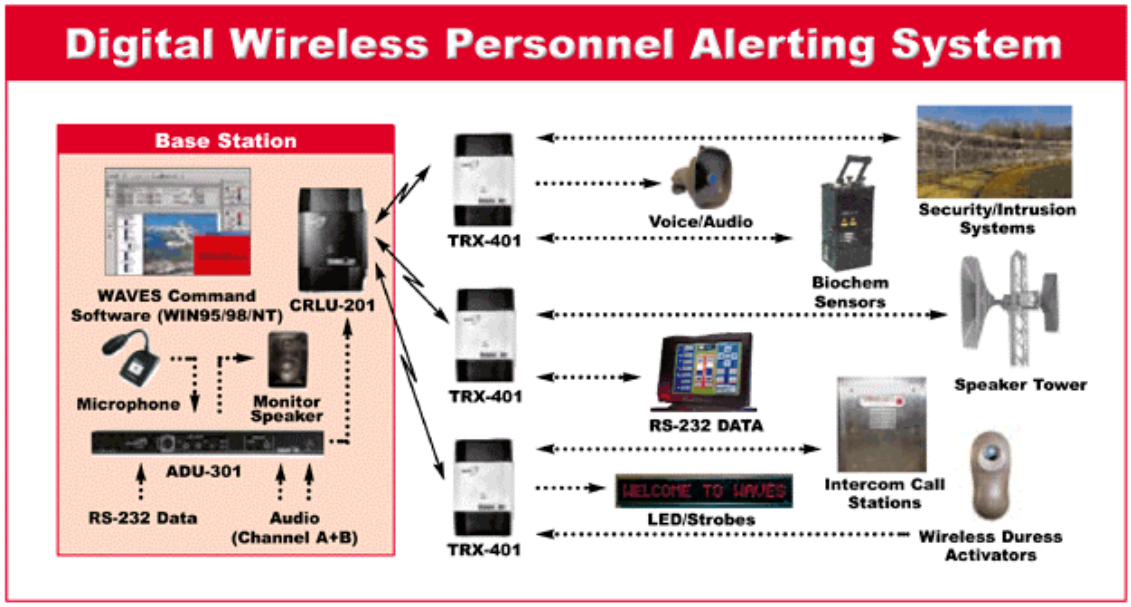
This chapter explains the essential elements of sound communication procedures and timely dissemination of critical information. The methods presented are intended to complement the preceding chapter on emergency services and can be used by the public sector, private sector, or for special venues.

Authenticators

Authenticators are instruments used to ensure and verify the identity of a person who is authorized to send and receive radio transmissions. This is typically a system of code words and/or number combinations published and periodically revised to ensure confidentiality. Authentication codes are restricted documents and are commonly marked "For Official Use Only". They should be distributed only to authorized individuals. It must be recognized at the onset of any disaster or crisis that the use of authenticators may be difficult to maintain due to the need for open communications with outside agencies.

Communications Testing

Facility communications systems and supporting equipment should be inspected and tested on a regular basis to ensure it is functioning properly. Testing can identify malfunctioning equipment, transmission or reception "dead spots," or the need for separate frequencies (i.e., for security, maintenance, HVAC, etc.). Facility management should take appropriate measures to correct deficiencies prior to an actual emergency.



Tests should be conducted simultaneously and include different systems and departments or organizations to identify interference or interoperability issues. Backup or redundant communications systems should also be tested.

Contact List

Current emergency telephone numbers for police, fire, and rescue agencies should be posted. As a threat condition increases, consider publishing the numbers often in the newspaper and request that radio and television stations announce these numbers periodically.

Information Dissemination

During increased threat levels, managers should establish procedures to report incidents and suspicious activities to local law enforcement agencies and other facility managers within their immediate area. Facility managers or security advisors may choose to develop and use an internal computer alert system to keep managers and employees apprised of the status of a threat.

Personnel attending critical threat-level meetings or other sensitive briefings should be positively identified by security managers via personnel security access lists, and have a "need to know" in order to participate. The facilitator conducting the meeting should verify the identities of all individuals using access lists, before discussing restricted or classified information.

Many documents outline sensitive agency information or security activities, vulnerabilities, and protective actions. This type of information requires additional protection using an information security or "need to know" program. When documents are not in use they should be secured and locked in appropriate metal cabinets, file cabinets, safes, etc.

Intelligence agencies normally brief organizational officials at specified times. However, during an emergency or if a terrorist incident has occurred, the intelligence element may provide valuable information to thwart or limit damage from a follow-up incident. Intelligence briefings are provided at different classification levels. The media has a right to know certain information and should be admitted to unclassified briefings periodically in order to keep the public informed.

Threat information at some point becomes public information and citizens should be alerted of the threat through the media. The media can advise the public to be alert and to report any suspicious person, object, or activity. Release as much detail as possible to news agencies via press releases and press conferences.

People often exaggerate threat information and can easily cause panic and chaos. Managers should immediately dispel rumors with extensive media campaigns.

State officials coordinate and provide information to local governments, law enforcement, and emergency service agencies regarding antiterrorism measures. This provides the opportunity for cross-flow of information and implementing security measures which may have been instituted within other jurisdictions.

It is important that the facility manager establish liaison with the local police or sheriff's department to coordinate security and perimeter control measures for the facility in the event of an emergency. Managers should review response procedures with law enforcement officials and private security officers for supporting neighboring facilities.

Facility managers should establish bomb threat procedures (including providing training for personnel) and place bomb threat information cards at each telephone. They should also plan and coordinate actions with local emergency response agencies.

Suspicious activity, people, or incidents must be immediately reported and investigated. Facility managers should instruct personnel to report suspicious vehicles, activity (e.g., clouds of smoke), or individuals (e.g., persons taking pictures), to the local law enforcement authorities by dialing 911.

Suspicious activity can be described as:

- Videotaping in and around the facility, the perimeter, and near restricted areas
- Probing events such as trespassing at several areas of the facility or site

- Unknown individual in a car on or near the property without explanation
- Individual(s) not known to employees striking up conversations with them in nearby restaurants, convenience stores, and gas stations and asking questions about "what goes on in their facility?" and so forth
- Individuals wandering in areas in which they are not authorized
- Unfamiliar individuals tailgating employees into restricted areas and claiming "I lost my badge" or "I can't find my badge"
- An unattended and parked vehicle with the engine running near the facility entrance.

Facility managers can establish a policy of communicating all such activity through the main SCC, if applicable.

Policies and procedures should address methods to conduct building and site inspections for suspicious articles, persons, vehicles, etc. Develop policy and legislation to mandate local firms to report theft of dangerous materials or excessive or suspicious purchases of hazardous materials to law enforcement authorities.

Facility management should provide security officers with information and training that allows them to identify potential threats. To assist in the detection process, security officers must be equipped with night vision equipment, binoculars, radios, etc.

Public Address System

The public address system is an integral part of a facility's emergency management system. It is used to notify building occupants of emergency evacuations or to broadcast messages to employees. Public address system speakers should be strategically installed and located throughout all areas of the building or site (including restrooms) to ensure all employees can hear emergency notifications. The system should be tested on a weekly basis and be connected to the facility's UPS system.

PART IV: ENCYCLOPEDIA

Chapter 5: Security Systems

Introduction

Security systems are generally defined as technological security applications used to enhance, (typically not to replace) other security features. Physical security experts should be consulted prior to purchase and installation, to determine the best security strategies to properly protect given assets. Managers should use this chapter to become familiar with the protective measure options available. These security systems can be used in a variety of settings and may be considered for use by themselves or, ideally (especially for high-risk facilities) as an integrated approach for the holistic security practitioner. These measures can be implemented by the public sector, private sector, or for special venues.

Alarm Systems

Intrusion detection and alarm systems are installed to provide protection of assets, employees, and company property. Alarm systems are designed to detect unauthorized entry and alert persons responsible for the security of the premises. The decision to install an alarm system should be made by the facility manager after determining the criticality of the location and level of protection required. The following are some capabilities and components of alarm systems.

An alarm system must be augmented by personnel assigned to react to alarm conditions. Because alarm systems vary, systems must be carefully selected and designed for each facility.

There are three basic types of alarm systems:

1. Local alarm system—activates an alarm condition in the immediate vicinity of the protected area. It is usually used when local security officers are within sight or hearing and can respond.
2. Alarm system connected to a 24-hour central alarm monitoring station—generally a commercial company that is contracted to provide intrusion and fire alarm monitoring. On activation of an alarm, the central monitoring station takes appropriate action, which may include notifying local police, fire/rescue departments, and building managers.
3. Proprietary alarm system—controlled and monitored within the facility. The system usually reports to an on-site SCC. Alarm response is provided by an on-site security force, which may be supplemented by local law enforcement. This type of system can also be monitored by local law enforcement agencies or by a central alarm monitoring station, providing a backup method of reporting and response. The coordination of response efforts should be considered.

Alarms must immediately detect intrusion and be forwarded to an SCC, police agency, or 24-hour monitoring system, which will activate appropriate response efforts and corrective measures.

Alarm transmission lines should be tamper resistant and enclosed in conduit. Signal alarm lines should be protected from the facility to the alarm monitoring point and indicate system malfunction. It should include a battery backup or be connected to the facility UPS system.

Consideration should be given to a secondary method of alarm transmission, such as cellular or radio backup, in the event normal transmission lines become inoperative.

An intrusion alarm and monitoring system should conform to UL and manufacturers' specifications. The system should be serviced, maintained, and tested on a regular basis.

Alarm contacts should be surfaced-balanced magnetic switches or concealed alarm contacts, which are common methods used to monitor entrance doors to protected areas. Card access systems, electronic cipher locks, or remote door releases should be tested after installation to ensure that the safety release motion sensor or release button (required by most fire codes) cannot be activated from outside the protected door.

- Install a high-quality intrusion detection system consisting of a sensor suite, transmission mode, notification scheme, and response mechanism that is appropriate to the facility's size, design, function, mission, culture, and other security features. Include arrangements for maintenance, service, and expansion as necessary.
- Alarms should be installed in selected zones including windows, evacuation areas, and doors leading into restricted areas, etc. Duress alarms should also be considered. Alarms should be tested regularly to ensure they operate effectively. Increase frequency of transmission line/signal security checks to weekly or daily as the threat level increases.
- Consider integrating the intrusion detection system with the existing or planned access control, visitor control, badging, communications, and fire protection systems, as appropriate.
- Conduct a comprehensive system test including sensors, transmission, notification, and response at least quarterly.
- Check transmission line security (hardwire) and verify transmission signal integrity (wireless) at least quarterly. Transmission lines should indicate any system malfunction.
- Review security systems contracts to verify your service priority and determine the vendor's procedures/capability for meeting service commitments and orders for additional system components during high demand periods.
- Consider arranging contingency/backup contracts for security systems service and augmentation (orders for additional system components).
- The system should include a UPS backup system for the SCC. Consideration should also be given to a secondary method of alarm transmission in the event normal transmission lines become inoperative.
- Contact switches should be balanced magnetic switches, common methods used to monitor doors to protected areas. Card access systems, electronic cipher locks, or remote door releases should be tested after installation to ensure that the safety release motion sensor or release button (required by most fire codes) cannot be activated from outside the protected door.

- Consider establishing internal capabilities to maintain and expand security systems (hire a security systems technician or team, as appropriate).

Consider whether an electric magnetic lock results in a "fail-open" or "fail-closed" condition in the event of power failure or fire alarm activation. For safety purposes, most systems default to fail-open, in which case procedures must be established to control access to the area during power failures or fire alarms (including false alarms). Otherwise, intruders may use false fire alarms or intentional power failures to circumvent the access control system and gain entry to the facility or restricted area. (See: Locks section).

Access Control Systems

Some facilities may need to install an electronic card access control system. Some locations may have inactive card access systems and need to activate them during increased threat levels. Employees may have been issued access cards (usually swipe or proximity) to

gain entrance to a facility. These systems provide management with an audit trail and the flexibility to grant access by date, time, location, etc. System administrators can quickly delete cards that have expired or are reported lost. Access card system and its configuration depends on the type of facility and the level of access control required.

- The system should include methods to prevent unauthorized individuals from entering the facility by piggybacking or following behind an authorized individual when a door is open.
- Consideration should be given to the amount and type of information printed on an access card. Return procedures for lost or stolen cards should not identify the location so that if the badge is lost it cannot be used by an unauthorized individual.
- It may become necessary to post security officers at access points into the facility to assist in access control. Depending on the situation, these officers may need to be supplemented by armed personnel.
- Some integrated access control systems display a photograph of the holder on a monitor at the security/reception desk when the card is used. This allows the security officer or receptionist to identify an individual at the point of entry.
- In critical infrastructure or where access requires additional levels of security, facility managers should consider integrating a PIN into the card access system. The PIN feature is used in conjunction with an access card and requires holders to use their card and enter a PIN to gain access.

- Biometric devices are becoming increasingly common as an identification measure for security and access control purposes. Biometric security devices are typically used to allow or deny an individual access to a controlled door leading into a restricted area. They may be used alone or in combination with other security components, such as a PIN or electronic access card. Biometric devices in use include:
  - Hand geometry
  - Thumb/finger reader
  - Iris scan
  - Facial recognition
  - Weight portal
- Intercom systems are often used to announce arrival of visitors or non-employees before entering the facility. Personnel should not allow access into secured or critical operating areas until the visitor's identity and reason for visit is verified. It is crucial that the intercom be supplemented with a CCTV monitor or other means of visual identification.

Surveillance Systems

A CCTV system enables security officers to remotely monitor areas of concern or interest. The system can allow operators to simultaneously monitor several areas and provides the opportunity to detect potential intruders or observe destructive acts.

CCTV systems can be used to monitor selective entry points of a facility. They can also be used to monitor critical operating areas such as HVAC, power stations, computer rooms, parking lots, loading and receiving docks, intercom systems, etc.

Facility managers considering a CCTV system should thoroughly research the type of cameras required, method of retaining video images (tape or digital), monitoring capabilities, and the placement of interior or exterior cameras. The three basic components of a CCTV system are the camera, monitor, and switcher. Other supplemental components can be added to the system such as video recording, motion detection, and video storage capabilities.

Cameras should provide video images of sufficient clarity for security audit and identification purposes. Consideration should be given to the types and styles of cameras that will be used. Interior cameras may have different viewing capabilities than exterior cameras. Illumination levels must be sufficient to provide high quality and clear video images of the monitored area.

Video monitors should be a minimum of 13 inches for a single camera operation and 19 inches for multiple cameras. Multiplex monitors, which allow viewing and recording of numerous cameras at one time, are also an option. Larger monitors can be positioned within the monitoring center and used for supplemental viewing of areas of concern.

Cameras can be programmed to activate in conjunction with an intrusion alarm or can be activated by motion. This arrangement should result in an alarm condition at the monitoring station (SCC) that automatically records the event.

Exterior cameras should have pan, tilt, and zoom capabilities. In areas where inclement weather may obscure monitoring, they should be enclosed in secure, weather-tight boxes with heat, wash, and wipe capabilities.

CCTV cameras should be programmed to record in "real time" and store images digitally. When digital storage is not possible, VHS tapes should be maintained for at least 30 days before recycling. VHS tapes should be replaced at least every 6 months to ensure clarity of images.

CCTV monitoring should occur in the SCC and can be viewed on a multiplex monitor.

Critical alarm areas monitored by CCTV cameras should activate an audible alarm within the SCC and automatically display the area of concern on a separate monitor where security personnel can remotely view the area.

Digitally stored CCTV systems can be remotely monitored by off-site managers. With proper controls, managers can access CCTV images through the Web.

The CCTV system should have an extended battery backup or be tied into the facility's UPS system to ensure continued operation during a power failure.

X-Ray

X-rays are devices that may be used to identify weapons, bombs, or other dangerous items. The use of x-ray technology is precautionary in lower threat levels, but may become a necessary as threat levels increase, especially when critical facilities are involved. Adequate training of the x-ray machine operator is critical to properly identify questionable items. Portable x-ray machines can be used during increased levels of security. (Also see vapor trace analyzers).

Magnetometers (Metal Detectors)

Metal detectors are commonly used at building or site entrances. Facility management should determine the need for these devices to ensure that explosives, weapons, or other dangerous items are not brought into a facility. Hand-held metal detectors are effective in isolating inspections of a specific area on a person and locating items constructed of porous metal, such as guns. Managers may use these devices periodically or randomly at entry points depending on the criticality of the location. Operators must be properly trained and familiar with detection criteria to use of these devices.

Vapor Trace Analyzer

This equipment is used to detect traces of explosive residue. Individuals who handle explosive devices often leave explosives residue on their hands or clothing, which is then transferred to other articles, such as laptops or briefcases. System operators can test suspected areas and receive near instantaneous readings. While these systems are costly, they are reliable and readily available. Main entry points of critical facilities and mailroom operations may consider using vapor trace analyzers.

CBRNE Defense

When equipped with advanced WMD detection devices for biological, chemical, or radiation releases (dirty bombs) on a site, alarms are positioned upwind to detect attacks. Unless enough detectors are installed to cover all wind directions, detectors must be moved so that they remain upwind of the facility.

Procedures for alarm acquisition, placement, and maintenance should be developed. These procedures should also address actions to be taken if an alarm occurs. Training and practice drills should be conducted regularly. Safe, sealed-off areas, protective clothing, antidotes, and decontamination supplies should all be considered in planning.

PART IV: ENCYCLOPEDIA

Chapter 6: Security Design

Advisory Note

This chapter provides threat mitigation strategies for physical security design to protect facilities against threats. Prior to implementing these measures managers should consult with the nearest FDLE RDSTF to discuss implementation. While many of these measures can be applied to a variety of facility categories, some are applicable only to very high threat facilities and typically for protection against specific standoff threats. Some of the other protective measures explained (e.g., doors), however, can be used by all facility risk categories and threat levels.

Aerial Denial

If a threat of helicopter or parachute insertion of aggressors is credible, an aerial denial plan should be prepared. Cables strung between poles above buildings or areas can be used to interdict or deter helicopter and parachutist from landing. However, an intruder could still descend from a helicopter via a rope.

The most effective method for protecting against this threat is to detect the intrusion and react. Two methods are the use of guards and rooftop lighting. A reaction force and alarm system should be prepared, trained, and equipped.

Doors

Facility managers should ensure that all exterior and interior doors requiring additional protection from intrusion are hung so that the hinges are on the inside of the door and thus are not vulnerable to removal of the hinge pins. Hinge protection methods include tack welding or peening the hinge pins to prevent easy removal, or using set screws in the knuckle to lock the hinge pins. Doors in which hinges can be removed should be provided with security studs in the hinge plates. These studs extend into the door and the door's frame and retain the door if the hinge pins are removed. Astragals should be installed to protect latch bolts from being tampered with.

Doors leading into spaces which require additional levels of security should be alarmed and monitored by either an on-site SCC or 24-hour alarm monitoring center.

For a minimal level of protection, provide stock hollow-steel or steel-clad doors with steel frames. For higher levels of protection, provide forced-entry-resistant doors set in reinforced masonry or concrete walls.

It may be advisable in extreme situations to construct masonry walls opposite steel exterior doors to create a foyer. The wall's purpose is to catch the door or its fragments if the door is blown open, limiting injury to the facility's occupants. Use stock hollow-steel or steel-clad doors and pressed steel frames for the interior and exterior foyer door. The interior and exterior doors should be offset from each other. In cases where explosives may be used, at high-risk facilities, use blast-resistant doors installed as above.

Door peepholes are simple and inexpensive tools often overlooked in security design. They should be installed in doors leading into sensitive or critical areas, particularly in areas that receive visitors on a regular basis (such as maintenance technicians).

When installing peepholes, ensure that the installation does not compromise the integrity of the door. It is important that employees are aware that it is necessary to screen individuals before opening the door. This type of security device should only be used when personal recognition is mandatory.

Where lockdown procedures are used, such as at schools, the hallway doors should be equipped with deadbolt locks which are keyed for access from the hall and with a turn knob on the room side.

Explosive Containers

These containers should be located where explosive devices may be found, such as at building entrances where inspections are conducted, mailrooms, and delivery docks. Untrained personnel who detect an explosive device should only use such a container in a dire emergency in order to minimize damage from an explosion and to facilitate inspection and transportation of the device by experienced law enforcement authorities. Moving a suspect device (especially one found versus mailed or shipped) is very dangerous and should not be attempted.

HVAC

Fresh air intakes for building HVAC systems should be protected against introduction of airborne contaminants such as anthrax spores, chlorine gas, or nerve agents. The simplest way to protect the intake is to relocate it to the roof, where access can be denied. Chemical detection alarm systems and filtration systems are available, but cannot protect against all types of contaminants. Zoning of HVAC systems by installing motorized, airtight dampers can be effective in minimizing exposure if an attack is detected. Emergency shutdown switches may be installed to quickly shut down the HVAC system.

Pre-Detonation Screens

To protect roofs, walls, and windows from attack by standoff weapons such as rocket-propelled grenades or mortar, installation of pre-detonation screens may be advisable. Such screens are heavy wire and cause the projectile to detonate before hitting the building. Protected windows should have heavy curtains to protect against glass shards and fragments. Walls should be masonry to stop fragments from a detonating weapon. The military considers a 6-inch thick concrete wall, or concrete block wall with concrete filled cells, as the standard for stopping such fragmentation.

Standoff weapons are designed to penetrate an armored vehicle, which means they will penetrate approximately a meter of concrete. The use of a pre-detonation screen can defeat such weapons if adequate standoff distance is provided. The distance between the pre-detonation screen and the building also depends on the building construction.

Roofs

Roof Reinforcement

Where concern from mortars or explosives placed on the roof exists, roof or ceiling reinforcement may be warranted.

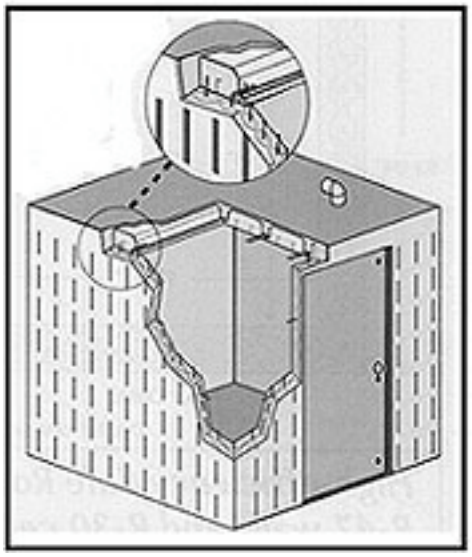
In multi-story buildings, the top floor may simply be evacuated, leaving the roof as a pre-detonation barrier, and using the floor below to protect against fragments. In this case, placement of sandbags on the floor may be advisable.

Normally, buildings are designed to support sufficiently heavy live loads so as to not require structural reinforcement for the added weight of the sandbags. Otherwise, the roof or ceiling just under it can be reinforced and the top floor can remain occupied. Qualified individuals should perform design and reinforcement because the added weight of the reinforcement may require structural supports.

Roof Access Control

Access to roofs by unauthorized individuals can pose a significant threat to HVAC fresh air intakes located on the roof, and raises the possibility of an explosive being placed. Managers should remove exterior ladders that provide roof access. Interior roof hatches should be secured and alarmed and consideration given to extending walls or erecting fencing to deny roof access.

Safe Room



If a threat of an airborne contaminant, intrusion, or threat to personnel exists, providing a safe room may be advisable. Safe rooms can be designed to counter airborne contaminants, intrusion, and explosive threats. Depending on the threat, safe rooms should have reinforced walls, ceilings, and floors, as well as reinforced doors with peepholes. The room may be isolated from the building HVAC system (have a separate air intake and filtration system) to protect against airborne contaminants. Equipment and supplies such as cellular phones, radios, first aid supplies, and water may be stockpiled inside the room depending on the assessed threat.

In schools, a safe room for protection from a bomb threat could be the most structurally sound area (hallway) in the interior of the building, not a gymnasium, which normally has high, concrete block walls subject to collapse from explosion overpressure.

Walls

Continuous walls that extend from the floor to the bottom of the floor of the next story should be used in sensitive or critical areas or for any room in which intrusion must be prevented. This construction method prevents potential perpetrators from accessing rooms by crawling over false or suspended ceilings or under false floors to insert listening devices or explosives, etc. Walls constructed of drywall over studs (standard frame construction) will not stop an intruder and must be reinforced with plywood. Penetrations in these walls for mechanical ducts must be considered and installing ducts with bars or other barriers that do not appreciably restrict the flow of air, but do prevent intrusion. In existing facilities without floor-to-ceiling walls, retrofitting can be accomplished using standard renovation techniques. Consider slab-to-slab construction in multi-tenant facilities for walls that adjoin other tenant areas to protect against intrusion from a neighboring suite.

Blast Walls

When adequate standoff distance cannot be achieved, one possible solution is to construct a blast wall. If properly located, blast walls can protect a building from a bomb blast and subsequent fragmentation. In any case, standard glass windows should be fitted with blast film or curtains. Blast walls can be made of concrete, wood, earth, stone, or even vegetation, but only concrete or a similar substance will protect against fragmentation. Earthen blast walls can be constructed by using berms or, on a temporary basis, by using earth-filled, manufactured plastic grid systems for that purpose.

Where building construction is masonry and windows have heavy curtains, protection from blast pressure and impulse may be sufficient. Blast walls should be located outside of the clear zone. However, locating a blast wall too far from a building can allow the shock wave to go over the wall and damage the building. Normally a concrete blast wall will be about 8 feet high, at least 8 inches thick, and set 20 inches into the ground. Design of a blast wall system should be performed by a qualified individual and be based on an anticipated bomb size.

Frame Reinforcement

Where masonry wall construction exists (load-bearing cinderblock with no concrete or steel columns) and the risk of a bombing is a concern, reinforcement of the wall should be considered. The blast pressure of a sizable bomb can cause a large wall, such as for a gymnasium, to fall into the building. If the roof is not supported by columns and beams, but simply rests on top of the masonry wall, it can collapse and cause far more casualties than the collapse of the wall. Large masonry load-bearing walls can be reinforced by adding steel columns and beams to support the roof in the event of wall failure. A structural engineer should design such reinforcement.

Wall Reinforcement

Reinforcement of walls may be necessary to protect against explosions and standoff weapons. The requirement for wall reinforcement will depend on the assessed size of the explosive device or type of weapon, the clear zone that can be achieved to protect against an explosive left near the building exterior, or the standoff distance for parking and adjacent roads to protect against car bombs.

The design of the wall reinforcement should be based on the bomb size and should be performed by a qualified individual. Normally, reinforcement walls to protect against blast would be constructed of masonry or reinforced concrete to protect buildings of frame construction. Blast walls may be a more economical option than wall reinforcement where space is available for them and not for an adequate standoff zone.

Windows

Windows present a weak point in the defense of any building. Snipers can engage targets through them, and not only do they not offer resistance to blast effects, they enhance the damage by shattering and creating glass projectiles. Window treatments come in two forms: obscuration and blast effect mitigation. Some countermeasures address both effects.

Curtains

In the event of an explosion, heavy curtains will entrap the glass shards and dissipate their energy, causing them to fall harmlessly to the floor. U.S. Army Corps of Engineers testing has determined that special blast curtains are no more effective against fragmentation than the less expensive heavy curtains available at local stores. When using heavy curtains instead of blast curtains, they must be kept closed in order for them to be effective. Policy should require that they be closed during appropriate threat conditions. In other cases, it may be necessary to disable traverse curtain rods. In addition to mitigating the effects of blasts, curtains obscure the occupants from snipers.

Blast Film

Blast film can be used to protect glass windows of occupied rooms, unless the window is glazed with some form of shatterproof glazing. This includes windows located on the

exterior of a building and in areas adjacent to parking lots, roadways, or other locations where sizable explosive devices could be located. A bomb detonation outside of the building can create a blast force that would shatter window glass, causing it to be blown into the room. The film would bind glass fragments, minimizing the danger of injury from glass shards. Blast film and certified installers are available through the General Services Administration (GSA). Blast film should be used in lieu of curtains in areas where it is undesirable to keep curtains closed or it is doubtful that the curtains will be kept closed. In addition to mitigating the effects of blasts, tinted blast film can be used to obscure the occupants.

Reinforced Glazing

Where the threat of an explosive device on the exterior of the building exists, replacement of window glass with polycarbonate or thermo-tempered glass may be advisable. Such glazing resists fragmentation and provides a heightened level of protection from bomb blasts. Tinted glazing provides obscuration and protection from a sniper. Further, bullet-proof glazing such as Lexguard ™ can protect even better against a sniper threat.

Window Obscuration

When the terrorist threat is from a sniper, obscuring the potential victim can defeat the threat. Some countermeasures for protecting windows from blasts are also applicable; blast film can be tinted, and curtains, if kept closed, are effective. One-way glass or tinted glazing can be used. Vegetative screening can provide an aesthetically pleasing option if the plantings are coniferous.

PART IV: ENCYCLOPEDIA

Chapter 7: Security Resources

Introduction

This chapter presents security resources available to managers for consideration, such as canine teams and security officers. These security tools are typically not necessary at all facilities, but may become a desired option during higher threat levels.

Augmentation

Prior to an emergency, facility management should evaluate the need to employ additional security officers during increased threat conditions. Such augmentation can be accomplished through existing security officers' contracts or through local security companies on a temporary basis if a security force is not regularly employed. During periods of increased security, facility managers should consider utilizing full-time company employees to augment security posts in an observation or support role.

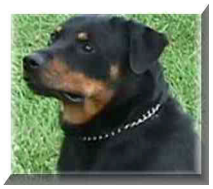
Managers should select enough security officers to fulfill their requirements and plan to increase the number of officers should the need arise. They should also prepare written procedures, which may include the use of dogs for routine or contingency operations.

Canines

Canines are an excellent deterrent and offer superb reliability. Dogs are extremely effective in inspecting large areas, locating contraband, and controlling individuals. Explosive detection, patrol, or guard dogs may be used for deterrence, random screening inspections, or detection, especially at frequently unmanned sites.

- Consider using explosive detection dogs, search dogs, or patrol dogs in appropriate threat conditions.
- Evaluate the need to establish routine or contingency contracts for a specific type of security dog support.
- Incorporate the use of dogs (routine or contingency) into security and emergency plans as well as post orders.
- Ensure that plans include adequate resources for sustaining dog support for appropriate time periods based on dog availability and periods of effectiveness.
- Ensure that organizational policies on privacy, personnel, workspaces, and personal property allow for the use of security dogs under various circumstances.

Patrol Dogs



A patrol dog is an animal that has been trained to inspect large areas and can be used in populated areas like stores, schools, or housing developments.

Explosive Detector Dogs (Bomb Dogs)

A patrol dog may be trained to detect explosives. During increased threat levels, these dogs may be used at entry points to inspect equipment, vehicles, and objects brought onto the site.

Sentry Dogs

Sentry dogs are trained to secure a specific area where they are left to roam or secured to a long (360 foot or larger) tether. They serve as a deterrent but are limited in where they may be used because they are usually identified as attack dogs.

Narcotic Detector Dogs

These dogs are trained to detect different types of drugs. During increased threats, drug dogs may be used to help control individuals entering or leaving a location.

Entrances

During periods of increased threat levels, facility managers should enhance security procedures for access into critical facilities by stationing security officers at entrance gates to the site.

Security officers should have specific duties that include ensuring that all vehicle occupants have company-issued ID cards and/or vehicles display distinctive identification issued by facility management, etc.

Security officers should also be equipped with necessary tools including radio communications, access lists, hand-held portable lights, etc.

The use of supplemental lighting devices to adequately illuminate areas (depending on criticality) may also be warranted.

Vehicle occupants or foot pedestrians who cannot furnish identification to the site should be directed to a remote area of the facility for further processing.

Patrols

During periods of increased threat levels security officers should conduct additional interior and exterior roving patrols. Depending on the facility size, exterior patrols should consist of both foot and mobile patrols.

Surface to Air Missiles (SAM)

Most terrorist organizations possess shoulder-fired missiles capable of downing an aircraft. Where applicable, identify arrival/departure paths for the facility/complex. These paths may include flight paths for aircraft (fixed wing or helicopter), ground, or water transport paths. Establish a mechanism to ensure these routes can be secured or assessed during periods of increased threat. Develop alternative plans for emergency evacuation routes and first responder entry in the event primary routes are rendered impassable by nature (e.g., storm) or by intent.

Local response forces and law enforcement should continually patrol the areas around airports or areas where a missile may be fired during heightened states of alert. In very high

threat conditions, employees and the general public should be asked to remain alert and report suspicious activities to help counter this threat.

Surveillance

During increased threat levels, security officers assigned to critical infrastructure or operations should increase their awareness levels to identify potential security threats. Such threats should be reported immediately to local law enforcement agencies.

PART IV: ENCYCLOPEDIA

Chapter 8: Special Venues

Introduction

As a state that annually hosts millions of international and domestic visitors attracted to its beaches, resorts, golf courses, theme parks, and university and professional sports teams, and as a destination for major conventions and trade shows, Florida must secure its many public venues. Whether considering the level of security for the Super Bowl in Tampa Bay in 2004 or the Lake County Fair, Florida faces considerable challenges in providing safe and enjoyable events to the public, while maintaining the necessary level of security in today's threat environment.

For the purposes of this chapter, public venues are defined as convention centers, stadiums (both indoor and outdoor), arenas, and halls, as well as large outdoor gathering areas hosting a concert, sporting event, show, or fair. Measures and recommendations are provided for each type of venue arrayed against the risk rating for that venue and measures to take for Elevated, High, and Severe threat levels.

Basic Planning Concept

Regardless of the venue, some basic planning concepts should be considered prior to the event. Because most of the venues in Florida will be very experienced in planning for an event, these steps may already be a familiar and integral part of your process, but will be presented to ensure that all issues are covered.

Form Your Planning Team

Regardless of the physical nature of the venue (open outdoor, outdoor in tents, indoor convention, or stadium, for example) an event planning team is needed to consider security and other event issues such as ticket processing, food service and vendor needs, preparation of display spaces or the playing field, and patron services such as first aid, missing children, and lost and found.

The event planning team should consist of:

- *Venue authority or operator* (could be a private organization such as a professional sports team owner, university, county, state, or special district)
- *Representative of the promoter, entertainer, sports team, or convention host* (Republican National Committee, Florida State Democratic Party, National Association of Manufacturers, the Tampa Bay Devil Rays, or the Southern Baptist Convention, for example)
- *Law enforcement:* Florida Highway Patrol, county sheriff or local police department supported by the FDLE Regional Domestic Security Task Force, the FBI, and U.S. Secret Service (USSS) as necessary
- *Venue director of security* or contract security manager
- *Fire department, rescue, and EMS*
- *The American Red Cross* (for large-scale first aid operations)
- *Chief usher*
- *Vendor* representatives
- *Parking control official*
- *Venue engineering technicians* (HVAC, power production, mechanical)

- *USSS* (if event is a national security event or is hosting the President, Vice President, or a USSS protectee)
- *Union representative* (if venue workers and support staff—electricians, gaffers, grips, actors, actresses—are in a labor organization)
- *Loading dock boss* (for major convention shows requiring delivery of display sets and items)

The team for major events should form, ideally, 1 year before the planned event and meet as often as necessary to plan for the event and consider these aspects:

- Purpose of event:
  - Political convention with USSS involvement
  - Major security event (Olympic venue, Pan Am Goodwill games, World Soccer Cup, and other international events) that may require USSS coordination
  - Major nonpolitical party national convention (but with potential for controversy, such as IMF, World Bank, right to life, pro-choice, labor union convention, or a religious gathering)
  - Major trade show event (consumer electronics, firearms show, high-tech research, military and space hardware) with high-value equipment
  - Concert (country music, R&B, rap, pop, jazz, new age) with a group that may or may not be controversial
  - Festival (Shakespeare, Renaissance Faire, folk, or new age festival)
  - Professional and NCAA sports (consider rival teams and fans, or high-profile, controversial sports events)
- Anticipate the threat environment
  - Conduct a preliminary threat assessment
  - Use Elevated or Yellow as Florida's minimum
  - Determine if risk will be higher based on previous similar venues
    - Obtain security environment from the last venue host (San Diego for Super Bowl XXXVII, for example, Salt Lake City for the 2002 Winter Olympics, or a previous national political convention city)
    - Obtain the security "playbook" from those hosts
- Plan for the anticipated threat environment.
  - Do this at least 6 months out
    - Update each month
    - Finalize 1 month prior to the event
    - Do not reduce once all security is set in place
- Write the security plan.
  - Assign responsibilities for:
    - Local threat assessment (FDLE, Florida Highway Patrol [FHP], FBI/USSS, sheriff, local law enforcement, and venue director of security
    - A survey of surrounding areas of the venue for potential vulnerabilities
    - Layering of security from innermost area (the highest level) to venue boundary or property line (the lowest level)
    - Security for the actors, entertainers, sports figures, distinguished visitors, candidates, etc., with appropriate "Protective Service Operations," (i.e., bodyguards)
    - Determining any special needs for the event:
      - Policy on hand-carried items into the venue

- Parking control
- Patron screening and processing
- Control and processing of vendor goods, displays, DVs
- First aid and EMS tents
- Lost children (for family-oriented events)
- Response cells (SWAT, countersurveillance on air and ground)
- Fire and rescue standby
- Assign responsibilities for these special needs
  - Obtain funding sources for these special services, police, and security overtime
  - Form a threat working group to meet at least monthly, then weekly 60 days prior to the event and daily 1 week prior
  - Form the event operations group or team to meet at least monthly, then weekly 60 days prior to the event and daily 1 week prior
  - Determine who will receive background checks

- Finalize security plans and procedures 1 month prior to the event.
  - Assess crowd size and potential for demonstrators outside the venue
    - The promoter can assist by using advance or will call ticket sales
    - Convention planners can tell you the attendance figures based on registration
    - Previous attendance such as sports events
    - Attendance rates in prior cities (such as rock group tours)
    - Police calls for service and response by demonstrators in prior cities
    - Experiences in your city or location with similar venue
    - Check Web sites for planned demonstrations at the event
- Publicize the security requirements, such as no hand-carried items, or if permitted water and necessary items (diapers, food, etc.) into the venue.
- Establish final parking plan and ensure sufficient buses and shuttles to move patrons from parking lots to the venue, considering the needs of the disabled. Remember that generally for sports events and concerts everyone arrives over a span of time, but everyone wants to leave at the same time.
- Issue credentials for essential venue support personnel.
  - Consult USSS on credentials needed for close-in access to their operations.
- Establish and agree on ground rules for bringing in merchandise, displays, sets, and other items for the venue such as delivery screening and working with the gaffers, grips, drivers (of the motorcade, limousines, show buses, semi trucks) and other support requirements.
- Run through the event with all police, federal agencies, security, and venue sponsor and discuss emergency evacuation, communications, chain of command, responsibilities, and support requirements.

One Week Prior To Event Start

- Set up full-time command center at least 1 week prior to the event and check all telephones, radios, CCTVs, and security systems.
- Test all patron-screening security equipment and conduct dry runs on each other to determine throughput of patrons (USSS will manage for events in which the President, Vice President, or a USSS protectee is to appear), adjusting as necessary.

- Dry-run response, tactics, and surveillance, and run checks of the venue security system.
- Issue credentials for temporary event workers.

One Day Prior To Event Start

- Thoroughly patrol the venue at least 24 hours prior to the start. Once a sweep is done of an area and it is "sanitized," it needs constant surveillance (security) over that portion of the venue or needs re-sweeping.
- Ensure that everyone is in place, systems are checked, there is backup power, everyone knows what everyone else is doing, what numbers to call, presence of police, and security staff responsibilities.

EXHIBIT 1 TO SPECIAL VENUES

Indoor Venues

1. The following security measures are the recommended best practices to be considered for special events held in civic centers/conference centers/performing arts centers/ auditoriums throughout the state of Florida.

- *Establish an integrated security plan.* This is key to a successful security program. The plan should address all security requirements, including contingency events, and should be coordinated with all agencies involved in the event. The plan should outline responsibilities for each element or department participating in each event and be used as a road map for how the operation will be conducted. The integrated plan should be composed of "living" documents and adjusted periodically to fit the needs of the various departments as well as adjust to developing situations. Comprehensive in nature, this is the one-stop-shop for telling all agencies the "who-what-when-where-and-how" of the particular event. Once developed, these plans need to be shared and exercised. Planning must address situations from normal to high threat conditions. Conducting after-action meetings shortly after each event should be the initial stages of planning for follow-on events.
- *Establish an SCC.* SCCs are the hub of every event. The need for SCCs should be identified early in the planning process and details such as location, makeup, and command and control should be specified and rehearsed. The location can be central to the special event or geographically separate. Also consider the establishment of alternative control center(s) with redundant system capabilities.
- *Provide positive access control for each event.* Access control should be initiated well away from the main event—beginning, for example, at the parking area or entrance to the parking area. Parking plans should take into consideration easy entry and exit of fans and emergency response vehicles. Parking attendants, if used, should be familiar with current threat conditions and trained on recognizing suspicious activities. As proximity to the main event decreases, more positive measures should be employed to ensure suspicious activities are reduced, observed, and countered by trained personnel. For large events, trained security personnel can mingle outside the gates to observe suspicious activities and provide a visible deterrent to criminal activities. At the entrance gate, trained staff should carefully scrutinize tickets that may be colored or otherwise coded for authenticity for entry to that specific event or specific area of the event. All access controllers/parking attendants should be easily identified by color-coordinated shirts, vests, and/or jackets.

- *Comply with the National Fire Protection Association's Life Safety Code Festival Seating Standard.* Coordinate with local life safety organizations to ensure compliance with all appropriate codes. This is especially important when large crowds gather in closed spaces like civic centers, etc., where non-static seating is arranged.
- *Conduct background checks of event staff.* Background checks should form the foundation for hiring the event staff. These checks should be conducted through all the local credit and law enforcement agencies. Follow up on all questionable information with the prospective hire. Start these at least 6 months prior for staff working close in to the performers, athletes, political figures, and other high-profile persons.

- *Install motion/intrusion detectors at critical points.* Motion detectors can be used to augment security forces after hours or in areas of little traffic during normal operating hours. Intrusion detectors are effective on doors and windows. Alarms should annunciate at a control center capable of alerting on-duty security personnel. Because of cost and the permanent nature of these detectors, consideration should be made in the early stages of planning. These devices are especially effective when used in conjunction with CCTVs to facilitate immediate remote evaluation of the alarm. As with all alarm systems, they are only as effective as the capability to immediately assess the alarm and respond with security personnel.
- *Conduct security training for security augmentation force.* Ensure that adequate training for security awareness and security procedures is conducted for all persons augmenting the security force. Tailor and focus training to the specific areas that these individuals will be working. For example, ticket takers and crowd controllers may need to complete different training depending on the event and/or position. Pairing augmentation personnel with regular security force members reinforces training and enhances continuity. Ensure your event security staff is trained in using metal detection wands and other equipment.
- *Use signs effectively.* Signs are an effective means to inform attendees of regulatory requirements, entry and exit routes (including emergency evacuation routes, if different), controlled or off-limits areas, and the location of information, security, and human services.
- *Establish crowd density reduction measures in front of main stage.* For the protection of both fans and the performer(s), crowd density reduction should be considered and implemented as individuals get closer to the main stage or event. For example, extra measures should be in place to prevent crowds from tightly gathering near the stage at a rock concert. This can be accomplished in a variety of ways and should always be coordinated with the performers' planning team prior to the event. If barriers are used, ensure they can "break way" without causing the crowd to bunch up and suffocate those in the first rows.
- *Consider banning certain activities like crowd surfing and moshing.* Safety of the fans and performers must be of paramount consideration when planning for and executing events. These activities often start as innocent fun, but can quickly become unruly and dangerous. For events that attract these types of activities, such as rock concerts, notices should be displayed at entrances and announcements made that warn spectators to avoid this type of behavior. Also, consider posting additional security around the main stage and other key areas. Have a plan to "receive" a surfer and remove them from the crowd out a side entrance. Use two to four security personnel for this task.
- *Limit parking near event.* Create standoff zones directly adjacent to the facility through effective parking plans.

2. The following identifies additional security measures (best practices) to be considered for implementation dependent upon increased identified risks, vulnerabilities, and threat level for the event.

- *Use CCTV at entry points, including loading docks.* Install CCTV cameras at vulnerable points, especially entry points, with monitors at the control center. Loading docks should also be equipped with CCTV cameras. These units may be static or rotating (pan and tilt). Consider installing videotaping machines. Videotaping should be continuous and recorded tapes stored for a specific period of time in order to be reviewed, if necessary.
- *Advertise security awareness with ticketing medium.* Consider advertising security awareness information on tickets. This can range from awareness of the national threat level system

to emergency actions. Augment this information with brochures at the gates, informational flyers and posters throughout the facility, and special audio and video announcement messages on public address and viewing systems.

- *Use metal detectors at entry points.* Consider using metal detectors at facility event entry points. Due to cost, metal detectors should be considered early in the planning process. If funding does not permit the purchase of permanent detectors, consider borrowing from area law enforcement agencies, other event locations not currently in operation, leasing the machines during higher threat conditions or, as an alternative, consider hand wands for use by augmentation forces at the entry points. If metal detectors are used, ensure operators are properly trained.
- *Use Pat Downs.* Consider using pat downs in conjunction with metal detectors or in place of metal detectors when detectors are not available. Use male and female augmenters, as appropriate, to conduct the pat downs, and ensure that they are properly trained. If suspicious items are discovered, detain the individual and alert the security or law enforcement officials on site. Calculate the number of tickets sold, allow at least 10 seconds per person for a quick pat down and add about 30 seconds for a quick handheld item check (check for weapons and explosives, not for makeup and combs) and then figure how many screeners are needed to keep the lines moving and avoid backups. Backups annoy patrons and can lead to impatience and some physical altercations.
- *Use explosive detectors/explosive containers.* Consider using explosive detection devices, including explosive-detection-trained canines for extremely high security venues. These devices not only add a level of security to prevent the introduction of explosives and firearms, but also reassure attendees of a safe environment. The ability of trained canines to assist in other law enforcement and crowd control functions is an added benefit. With or without detection devices, explosive blast containers should be strategically located throughout the facility to allow the segregation of suspicious items.
- *Position security at loading docks.* A tremendous amount of activity takes place at loading docks. Consider placing security officers or augmentation forces at loading docks when shipments arrive or depart. Ensure officers are trained on awareness procedures and are equipped with communications equipment to sound the alarm. Consider inspecting vehicles, screening deliveries, and placing CCTV cameras at the loading docks.
- *Increase parking limitations near event.* During periods of higher risk and/or threat, consider thinning out or eliminating spectator parking in areas near or adjacent to the special event. The parking areas for large vehicles, including vendor vehicles, should be restricted to areas of even greater distance from the event.

EXHIBIT 2 TO SPECIAL VENUES

Open Venues

1. The following security measures are the recommended best practices to be considered for special events held at open or outdoor venues throughout the State of Florida. Open Venues include street festivals, rallies, fairs, concerts, and other activities not confined to a building or stadium/arena-type facility.

- *Establish an integrated security plan.* This is key to a successful security program. The plan should address all security requirements, including contingency events and should be coordinated with all agencies involved in the event. The security plan outlines responsibilities for each element or department participating in each event and be used as a road map for how the operation will be conducted. The integrated security plan should be composed of "living" documents and adjusted periodically to fit the needs of the various departments and to adjust to developing situations. Comprehensive in nature, this is the one-stop-shop for telling all agencies "the who-what-when-where-and-how" of the particular event. Once developed, these plans need to be shared and exercised. Planning must address situations from normal to high threat conditions. Conducting after-action meetings shortly after each event should be the initial stages of planning for follow-on events.
- *Consider planning activities prior to the event.* Consider the following planning activities that should be completed and/or conducted prior to the event:
  - *Include a walk-through prior to the event.* Security for events, even those on a recurring basis, should include a walk-through several days before the scheduled event. The walk-through provides special event managers with first-hand knowledge of the layout, entry and exit routes, and any changes to the layout since the event last occurred. It also gives event managers a ground-level view of parking areas and other access points. Have your event security chiefs, ushers, and others accompany the manager on the walk-through.
  - *Ensure continuity of planning staff.* Planning should involve a measure of continuity. Written plans are the foundation of the planning process and should be augmented by staff members with experience in the event. The experienced staff member provides look-back continuity and can add flexibility to the written plans.
  - *Coordinate with local medical staff and facilities.* Medical personnel are a key element on the team. It is important to keep them abreast of developing situations in case their services are needed. Consider positioning a representative from the local medical facility in the command post or, at minimum, provide them with a radio for easy contact. They must be well versed on emergency entry and exit routes. They should also be kept advised of any changing threats in order to be prepared to deal with various types, severity, and numbers of injuries.
  - *Plan with highway department to ensure access/departure routes are open.* Traffic routes into and out of the special venue site help ensure orderly movement and should be planned. Consider establishing alternative routes for use during emergency situations—either natural or man-made. These routes must be coordinated with local transportation departments who have responsibility for the roadways. Their cooperation may be needed to re-route other traffic if the situation warrants. This planning must start when developing initial special event plans.
  - *Establish interjurisdictional agreements between law enforcement and security forces.* If, during the event, there will be police and security forces from more than one agency or department, it is critical that written agreements are made in advance concerning

jurisdictional issues, arming policies, and event responsibilities. Coordination should be done in the initial planning phases and contained in the basic security plan. Jurisdiction issues must be spelled out and understood by all security personnel. For example, an event may have federal, state, highway patrol/state police/department of public safety, municipal and county law enforcement agencies in addition to contract security forces, with each providing certain elements of security at the same event.

- *Conduct background checks of event staff.* Background checks should form the foundation for hiring the event staff. These checks should be conducted through all the local credit and law enforcement agencies. Follow up on all questionable information with the prospective hire. Start these at least 6 months prior for staff working close in to the performer, athletes, political figures, and other high profile persons.
- *Conduct security training for security augmentation force.* Ensure that adequate training for security awareness and security procedures is conducted for all persons augmenting to the security force. Tailor and focus training to the specific areas that these individuals will be working. For example, ticket takers and crowd controllers may need to complete different training depending on the event and/or position. Pairing augmentation personnel with regular security force members reinforces training and enhances continuity.
- *Use signs effectively.* Signs are an effective means to inform attendees of regulatory requirements, entry and exit routes (including emergency evacuation routes, if different), controlled or off-limits areas, and the location of information, security, and human services.
- *Establish mobile control center with redundant capability.* Control centers are the hub of every event. The need for control centers should be identified early in the planning process and details such as location, makeup, and command and control should be specified and rehearsed. Position mobile command centers to allow maximum flexibility in controlling event security. Considerations for special event managers include, but should not be limited to, accessibility of supervisors and other response forces from the control center and interoperability of the communications equipment.
- *Provide clearly identified entry and exit routes for first responders.* Emergency response teams are of little value if they cannot reach the scene or evacuate people from the scene efficiently and effectively. Planning must include the ability of first responders to reach the scene quickly and to exit safely and expeditiously. Ensure that crowd control and security forces are familiar with the routes and can quickly clear the way when and as necessary.
- *Use rented golf carts for response teams.* Crowded and/or cramped special venues may not be practical for regular patrol vehicles or for having security forces on foot. An efficient compromise is to use golf cart-type vehicles. These vehicles can carry security forces, medical personnel, and other first responders quickly to a scene without being obtrusive. These vehicles should be conspicuously marked to ensure safe response and a readily identifiable presence for citizens seeking assistance or attempting to notify security forces of suspicious or criminal activity. Mounted horse patrols are also an excellent means of providing these capabilities with the ability to go places vehicles cannot go as well as to assist in crowd control.
- *Use outlying parking areas and shuttle patrons to event.* Consider creating standoff zones by moving parking areas away from the special venue to outlying areas. This reduces the opportunity for terrorists to position explosive-laden vehicles close to the venue. It also provides a greater opportunity for security personnel to observe individuals who may be carrying explosives and/or other dangerous articles. Consider providing shuttle service to event attendees who are required to park in outlying areas. Arrange for rental or use

of public transit buses or private motor coaches. Be prepared to have several special-needs vans or surreys (minibus) available for disabled patrons.

- *Ensure sanitation operations and trash removal are a continuous priority.* Many outdoor events have erupted in chaos because sanitation, portable toilets, and trash removal needs were not satisfied in a timely fashion. Involve the local sanitation contractor in the planning process at the beginning stages of planning and ensure schedules are maintained throughout the event.
- *Defer press questions and comments to special event media spokesperson.* Establish a media spokesperson during the planning phase. Make it clear to the special event staff that all media inquiries should be directed to the media spokesperson. Allowing members of the security staff to estimate crowd numbers has tarnished some large events in the past. While seemingly an innocent issue, event organizers may become dissatisfied if their "desired" numbers do not match the estimates of the event security staff. The mission of the security staff is to provide security and safety for the spectators, not to be a public relations interface, and this should be emphasized and enforced at all times.
- *Use the same communications frequencies for command and control.* Set aside one frequency for use by all on-site special event elements to monitor event activities. This frequency should be identified in writing during the planning stages and given to police forces, medical teams, fire units, and other emergency response units. Ideally there should be separate frequencies for other intrafunction communication.
- *Color code responding forces for easy recognition.* Consider using different color schemes for different emergency services elements (i.e., security force in blue, emergency medical technicians (EMT) in maroon, safety in yellow, etc.). This should be spelled out in detail in the security plan and coordinated and agreed upon by all agencies. This gives responders, spectators, and managers visual access to the location of different units. Issue t-shirts and/or windbreakers (or jackets or parkas) or hats that read:
  - Event Security Staff
  - Police
  - EMS/Medical Staff
  - Event Assistance and Ushers
  - Parking Warden
  - Traffic Warden

2. The following identifies additional security measures (best practices) to be considered for implementation depending on increased identified risks, vulnerabilities, and threat level for the special event.

- *Advertise security awareness with ticketing medium.* Consider advertising security awareness information on tickets as well as on the Web site. This can range from awareness of the national threat level system to emergency actions. Augment this information with brochures at the gates, informational flyers and posters throughout the special event facility, and special audio and video messages on public address and viewing systems.
- *Use strategic portable lighting.* Adequate lighting is a very effective security tool. Portable lighting adds flexibility by allowing special event managers to adjust to specific situations and conditions. During higher threat conditions, use portable lighting to illuminate avenues of approach and remote parking areas, and to augment gaps in permanent lighting.
- *Position CCTV cameras on top of mobile command post.* CCTV cameras can add significantly to the decision-making process of special event security managers. They enable them to see situations develop. They also reduce the need for security officers in non-critical areas

that may be more efficiently used elsewhere. Consider using pan and tilt, rotating, and zoom CCTV cameras.

— The 2003 Super Bowl held in San Diego's Qualcomm Stadium had an intelligent CCTV system consisting of 39 cameras that permitted a 360-degree view of the venue.

- *Position TV sets in command post/command center.* Sometimes the fastest way to learn of developing events is to gather information from local news stations. Consider putting TVs in the command center. This will allow for the monitoring of local and national news, which may be important for up-to-date situation developments or different perspectives of local events and situations.
- *Use random observers.* Observers equipped with observation devices and appropriate communications equipment, and positioned on rooftops, towers, and/or higher terrain, can identify and provide real-time input to the command post/command center regarding developing situations. Using observation devices capable of all-weather usage also enhances flexibility.
- *Use helicopters.* Helicopters provide a flexible response capability to large areas, are unencumbered by on-ground obstacles, and provide a flexible and unique vantage point for security personnel. They can also be used as an alternative command and control platform for security forces. They can be used in situations from supporting traffic operations to managing disaster scenes. Helicopters provide on-scene commanders a view of the entire area and can help maneuver forces during crisis situations and, if needed, can be used for medical evacuation purposes. When equipped with searchlights and or thermal imaging devices, they can be invaluable during periods of limited visibility. Additionally, a helicopter provides a powerful visible and audible deterrent at significant distances. Another tactic is that if the event is sponsored by a company that rents the Goodyear ™ blimp or other airship, station a security expert in the cabin to act as an additional observer.
- *Consider use of temporary flight restrictions over event area.* One way to minimize the risk of aerial attacks is to restrict the airspace over particular events, especially during periods of increased threats. Coordination with local FAA officials should start at the beginning of the planning process. Depending on the event, an exception may be granted to members of the media as well as law enforcement helicopters and small planes.
- *Use undercover/intelligence agents to gather pre-event information.* Establish contact with local, state, and federal law enforcement agencies early in the planning phase to determine if they have any threat information that may affect the special event. This information can be critical in determining if additional security measures or precautions are necessary and can head off problems before they occur.
- *Use explosive detectors/explosive containers.* Consider using explosive detection devices, including explosive-detection-trained canines. These devices not only add an additional level of security to prevent the introduction of explosives and firearms, but also reassure attendees of a safe environment. The ability of trained canines to assist in other law enforcement and crowd control functions is an added benefit. With or without detection devices, explosive blast containers should be strategically located throughout the facility to allow the segregation of suspicious items.

Exhibit 3 to Special Venues

Stadiums/Arena Venues

1. The following security measures are the recommended best practices to be considered for special events held at stadiums/arenas throughout the state of Florida. This includes facilities such as football stadiums, baseball stadiums, and racetracks (i.e., Daytona 500 racetrack).

- *Establish an integrated security plan.* This is key to a successful security program. The plan should address all security requirements, including contingency events, and should be coordinated with all agencies involved in the event. The security plans outlines responsibilities for each element or department participating in each event and be used as a road map for how the operation will be conducted. The integrated security plan should be composed of "living" documents and adjusted periodically to fit the needs of the various departments and to adjust to developing situations. Comprehensive in nature, this is the one-stop-shop for telling all agencies the "who-what-when-where-and-how" of the particular event. Once developed, these plans need to be shared and exercised. Planning must address situations from normal to high threat conditions. Conducting after-action meetings shortly after each event should be the initial stages of planning for follow-on events.
- *Consider planning activities prior to the event.* Consider the following planning activities that should be completed and/or conducted prior to the event:
  - *Include a walk-through prior to the event.* Security for special events, even those on a recurring basis, should include a walk-through several days before the scheduled event. This provides special event managers with first-hand knowledge of the layout, entry and exit routes, and changes to the layout since the event last occurred. It also gives special event managers a ground-level view of parking areas and other access points.
  - *Ensure continuity of planning staff.* Planning should involve a measure of continuity. Written plans are the foundation of the planning process and should be augmented by staff members with experience in the event. The experienced staff member provides a look-back continuity and is able to add flexibility to the written plans. Have your event security chiefs, ushers, and others accompany the manager on the walk-through.
  - *Coordinate with local medical staff and facilities.* Medical personnel are a key element of the team. It is important to keep them abreast of developing situations in case their services are needed. Consider positioning a representative from the local medical facility in the command post or, at a minimum, provide them with a radio for easy contact. They must be well versed on the emergency entry and exit routes. They should also be kept advised of any changing threats in order to be prepared to deal with various types, severity, and numbers of injuries.
  - *Plan with highway department to ensure access/departure routes are open.* Traffic routes into and out of the special venue site help ensure orderly movement and should be planned. Consider establishing alternative routes for use during emergency situations—either natural or man-made. These routes must be coordinated with local transportation departments who have responsibility for the roadways. Their cooperation may be needed to re-route other traffic if the situation warrants. This planning must start when developing initial event plans.
- *Develop close coordination with supporting agencies.* The success of an event depends largely on each agency working together. A viable, well-coordinated security plan allows for the

smooth interaction between security, fire, medical, and media personnel. Planning should include events during normal event operations and during situations of heightened security operations.

- *Ensure interoperability of communications systems.* It is critical for first responders to communicate effectively and efficiently with other forces. This can be accomplished either by using radios from one department (such as the police department) for all first responders, or by allowing all responders to tune in to one frequency. This should be considered and detailed in the security plan.
- *Establish interjurisdictional agreements between law enforcement and security forces.* If, during the event, there will be security forces from more than one agency or department, it is critical that agreements be made in advance concerning jurisdictional issues, arming policies, and event responsibilities. This should be done in the initial planning phases and contained in the basic security plan. Jurisdiction issues must be spelled out and understood by all security personnel. For example, an event may have federal, state, highway patrol, municipal, and county law enforcement agencies in addition to contract security forces, with each providing certain elements of security within the same event.
- *Establish an SCC.* SCCs are the hub of every event. The need for SCCs should be identified early in the planning process and details such as location, makeup, and command and control should be specified and rehearsed. The location can be central to the event or geographically separate. Also consider the establishment of alternative control center(s) with redundant system capabilities.
- *Conduct background checks of event staff.* Background checks should form the foundation for hiring the event staff. These checks should be conducted through all the local credit and law enforcement agencies. Follow up on all questionable information with the prospective hire. Start these at least 6 months prior for staff working close in to the performers, athletes, political figures, and other high profile persons.
- *Conduct security training for security augmentation force.* Ensure adequate training for security awareness and security procedures is conducted for all persons augmenting the security force. Tailor and focus training to the specific areas that these individuals will be working. For example, ticket takers and crowd controllers may need to complete different training depending on the event and/or position. Pairing augmentation personnel with regular security force members reinforces training and enhances continuity.
- *Use signs effectively.* Signs are an effective means to inform attendees of regulatory requirements, entry and exit routes (including emergency evacuation routes, if different), controlled or off-limits areas, and the location of information, security, and human services.
- *Provide clearly identified entry and exit routes for first responders.* Emergency response teams are of little value if they cannot reach the scene or evacuate individuals from the scene efficiently and effectively. Planning must include the ability of first responders to reach the scene quickly and to exit safely and expeditiously. Ensure that crowd control and security forces are familiar with the routes and can quickly clear the way when and as necessary.
- *Use outlying parking areas and shuttle spectators to event.* Consider creating standoff zones by moving parking areas away from the special venue to outlying areas. This reduces the opportunity for terrorists to position explosive-laden vehicles close to the venue. It also provides a greater opportunity for security personnel to observe individuals who may be carrying explosives and/or other dangerous articles. Consider providing shuttle service to event attendees who are required to park in outlying areas. Arrange for rental or use

of public transit buses or private motor coaches. Be prepared to have several special-needs vans or surreys (minibus) available for disabled patrons.

- *Ensure sanitation operations and trash removal are a continuous priority.* Many outdoor events have erupted in chaos because sanitation, portable toilets and trash removal needs were not satisfied in a timely fashion. Involve the local sanitation contractor in the planning process at the beginning stages of planning and ensure schedules are maintained throughout the event.
- *Defer press comments to special event media spokesperson.* Establish a media spokesperson during the planning phase. Make it clear to the special event staff that all media inquires should be directed to the media spokesperson. Allowing members of the security staff to estimate crowd numbers has tarnished some large events in the past. While seemingly an innocent issue, event organizers may become dissatisfied if their "desired" numbers do not match the estimates of the event security staff. The mission of the security staff is to provide security and safety for the spectators, not to be a public relations interface, and this should be emphasized and enforced at all times.
- *Use the same communications frequencies for command and control.* Set aside one frequency for use by all on-site elements to monitor event activities. This frequency should be identified in writing during the planning stages and given to police forces, medical teams, fire units, and other emergency response units. Ideally there should be separate frequencies for other intrafunction communication.
- *Consider CCTV cameras at access control points and other key points.* Consider using CCTV cameras to monitor access control points and other key locations around the special venue. Cameras can help security managers view situations, can help reduce manpower (unless the threat dictates otherwise), and can help document situations requiring legal action. Consider using temporary camera setups for areas not used on a recurring basis
- *Color code responding forces for easy recognition.* Consider using different color schemes for different emergency services elements (i.e., security force in blue; EMTs in maroon, and safety in yellow, etc.). This should be spelled out in detail in the security plan and coordinated/agreed upon by all agencies. This gives responders, spectators, and managers visual access to the location of different units leave t-shirts and/or windbreakers (or jackets or parkas) or hats that read:
  - Event Security Staff
  - Police
  - EMS/Medical Staff
  - Event Assistance and Ushers
  - Parking Warden
  - Traffic Warden
- *Use teams composed of multiple agencies.* Consider posting members from different agencies together on the same patrol. This would facilitate communications between agencies and serve to eliminate jurisdictional problems if and when they occur.
- *Use public affairs to help publicize security awareness.* Public affairs officials are key members of the event staff. Planning should include the media to publicize security awareness information for spectators before and during the event. This can take the form of newspaper ads, radio and TV spots, and flyers and posters throughout the city and event location.
- *Exercise vendor control.* A separate access point should be established for vendors. Consider issuing picture ID cards to vendors that come routinely. Issue generic vendor passes to vendors who make few or infrequent visits. Ensure these are backed up by a visitor

control log and maintained after each event. Vendor access control must be set up several days prior to the event to ensure proper security.

- *Use positive access control (i.e., turnstiles).* Set up turnstiles or other devices that ensure only authorized personnel enter the special venue. This is critical to a sound security program. The security force at access points should be augmented with CCTV cameras, as they provide a valuable method to identify personnel coming through the access checkpoints. Use barriers or other means to channel the public as they approach access control points. This precludes a rush of people at the access point/turnstiles and is critical to maintaining positive access control. Consider positioning security officers outside the access points for crowd control. If available, assign police canine teams at the access points as a deterrent.
- *Assign parking and issue windshield placards for special parking areas.* For parking areas close to the event or in areas designated as special parking areas, develop parking permits or placards and issue them to persons authorized to park in those areas. Include illustrations of the parking permits in the security plan and coordinate among the various agencies. It also is recommended that a document or book be provided to parking supervisors with examples of these passes and the names of persons authorized to use them.
- *Maximize use of natural and man-made barriers.* Use creative design patterns to maximize the use of natural and man-made barriers to create standoff zones. This is especially useful in the planning stages of new stadiums and structures. Natural streams, ditches or culverts, earthen berms, etc., can be used to create standoff zones without appearing obtrusive.
- *Pre-event security sweep.* Prior to opening the venue to the public, a thorough patrol sweep should be conducted of the entire controlled special venue as well as outer clear zones. Sufficient time must be allowed to ensure a thorough check of the venue. Consider employing explosive-detecting dog teams, if available, as part of the pre-event sweep. Also, consider having the dog teams available during the event as a deterrent.

2. The following identifies additional security measures (best practices) to be considered for implementation dependent upon increased identified risks, vulnerabilities and threat level for the event.

- *Provide basic antiterrorism education and awareness to security staff.* Ensure that security and site personnel receive basic antiterrorism education and awareness. This should be an ongoing effort conducted on a regular basis. Training should include but not be limited to awareness of the national threat warning system; awareness of local threats including the proximity of international or domestic terrorist groups to the site; and alarm/response procedures. See sample training plan in the Appendix.
- *Provide security education and awareness to the public.* Consider advertising security awareness information on tickets. This can range from awareness of the national threat level system to emergency actions. Augment this information with brochures at the gates and informational flyers throughout the special event facility.
- *Limit size and scope of hand-carried bags, coolers, etc.* As the threat level increases, consideration must be made to limit the size and scope of hand-carried bags and parcels into the special venue. This greatly reduces the risk of individuals carrying explosives or other weapons onto the site. This information should be broadcast in the pre-event publicity and printed on the event tickets.
- *Mandate use of "clear" baggage.* In addition to, or in lieu of, limiting the size and scope of baggage, is the option of mandating transparent hand-carried baggage, especially during periods of increased threats. This helps satisfy security issues by allowing security staff

members to see the contents of bags while allowing spectators to carry personal belongings into the event area.

- *Place vendors outside control zone.* To minimize congestion at some special venues or during periods of increased risk/threats, consider placing vendors outside the security control zone (outside the entrance gates). This serves several purposes. It reduces congestion inside the gates and allows those areas to be more easily monitored. It also reduces the opportunity for patrons to carry large, bulky items inside the area. Placing vendors outside the gates gives patrons the opportunity to purchase souvenirs before entering the facility and place them in their vehicles, or to defer purchasing items until after the event, as they depart the area.
- *Consider use of temporary flight restrictions over event area.* One way to minimize the risk of aerial attacks is to restrict the airspace over particular events, especially during periods of increased threats. Coordination with local FAA officials should start at the beginning of the planning process. Depending on the event, an exception may be granted to members of the media as well as law enforcement helicopters and small planes.
- *Position TV sets in command post/command center.* Sometimes the fastest way to learn of developing events is to gather information from local news stations. Consider placing TVs in the command center. This will allow for the monitoring of local and national news, which may be important for up-to-date situation developments or different perspectives of local events and situations.
- *Use random observers.* Observers equipped with observation devices and appropriate communications equipment positioned on rooftops, towers and or higher terrain can identify and provide real-time input to the command post/command center regarding developing situations. Using observation devices capable of all-weather usage enhances flexibility.
- *Use helicopters.* Helicopters provide a flexible response capability to large areas, are unencumbered by on-ground obstacles, and provide a flexible and unique vantage point for security personnel. They can also be utilized as an alternative command and control platform for security forces. They can be used in situations from supporting traffic operations to managing disaster scenes. Helicopters provide on-scene commanders a view of the entire area and can help maneuver forces during crisis situations and, if needed, can be used for medical evacuation. When equipped with searchlights and/or thermal imaging devices, they can be invaluable during periods of limited visibility. Additionally, a helicopter provides a powerful visible and audible deterrent at significant distances. Another tactic, if the event is sponsored by a company that rents the Goodyear ™ blimp or other airship, is to station a security expert in the cabin to act as an observer.
- *Use undercover/intelligence agents to gather pre-event information.* Establish contact with local, state, and federal law enforcement agencies early in the planning phase to determine if they have any threat information that may affect the special event. This information can be critical in determining if additional security measures or precautions are necessary and can head off problems before they occur. This information can be critical in determining if additional security measures or precautions are necessary and can head off problems before they occur.
- *Use of explosive detectors/explosive containers.* Consider using explosive detection devices, including explosive-detection-trained canines. These devices not only add a level of security to prevent the introduction of explosives and firearms, but also reassure attendees of a safe environment. The ability of trained canines to assist in other law enforcement and crowd control functions is an added benefit. With or without detection

devices, explosive blast containers should be strategically located throughout the facility to allow the segregation of suspicious items.

- *Use large buses/vehicles as barriers.* As the threat condition increases and parking is moved further from the site, consider using large vehicles as barriers. For example, in the clear standoff zone, consider replacing the parked vehicles with parked buses to serve as barriers. Also, large trucks and/or heavy machinery, such as bulldozers, may be used to block key avenues from advancing vehicles.
- *Exercise control of large vehicles.* The larger the vehicle, the more potential there is for various problems and/or threat scenarios. Consideration should be given, as threat conditions increase, to staging oversized vehicles such as semi trucks in a quarantined area a safe distance from the venue site and other parking areas.

PART V: APPENDIX

Acronyms

ADDIE	Analyze, Design, Develop, Implement and Evaluate
AIA	American Institute of Architects
AMA	American Management Association
AMWA	American Metropolitan Water Association
ANSIR	Awareness of National Security Issues and Response
ARC	American Red Cross
ASHP	American Society of Health-System Pharmacists
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
ASIS	American Society for Industrial Security, International
ASSHTO	American Association of State Highway and Transportation Organization
AT	Antiterrorism
ATF	Bureau of Alcohol, Tobacco and Firearms
ATSA	Aviation and Transportation and Security Act
ATTF	Antiterrorism Task Force
AWWARF	American Water Works Association Research Foundation
BMS	Balanced Magnetic Switch
BOMA	Building Owners and Managers Association
C2	Command and Control
C4	Command, Control, Communication and Computer Systems
CAD	Computer-Aided Design
CBR	Chemical, Biological, Radiological
CBRNE	Chemical, Biological, Radiological, Nuclear Materials or High-Yield Explosive Devices
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control
CERIAS	Center for Education and Research in Information Assurance and Security
CFR	Code of Federal Regulation
CI	Counterintelligence
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Planning
CM	Consequence Management
COMSEC	Communication Security
CPX	Command Post Exercise
CSB	Center for Study of Bioterrorism
CT	Counterterrorism
CTC	Counterterrorism Center
DHS	Department of Homeland Security
DoD	Department of Defense
DoE	Department of Energy
DOJ	Department of Justice
DoS	Department of State
DOT	Department of Transportation
DSTF	Domestic Security Task Force
DVs	Distinguished Visitors
EEFI	Essential Elements of Friendly Information
EF	Earth First!
EMA	Emergency Management Agency
EMT	Emergency Medical Technician
EPA	Environmental Protection Agency
ER	Emergency Response
ERT	Emergency Response Team
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FDLE	Florida Department of Law Enforcement
FEMA	Federal Emergency Management Agency
FEPA	Florida Emergency Preparedness Association
FFC	Federal Facilities Council

FHP	Florida Highway Patrol
FIGHT	Florida Initiative Against Homeland Terrorism
GAO	U.S. General Accounting Office
GIS	Geographic Information Systems
GSA	General Services Administration
GSA FTS	General Services Administration, Federal Technology Service
HAZMAT	Hazardous Materials
HHS	U.S. Dept. of Health and Human Services
HRD	Human Resources Department
HRT	Hostage Response Team
HVAC	Heat Ventilation and Air Conditioning
IAAM	International Association of Assembly Managers, Inc.
IACSP	International Association for Counterterrorism and Security Professionals
IAEM	International Association of Emergency Managers
IED	Improvised Explosive Device
IFMA	International Facility Management Association
INFOSEC	Information Security
ISD	Instructional Systems Design
IT	Information Technology
LBNL	Lawrence Berkeley National Laboratory
MSHARPP	Mission, Symbolism, History, Accessibility, Recognizability, Population, Proximity
MTS	Mitretek Systems
NA	The National Academies
NARAC	National Atmospheric Release Advisory Center
NBAA	National Business Aviation Association, Inc.
NBC	Nuclear, Biological, Chemical
NCIC	National Criminal Information Center
NEMA	National Emergency Management Association
NFPA	National Fire Protection Association
NGA	National Governors' Association
NHSK	National Homeland Security Knowledgebase
NIAP	National Information Assurance Partnership
NIBS	National Institute of Building Sciences
NIJ	National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NLC	National League of Cities
NOC	Network Operations Center
ODP	Office for Domestic Preparedness
OHM	Office of Hazardous Materials
OHMS	Office of Hazardous Material Safety
OPPAGA	(Florida) Office of Program Policy Analysis & Government Accountability
OSHA	Occupational Safety & Health Administration
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PSO	Protective Service Operation
PTE	Potential Terrorist Element
RAM	Random Antiterrorism Measure
RDSTF	Regional Domestic Security Task Force (Florida)
RSPA	Research and Special Programs Administration'
SAM	Surface to Air Missile
SBCCOM	U.S. Army Soldier and Biological Chemical Command
SC	Security Council
SCC	Security Control Center
SET	Security Education and Training
SMO	Security Management Online
TCM	Terrorism Consequence Management
TISP	The Infrastructure Security Partnership
TSA	Transportation Security Administration
TWG	Threat Working Group

UPS	Uninterrupted Power Supply or Source
USACE	U.S. Army Corps of Engineers
USPS	U.S. Postal Service
USSS	U.S. Secret Service
VA	Vulnerability Assessment
WBDG	Whole Building Design Guide
WMD	Weapons of Mass Destruction

PART V: APPENDIX

References

A Plan for Threat Management, Violence in the Workplace, Vol. IV, Protection of Assets Manual, by Carwood, J. S., The Merritt Company, 1995

Burdens of Stress Drive Many People Over the Edge, by Thompson, S.L., Air Force Communications Command Intercom, 1990

Dealing with Dangerous Employees, by Walton, J. B., Security Management, American Society for Industrial Security, 1993

Duty to Protect, by Ingber, C. J., Security Management, American Society for Industrial Security, 1993

Fear and Violence in the Workplace, Northwestern National Life Insurance Company, 1993

Feelings, Customer Service Excellence, by Tschol, J., Better Than Money Corporation, 1988

Handbook of Loss Prevention and Crime Prevention, 3rd Edition, Lawrence J. Fennelly, Ed., Butterworth-Heinemann, 1999

Homeland Defense and Domestic Terrorism: A Selected Bibliography, Naval War College, Library Notes, Vol. 29, No. 2, 2000 http://www.nwc.navy.mil/library/3Publications/Eccles%20Library/LibNotes/libhomelandef.htm

Hospital and Healthcare Security, 4th Edition, by Russell L. Colling, Butterworth-Heinemann, 2001

Introduction to Security, 6th Edition, Robert J. Fischer and Gion Green, Butterworth-Heinemann, 1998

Planning for the Unpredictable, by Herman, M. B., Security Management, American Society for Industrial Security, 1992

Practical School Security: Basic Guidelines for Safe and Secure Schools, by Kenneth S. Trump, Corwin Press, 1998

Protection of Assets Manual, Volumes I–IV, POA Publishing, updated monthly

Safe Schools: A Security and Loss Prevention Plan, by J. Barry Hylton, Butterworth-Heinemann, 1996

Security Business Practices Reference, Volumes II and III, ASIS International, 1999–2000

Security Supervision: Theory and Practice of Asset Protection, 2nd Edition, by Sandi J. Davies and Ronald R. Minion, Ed., International Foundation for Protection Officers and Butterworth-Heinemann, 1999

Stress, Sanity, and Survival, by Woolfolk, R.L. and Richardson, F. C., Monarch, 1978

Tailored Training, by McGarvey, R., American Way Magazine, American Airlines Publishing, 2002

Terrorism Threat Handbook, Interagency OPSEC Support Staff (U.S. Government), June 2001

The Adult Learner, by Knowles, M. S. Butterworth-Heinemann, 1998

The Avenger Personality, by DePue, *R.,* The Academy Group, Inc., 1993

The Handbook for Effective Emergency and Crisis Management, by Mayer Nudell and Norman Antokol, 1988

The World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, Federal Emergency Management Agency (US Government), May 2002

Ticking Bombs: Defusing Violence in the Workplace, by Mantell, M. R., Business One Irwin, 1994

Violence in the U.S. Postal Service, House of Representatives, U.S. Government Printing Office, 1992

Workplace Violence, Perils of a Growing Epidemic, Lipman Report Editors, The Guardsmark, Inc., 1995

PART V: APPENDIX

Glossary

Antiterrorism (AT): Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts. This includes limited response and containment by local forces.

Antiterrorism Adviser: The agency AT adviser charged with managing the AT program.

Antiterrorism Awareness: Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism.

Antiterrorism Plan (AT Plan): A written document with measures provided to establish and maintain an AT program.

Assessment:

- Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity.
- Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents."

Avenue of Approach: The air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path.

Barrier: A coordinated series of obstacles designed or used to channel, direct, restrict, delay, or stop the movement of an opposing force and impose losses in personnel, time, and equipment on the opposing force. Barriers can be natural, or man-made, or a combination of the two.

Barrier Plan: A comprehensive, coordinated plan that includes responsibilities, general location of unspecified and specific barriers, special instructions, limitations, coordination, and completion times. The plan may designate locations of obstacle zones or belts. It is normally prepared as an annex to a contingency or larger operations plan.

Backscatter: A portion of the laser energy that is scattered back in the direction of the seeker by an obscurant. In the terrorism realm, this term is often associated with a type of x-ray device known as a backscatter x-ray machine.

Biological Agent: A microorganism that causes disease in people, plants, or animals or the deterioration of material.

Biological Defense: The methods, plans, and procedures involved in establishing and executing defensive measures against attacks using biological agents.

Biological Threat: A threat that consists of biological material planned to be deployed to produce casualties in people or animals or to damage plants.

Biological Weapon: An item that projects, disperses, or disseminates a biological agent, including arthropod vectors.

Blast Effect: Destruction of or damage to structures and people by the force of an explosion on or above the surface of the ground. Blast effect may be contrasted with the cratering and ground-shock effects of a projectile or charge that goes off underground.

Blast Line: A horizontal radial line on the surface of the earth originating at ground zero on which measurements of blast from an explosion are taken.

Blast Wave: A sharply defined wave of increased pressure rapidly propagated through a surrounding medium from a center of detonation or similar disturbance.

Blister Agent: A chemical agent which injures the eyes and lungs and burns or blisters the skin. It is also called a vesicant agent.

Blood Agent: A chemical compound, including the cyanide group, that affects bodily functions by preventing the normal use of oxygen by body tissues.

Chemical Agent: A toxic chemical intended for use in terrorist or military operations.

Chemical Defense: The methods, plans, and procedures involved in establishing and executing defensive measures against an attack using chemical agents.

Chemical Weapon: Munitions or devices designed to cause death or harm through toxic properties of chemical agents when released.

Cipher Lock: A locking mechanism using an alphabetic, numeric, electronic, or mechanical keypad to control entrance.

Civil Defense: Activities and measures designed or undertaken to:

- Minimize the effects on the civilian population resulting from an enemy (terrorist) attack against the United States
- Deal with the immediate emergency conditions that would be created by such an attack
- Effectuate emergency repairs to or the emergency restoration of, vital utilities and facilities destroyed or damaged by such an attack.

Civil Defense Intelligence: The product resulting from the collection and evaluation of information concerning all aspects of the situation in the United States and its territories that are potential or actual targets of an enemy attack, including the pre-attack phase, emergency measures taken, and estimates of the civil population's preparedness.

In the event of an attack, the information will include a description of conditions in the affected area with emphasis on the extent of damage, fallout levels, and casualty and resource estimates.

This product is required by civil authorities to formulate decisions, conduct of operations, and continue the planning processes.

Civil Disturbance: Group acts of violence and disorder prejudicial to public law and order.

Classification: The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Classified Information: Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

Closed Circuit Television (CCTV): Still or video cameras connected to televisions that are used to detect or monitor activities. They also may be used as a crime deterrent.

Collective Nuclear, Biological, and Chemical (NBC) Protection: Protection provided to a group of individuals in an NBC environment. Generally refers to a facility shelter capable of withstanding NBC events.

Combating Terrorism: Encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism

throughout the threat spectrum, including terrorist use of chemical, biological, radiological, nuclear materials, or high-yield explosive devices (CBRNE).

Command and Control (C2): The exercise of authority and direction by a designated manager or director over assigned personnel. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a manager in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Command and Control System: The facilities, equipment, communications, procedures, and personnel essential to a manager or director for planning, directing, and controlling operations.

Command Center: A facility from which an organizational manager, director, or their representatives direct operations and control forces. It is organized to gather, process, analyze, display, and disseminate planning and operational data and perform other related tasks.

Command, Control, Communications, and Computer Systems (C4): Integrated systems of policies, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a manager's exercise of command and control across the range of operations. Also called C4 systems.

Command Post Exercise (CPX): An exercise in which the participants are simulated that involves the manager, staff, and communications within and between departments and corporate headquarters.

Communications Security (COMSEC): The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes: crypto-security, transmission security, emission security, and physical security of communications security materials and information.

Compromise: The known or suspected exposure of clandestine personnel, site information, or other assets, or of classified information or material, to an unauthorized person.

Computer Security: The protection resulting from all measures to deny unauthorized access and exploitation of computer systems.

Consequence Management (CM): Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the states to respond and the federal government to provide assistance as required.

Contingency Plan: A plan for major contingencies that can reasonably be anticipated in the principal geographic sub-areas of the organizational structure.

Counterintelligence (CI): Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or persons, or international terrorist activities.

Counterintelligence Analysis: The function of assimilating, evaluating, and interpreting information about areas of CI prepotency and responsibility. Information derived from all available sources is considered and integrated in the analytical process.

Counterintelligence Collection: The systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons.

Counterintelligence Investigation: Counterintelligence investigations establish the elements of proof for prosecution or administrative action. They can provide the basis for or be developed from conducting counterintelligence operations. Counterintelligence investigations are conducted against individuals or groups suspected of committing acts of espionage, sabotage, sedition, subversion, terrorism, and other major security violations as well as failure to follow agency directives governing reporting of contacts with foreign citizens and "out-of-channel" requests for information. Counterintelligence investigations provide policy makers with information to eliminate security vulnerabilities and to otherwise improve the security posture of threatened interests.

Counterintelligence Operation: Actions taken against foreign intelligence services to counter espionage and other clandestine intelligence activities damaging to the national security.

Counterintelligence Production: The process of analyzing all source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats and developing it into a final product that is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations.

Counterintelligence Support: Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons.

Countersabotage: That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent sabotage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting sabotage.

Countersurveillance: All measures, active or passive, taken to counteract hostile surveillance.

Counterterrorism (CT): Offensive measures taken to prevent, deter, and respond to terrorism.

Critical Intelligence: Intelligence that is crucial and requires the immediate attention of a manager. It is required to enable a manager to make decisions regarding a timely and appropriate response to actions by the potential or actual enemy. It includes but is not limited to the following:

- Strong indications of the imminent outbreak of hostilities of any type (warning of attack)
- Aggression of any nature against a specific area, agency, or department
- Indications of the use of nuclear, biological, and chemical weapons (targets).

Critical Node: An element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct operations.

Crypto-Security: The component of communications security that results from the provision of technically sound crypto systems and their proper use.

Current Intelligence: One of two categories of descriptive intelligence that is concerned with describing an existing situation. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or persons, or international terrorist activities.

Daily Intelligence Summary: A report prepared in message form at the corporate or department headquarters that provides higher, lateral, and subordinate agencies with a summary of all significant intelligence produced during the previous 24-hour period.

Damage Assessment:

- A determination of the effect of attacks on targets
- A determination of the effect of a compromise of classified information on a department or site.

Deception: Measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests.

Deception Means: Methods, resources, and techniques that can be used to convey information to the deception target.

- Physical Means—Activities and resources used to convey or deny selected information to an unauthorized entity. (e.g., operations, including exercises, reconnaissance, and training activities; use of dummy equipment and devices, tactics, logistic actions, stockpiles, and repair activity; and test and evaluation activities.)
- Administrative Means—Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a person or agency.

Declassification: The determination that, in the interests of agency security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation.

Delaying Operation: An operation in which a security force that is under pressure trades space for time by slowing the enemy's momentum and inflicting maximum damage on the enemy without, in principle, becoming decisively engaged.

Denied Area: An area controlled by enemy or unfriendly forces in which friendly forces cannot expect to operate successfully within existing operational constraints and security force capabilities.

Destroyed: A target so severely damaged that it can neither function as intended nor be restored to a usable condition. In the case of a building, all vertical supports and spanning members are damaged to such an extent that nothing is salvageable. In the case of bridges, all spans must have dropped and all piers must require replacement.

Detection:

- In tactical operations, the perception of an object of possible interest but unconfirmed by recognition
- In surveillance, the determination and transmission by a surveillance system that an event has occurred
- In NBC environments, the act of locating NBC hazards by use of NBC detectors or monitoring and/or survey teams.

Deterrence: The prevention of action through fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

Direct Fire: Gunfire delivered on a target, using the target as a point of aim for either the gun or the director.

Directive:

- A communication in which policy is established or an action ordered

- A plan issued with the intent of putting it into effect when so directed or in the event that a stated contingency arises
- Broadly speaking, any communication that initiates or governs action, conduct, or procedure.

Disaster Control: Measures taken before, during, or after hostile action or natural or man-made disasters to reduce the probability of damage, minimize its effects, and initiate recovery.

Emission Security: The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

Enemy Capabilities: Those courses of action of which the enemy is physically capable and that, if adopted, will damage, destroy, or impede a department from accomplishing its mission or charter. The term "capabilities" includes not only the general courses of action open to the enemy, such as attack, defense, reinforcement, or withdrawal, but also all the courses of action possible under each general course of action. "Enemy capabilities" are considered in light of all known factors affecting operations, including time, space, weather, terrain, and the strength and disposition of enemy forces.

Engage: To bring the enemy under fire.

Environmental Considerations: The spectrum of environmental media, resources, or programs that may impact, or be affected by the planning and execution of operations. Factors may include, but are not limited to, environmental compliance, pollution prevention, conservation, protection of historical and cultural sites, and protection of flora and fauna.

Environmental Threat Assessment: Multimedia medical assessment for biological, chemical, physical, and radiological hazards at an established site.

Escort:

- An armed guard who accompanies visitors (generally public tours or uncleared contract workers) in highly sensitive areas
- An employee (unarmed) assigned to accompany, assist, or guide an individual or group.

Espionage: The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation or terrorist organization.

Essential Elements of Friendly Information (EEFI): Key questions likely to be asked by adversary officials and intelligence systems about friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness.

Establishment: A site, compound, or facility, along with its personnel and equipment, organized as an operating entity.

Evacuation:

- The process of moving a person who is wounded, injured, or ill to and/or between medical treatment facilities
- The clearance of people, animals, or material from a given locality
- The controlled process of collecting, classifying, and shipping unserviceable or abandoned equipment to appropriate reclamation, maintenance, technical intelligence, or disposal facilities
- The ordered or authorized departure of nonessential employees from a specific area.

Event Matrix: A description of the indicators and activity expected to occur in each named area of interest. Normally a cross-reference of each named area of interest and indicator with the times they are expected to occur and the courses of action they will confirm or deny.

Event Template: A guide for collection planning. Depicts the named areas of interest where activity or lack of activity will indicate which course of action the adversary has adopted.

Exercise: A simulated operation involving planning, preparation, and execution carried out for the purpose of training and evaluation. It may be a multi-agency or single-unit exercise.

Facility: A real property entity consisting of one or more of the following: a building, structure, utility system, pavement, or underlying land.

Fallout: The precipitation to earth of radioactive particulate matter from a nuclear cloud; also applies to the particulate matter itself.

Fences: Structures erected; to provide a security measure to deter potential trespassers from accessing specific areas, to ensure safety, and to channel individuals to authorized ingress or egress points.

Food and Water Vulnerability: The susceptibility to overt/covert attack of food and water assets or sources that could cause incapacitation or death.

First Responder Phase: A phase of emergency response units in which:

- Health care providers focus to save life and limb and stabilize the patient sufficiently to withstand evacuation to the next level of care
- Law enforcement establishes control, ensures safety, and renders aid
- Fire department establishes cordons and fire control, renders aid, and performs rescue functions.

Hardened Site: A site, normally constructed under rock or concrete cover, designed to provide protection against the effects of conventional weapons. It may be equipped to provide protection against the side effects of a nuclear attack or against a chemical or a biological attack.

Hardware:

- The generic term dealing with a physical item as distinguished from its capability or function, such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object
- In data automation, the physical equipment or devices forming a computer and peripheral components.

High Explosive Cargo: Cargo such as artillery ammunition, bombs, depth charges, demolition material, rockets, and missiles.

High-Risk-of-Capture Personnel: Personnel whose position or assignment makes them particularly vulnerable to capture by terrorists.

High-Risk Personnel: Personnel who by their grade, assignment, symbolic value, or relative isolation are likely to be attractive or accessible terrorist targets.

High-Value Target: A facility, person, equipment, or information, the loss of which would be expected to seriously degrade important functions.

Hostile Act:

- An attack or other use of force by any civilian or terrorist(s) (with or without national designation) against United States citizens and property, including U.S. commercial assets
- Force used directly to preclude or impede the mission and/or duties of employees or the general public.

When a hostile act is in progress the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat.

Hostile Intent: The threat of imminent use of force by a terrorist, or organization against department or agency and/or U.S. national interests, U.S. forces and, in certain circumstances, U.S. nationals, their property, U.S. commercial assets, and other designated non-U.S. forces, foreign nationals, and their property.

- When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. A determination that hostile intent exists and requires the use of proportional force in self-defense must be based on evidence that an attack is imminent. Evidence necessary to determine hostile intent will vary depending on the state of political tension, unit preparations, intelligence, and indications and warning information.

Hot Pursuit: Pursuit commenced within the territory, internal waters, archipelagic waters, territorial sea, or territorial airspace of the pursuing state and continued without interruption beyond the territory, territorial sea, or airspace.

- Hot pursuit also exists if pursuit commences within the contiguous or exclusive economic zones or on the continental shelf of the pursuing state, continues without interruption, and is undertaken based on a violation of the rights for the protection of which the zone was established
- The right of hot pursuit ceases as soon as the hostile force pursued enters the territory of another state. This definition does not imply that force may or may not be used in connection with hot pursuit. Note: This term typically applies only to law enforcement activities.

Hostage: A person held as a pledge that certain terms or agreements will be kept.

Improvised Explosive Device (IED): A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.

Incapacitating Agent: An agent that produces temporary physiological or mental effects, or both, which will render individuals incapable of concerted effort in the performance of their assigned duties.

Indicator: In intelligence use, information that reflects the intention or capability of a potential enemy to adopt or reject a course of action.

Individual Protection: Actions taken by individuals to survive and continue the mission under conventional, nuclear, biological, and chemical attacks or conditions.

Industrial Chemicals: Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for human use. Hydrogen cyanide, cyanogen chloride, phosgene, and chloropicrin are industrial chemicals that also can be chemical agents.

Information Security (INFOSEC): The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. IT includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

Initial Response Force: The first unit, usually law enforcement, on the scene of a terrorist incident.

Intelligence:

- The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas
- Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Intelligence Estimate: The appraisal of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption.

Intelligence Source: The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors.

Intelligence Summary: A report providing a summary of intelligence items at frequent intervals.

Intelligence System: Any formal or informal system to manage data gathering, obtain and process data, interpret data, and provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations but includes any system, in all its parts, that accomplishes the listed tasks.

Interdiction: An action to divert, disrupt, delay, or destroy a terrorist's potential before it can be used effectively against friendly assets.

Intruder: An individual, unit, or weapon system in or near an operational or exercise area that presents the threat of intelligence gathering or disruptive activity.

Lighting: Multiple types are designed for various security applications. Outdoor security applications can differ greatly from typical indoor office or home applications.

Lux: Light measurement representing the number of lumens per square meter or foot-candles (fc) per square foot. One fc is equal to 10.76 lux (1:10 ratio). Typical exterior perimeter lighting is 0.2fc of illumination while an office parking lot may be close to 1.00fc.

Medical Intelligence: Intelligence resulting from collection, evaluation, analysis, and interpretation of medical, bioscientific, and environmental information of interest to strategic planning and to contingency medical planning and operations.

National Crime Information Center (NCIC): A computerized index of criminal justice information (e.g.; criminal record history information, fugitives, stolen properties, missing persons). It is available to federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year.

Personal Health Protection: Protective measures to medical threats provided by the medical community.

Personnel: Administrators, trainers, and operators that implement the security system.

Physical Security: The component of security that results from all physical measures necessary to safeguard equipment, personnel, and documents from access to or observation by unauthorized persons and to safeguard them against espionage, sabotage, damage, and theft.

Physical Security Plan: A comprehensive written plan providing proper and economical use of personnel and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

Policies and Procedures: Statements of responsibilities and operational techniques and the required means of achieving them.

Proactive Measures: Measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur.

Protective Measures: Actions taken to diminish, deter, delay, thwart, or otherwise minimize the damage of terrorist attacks.

Protective Services: A specialized law enforcement activity that increases the personal safety and security of distinguished personnel or other protectee (e.g., special witness). The activity may be limited to protective threat assessment or may extend to a major protective service operation involving numerous employees and considerable resources.

Protective Service Operation (PSO): The use of specialized techniques and procedures by law enforcement personnel to ensure a protectee's personal safety and security during a specific event, while traveling, or over an extended period of time. When required, a PSO can be tailored to provide 24-hour protection. In such cases, the security detail establishes defensive overt or clandestine perimeters around the protectee for the term of the PSO at the residence, during travel, and at all sites on the protectee's daily itinerary.

Random Antiterrorism Measure (RAM): Random, multiple security measures that consistently change the look of a terrorism protection program. RAMs introduce uncertainty to an overall protection program to defeat surveillance attempts and make it difficult for a terrorist to accurately predict actions.

Restricted Area: An area under special control in which additional security measures are employed to prevent unauthorized entry.

Security Adviser: This individual has responsibility for a security education and training program.

Security Alarms: Electronic devices that detect (at varying levels of probability) people, animals, and vehicles.

Security Council (SC): The single governing body responsible for site security. Organizational leaders are responsible for establishing the SC to implement programs for the protection of personnel, property, and resources under their control. Security programs must meet specified company protection criteria. The responsible lead security manager coordinates and implements mandated security programs. Designated department chairs ensure implementation of security practices by assigned employees.

Security Education and Training: Ideally, this program is an integral part of the employee's orientation to the company and continues throughout his or her career. Individuals should receive security training that is appropriate for their responsibilities and location. Security

plans should be exercised on a regular basis and as needs change. This program is the responsibility of the Security Adviser.

Security Officers:

- An individual whose primary task is to protect personnel, facilities, and equipment while also observing and reporting information
- Acts as a deterrence and delay element.

Signage: Minimum of 6-inch letters of a basic font, such as Times New Roman, Arial, or Helvetica, is necessary to be seen at a distance of 50 feet.

Survivability: The ability to withstand or repel an attack or other hostile action to the extent that essential functions can continue or be resumed after the hostile action.

Terrorism: The calculated use of unlawful violence or threat of unlawful violence to inculcate fear. It is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorism Consequence Management (TCM): Preparedness and response for mitigating the consequences of a terrorist incident, including the use of a weapon of mass destruction. Consequence management activities are designed to support the lead federal agency (domestically, Federal Emergency Management Agency [FEMA]; overseas, Department of State [DoS]) and include measures to alleviate damage, loss of life, hardship, or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

Terrorism Threat Analysis: A continuous process of compiling and examining all available information concerning potential terrorist activists by groups that could target a facility. A threat analysis will review factors of the presence of a terrorist group, operational capability, activity, intentions, and operating environment.

Terrorism Threat Assessment: The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat and the product of a threat analysis for a particular unit or activity.

Terrorist: An individual who uses violence, terror, and intimidation to achieve an objective.

Terrorist Groups: Any element, regardless of size or espoused cause, that commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives.

Terrorist Incident Response Measures: A set of procedures in place for response forces to deal with the effects of a terrorist incident.

Threat and Vulnerability Assessment (VA): In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis.

Threat Working Group (TWG): An AT advisory body for the department, agency, or corporation. Key functions include analyzing threats and providing recommendations to management concerning potential threat condition changes, AT, and other measures based upon potential threats to facilities or personnel. Core membership should include at a minimum the AT adviser, law enforcement, intelligence and medical agencies, and other agencies as required by the department.

Transmission Security: The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than crypto-analysis.

Vulnerability:

- The susceptibility of a department or agency to any action by any means that reduces its effectiveness
- The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment
- In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information systems.

Vulnerability Assessment: An evaluation (assessment) to determine the vulnerability of an area, facility, port, vehicle, residence, or other site to a terrorist attack. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

Weapons of Mass Destruction (WMD): Weapons capable of a high order of destruction and/or used in such a manner as to kill large numbers of people. WMD can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

PART V: APPENDIX

Web Sites

Web Sites by Organization

Acronym	Organization	Description	Web Site
AASHTO	American Association of State Highway and Transportation Officials	A nonprofit representing highway and transportation departments in the U.S.; represents all five transportation modes: air, highways, public transportation, rail, and water	http://www.transportation.org/programs/services.nsf/homepage/overview
AIA	American Institute of Architects	Information on building design	http://www.aia.org
AMA	American Management Association	Information on facilities protection	http://www.amanet.org
AMWA	American Metropolitan Water Association	Membership organization with information and resources	http://www.amwa.net/security/index.html
ANSIR	Awareness of National Security Issues and Response	FBI's National Security Awareness Program. Disseminates unclassified national security threat and warning information to U.S. corporations, law enforcement, and other government agencies	http://www.fbi.gov/hq/ci/ansir/ansirhome.htm
ARC	American Red Cross	Disaster services	www.redcross.org/services/disaster/beprepared/
ASHP	American Society of Health System Pharmacists	Emergency preparedness–counterterrorism resource center	http://www.ashp.org/emergency/
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers	Advances arts and sciences of heating, ventilation, air conditioning, and refrigeration through research, standards writing, continuing education, and publications	http://xp20.ashrae.org
ASIS	American Society for Industrial Security, International	Security management information	www.asisonline.org
ATF	Bureau of Alcohol, Tobacco and Firearms	Enforces the federal laws and regulations relating to alcohol, tobacco, firearms, explosives, and arson	www.atf.treas.gov
AWWARF	American Water Works Association Research Foundation	Sponsors research to help water utilities provide infrastructure reliability	http://www.awwarf.com/index.html
BOMA	Building Owners and Managers Association	Information on emergency planning and security assessment	http://www.boma.org/emergency
CDC	Centers for Disease Control and Prevention	Health guidance	www.cdc.gov
CEMP	Comprehensive Emergency Management Plan	Florida plan that establishes framework to ensure it will be adequately prepared	http://www.floridadisaster.org/bpr/Projects/CEMP%20Online/cemp2000.htm
CIA	Central Intelligence Agency	Intelligence activities and correlating, evaluating, and disseminating intelligence that affects national security	http://www.cia.gov
CSB	Center for Study of Bioterrorism	Lists Internet resources, reference materials, articles, free downloads, and material to order	http://www.slu.edu/colleges/sph/csbei/bioterrorism/index.htm
DoD	U.S. Department of Defense	Provides the military forces needed to deter war and protect the security of our country	http://www.defenselink.mil/admin/about.html
DoD	Lock Program	Glossary of terms	http://locks.nfesc.navy.mil/Glossary.htm

Acronym	Organization	Description	Web Site
DOE	U.S. Department of Energy	Information on disaster preparedness, and emergency response	http://energy.gov/security
EPA	U.S. Environmental Protection Agency	Provides leadership in the nation's environmental science, research, education, and assessment efforts	http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ct-publ.htm
FBI	Federal Bureau of Investigation	Investigative categories include counterterrorism, foreign counterintelligence, organized crime/drugs, violent crimes and major offenders, and financial crime	www.fbi.gov
FDLE	Florida Department of Law Enforcement	Provides information on Domestic Security	http://www.fdle.state.fl.us/osi/DomesticSecurity/
FEMA	Federal Emergency Management Agency	Advises on building codes and flood plain management, teaches how to get through a disaster, helps equip local and state emergency preparedness teams, trains emergency managers, and supports fire service	http://www.fema.gov/about/what.shtm
FEPA	Florida Emergency Preparedness Association	Organization of emergency management professionals created to advance emergency management programs	http://www.fepa.org/
FFC	Federal Facilities Council	Facilities-related publications available online	http://www7.nationalacademies.org/ffc/
GSA FTS	General Services Administration, Federal Technology Service	Provides information technology and network services solutions to government agencies	www.gsa.gov
IACSP	International Association for Counterterrorism and Security Professionals	A membership organization that is a center of information and educational services	http://www.iacsp.com/index.html
IAEM	International Association of Emergency Managers	Terrorism resources	http://www.iaem.com/terrorism1.html
IFMA	International Facility Management Association	Security-related training courses, membership association	www.ifma.org
LBNL	Lawrence Berkeley National Laboratory	Safeguarding buildings	http://securebuildings.lbl.gov
MTS	Mitretek Systems	Nonprofit scientific research systems engineering company	http://www.mitretek.org/home.nsf
NARAC	National Atmospheric Release Advisory Center	Provides tools and services that map the probable spread of hazardous material	http://narac.llnl.gov
National Academies	The National Academies	Web resources for first responders on bioterrorism and public safety, with a search engine of more than 3,000 related Web pages	http://www.nap.edu/shelves/first/
NBAA	National Business Aviation Association, Inc.	A nonprofit organization for business aviation	http://www.nbaa.org/index.htm
NEMA	National Emergency Management Association	Professional association of and for state emergency management directors	http://www.nemaweb.org/index.cfm
NGA	National Governors' Association	Provides practical information and guidance for governors to help plan for and respond to emergencies	http://www.nga.org/center/security/1,1480,,00.html
NHSK	National Homeland Security Knowledgebase	Homeland security information resource	http://www.twotigersonline.com/resources.html
NIBS	National Institute of Building Sciences	Knowledge source for building regulations, science, and technology	http://www.nibs.org
NIPC	National Infrastructure Protection Center	Serves as focal point for threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures, including telecommunications, energy, banking and finance, water systems, government operations, and emergency services	http://www.nipc.gov/about/about.htm

Acronym	Organization	Description	Web Site
NIOSH	National Institute for Occupational Safety and Health	Offers guidance, publications, and training	http://www.cdc.gov/NIOSH/homepage.html
NLC	National League of Cities	Provides research, information sharing, and advocacy	http://www.nlc.org/nlc_org/site/
ODP	Office for Domestic Preparedness	Within the Department of Justice (DOJ), responsible for enhancing the capacity of state and local jurisdictions to respond to and mitigate the consequences of incidents of domestic terrorism	http://www.ojp.usdoj.gov/odp/whatsnew/whats_new.htm
OSHA	Occupational Safety and Health Administration, Department of Labor	Mission is to prevent work-related injuries, illnesses, and deaths	www.osha.gov
SBCCOM	U.S. Army Soldier and Biological Chemical Command	Provides support in three main areas of defense	http://www.sbccom.army.mil
SMO	Security Management Online	Links to online security management articles	http://www.securitymanagement.com
TISP	The Infrastructure Security Partnership	Promotes joint efforts to improve antiterrorism and asset protection methods and techniques	http://www.tisp.org/
USACE	U.S. Army Corps of Engineers	Basic information on building protection	http://buildingprotection.sbccom.army.mil/basic/
USPS	U.S. Postal Service	Mail security	www.usps.gov
WBDG	Whole Building Design Guide	Security-related design information	http://www.wbdg.org

Web Sites by Security Topic

Assessments

Organization	Link/Reference	Description
American Water Association	http://www.awwa.org/bookstore/product.cfm?id=65233 http://www.awwa.org/advocacy/govtaff/finalsecuritystrategy.pdf	Publication: "Security Risk Assessment for Water Utilities" Water security strategy for systems serving populations of less than 100,000
Be Aware Sponsored by Fertilizer Institute, BATF, Association of American Plant Food Control Officials, Agriculture Retailers Association	http://www.atf.treas.gov/pub/threat/secure2.htm	General information to evaluate facility security and reduce vulnerability
BOMA	http://www.boma.org/emergency	Information on emergency planning and security assessment
Disaster-Resource.com	http://www.disaster-resource.com/articles/02p_045.shtml	Commercial site summarizing risk analysis. Fact sheet: "Business Continuity Planning: All the Right Moves"
Florida Department of Education	http://www.firn.edu/doe/besss/safe_passage/safe_passage.htm	"District Safety and Security Self-Assessment"
FDLE and Division of Emergency Management	http://www.fdle.state.fl.us/publications/anti-terrorism.pdf	Assesses Florida's antiterrorism capabilities
Florida Office of Program Policy Analysis and Government Accountability (OPPAGA)	http://www.oppaga.state.fl.us/school_districts/safety/2002%20Safety&Security%20Practices%20(Practices%20and%20Indicators).doc http://www.oppaga.state.fl.us/reports/pdf/0263rpt.pdf	School safety and security best practices with associated indicators School safety and security best practices approved by the commissioner of education, December 2002
NIJ in partnership with the DOE's Sandia National Laboratories	http://www.ncjrs.org/pdffiles1/nij/195171.pdf	Prototype of 12-step methodology to assess security of chemical facilities within U.S.

Organization	Link/Reference	Description
Research and Special Programs Administration's (RSPA) Office of Hazardous Materials Safety (OHMS)	http://hazmat.dot.gov/rmsef.htm	Risk management self-evaluation framework for transportation of hazardous materials—best practices
FEMA	http://www.fema.gov/library/bizindex.shtm	Emergency management guide for business and industry
National Business Association	http://www.saftnet.net/webmail/newsletter1002_nba.html	Commercial information recommended by National Business Association. Newsletter on emergency management information for small business
WBDG	http://www.wbdg.org/design/resource.php?cn=2.7.4&cx=0&rp=27	Threat/vulnerability assessments and risk analysis

Aviation

Organization	Link/Reference	Description
Aircraft Owners and Pilots Association	www.aopa.org	Private aircraft owners and pilots
Airports Council International North America	www.acina.org	Represents city and county airports
Experimental Aircraft Association	www.eaa.org	Experimental aircraft owners and pilots
Federal Aviation Administration (FAA)	http://www1.faa.gov	Airport/aviation regulations
National Association of State Aviation Officials	www.nasco.org	Represents state aviation offices
National Aviation Association Inc.	http://www.nbaa.org/ops/security/bestpractices.htm	Best practices for business aviation security
Security Management Online	http://www.securitymanagement.com	"Airing on the Side of Safety"
Transportation Security Administration (TSA)	http://www.tsa.gov/public/index.jsp	Security aviation regulations
U.S. General Accounting Office (GAO)	http://www.gao.gov/new.items/d03253.pdf	Security program–registered traveler program

Buildings

Organization	Link/Reference	Description
AIA	http://www.aia.org/security/	Building security by design information
ASHRAE	http://xp20.ashrae.org/about/extraordinary.pdf	Risk management guidance
BOMA	http://www.boma.org/emergency	Information on emergency planning and security assessment
BOMA, Calgary	http://www.boma.ca/Ontario%20Emergency%20Guide.pdg	Security and emergency planning
CDC—NIOSH	http://www.cdc.gov/niosh/emres01.html	Emergency response resources
CDC	http://www.ojp.usdoj.gov/odp/assessments/definition.htm	Advice for safeguarding buildings against chemical or biological attack
EPA	http://wpa.gov/iag/schools/ http://www/epa.gov/iaq/largebldgs/baqtoc.html	Procedures and checklist for developing building profile "Building Air Quality: A Guide for Building Owners and Facility Managers"
FFC	http://www7.nationalacademies.org/ffc/	Facilities-related publications available online
Headquarters Department of the Army	http://www.iaam.org/CVMS/CVMSsafety.htm	"Physical Security Field Manual, No. 3-19.30"

Organization	Link/Reference	Description
LBNL	http://securebuildings.lbl.gov/secure.html	Web site for emergency personnel and building operators that contains advice for dealing with a biological or chemical release in a building
Solicitor General of Ontario	http://www.boma.ca/Ontario%20Highrise%20Emergency%20Guide.pdf	Report: "A Guide to Strengthen Emergency Management of High-Rise and High-Risk Buildings"
USACE	http://buildingprotection.sbccom.army.mil/basic/	Basic information on building protection
SBCCOM	http://buildingprotection.sbccom.army.mil/basic/index.htm	Basic information on building protection

Chemical, Biological, Radiological, Nuclear Explosive

Organization	Link/Reference	Description
American Security Council	http://www.americanchemistry.com/cmawebsite.nsf/s?readform&nnar-53rkt8	Report: "Guide to Site Security in the U.S. Chemical Industry"
Center for Civilian Biodefense Strategy	http://www.hopkins-biodefense.org	"New Developments"
Center for Infectious Diseases	http://www1.umn.edu/cidrap/content/bt/bioprep/planning/bt-prep-planning.html	Bioterrorism preparedness, planning, and response
CDC and NIOSH	http://www.cdc.gov/niosh/bldvent/2002-139.html	Guidance for protecting building environments from airborne chemical, biological, or radiological attacks
CSB	http://www.slu.edu/colleges/sph/csbei/bioterrorism/index.html	Comprehensive site maintained by Saint Louis University School of Public Health
CDC	http://www.cdc.gov	Heath guidance for CBR agents
CDC	http://www.bt.cdc.gov	Information on bioterrorism
CIA	http://www.cia.gov/cia/publications/cbr_handbook.htm	Chemical, biological, radiological incident handbook
LBNL	http://securebuildings.lbl.gov	Safeguarding buildings against chemical or biological attack
MTS	http://www.mitretek.org/home.nsf/BusinessAreas/HomelandSecurity	Role in homeland security and counterterrorism
National Academies	http://www.nap.edu/shelves/first/	Responding first to bioterrorism—searchable "Webshelf"
NARAC	http://narac.llnl.gov	Provides tools and services that map the probable spread of hazardous material
SBCCOM	http://www.sbccom.army.mil	Provides support in three main areas of defense
U.S. Dept. of Health and Human Services (HHS)	http://www.hhs.gov/disasters/index.shtml	Disasters and emergencies

Emergency Response and Services

Organization	Link/Reference	Description
ASIS	http://www.asisonline.org	Has link to crises response resources
Best Practice in Emergency Services	http://www.emsbest.com	Monthly online newsletter for fire and EMS managers
CDC–NIOSH	http://www.cdc.gov/niosh/emhaz2.html#elements	Suggested guidance for supervisors at disaster rescue sites
CDC–NIOSH	http://www.cdc.gov/niosh/unp-trinstrs.html	Traumatic incident stress: information for emergency response workers
EPA	http://www.epa.gov/superfund/programs/er/index.htm	Emergency response (ER) program
Florida Division of Emergency Management	http://www.floridadisaster.org/bpr/EMTOOLS/Terrorism/Summit/	*Terrorism Summit Handbook*—see Annex B for "Incident Response Plan" and Chapter 2 for descriptions of "The Response Organization"
International Association of Assembly Managers, Inc. (IAAM)	http://www.iaam.org/CVMS/TerrorismFacts.pdf	Terrorism response planning for venue managers
Iowa Emergency Management Division	http://www.state.ia.us/government/dpd/emd/Iowa%20Fire%20Assessment%20Final%20Form.doc	Publication: "Fire Operations Capabilities Assessment Tool for Response to Weapons of Mass Destruction"
NGA Center for Best Practices	http://www.nga.org/cda/files/081202HSPRIORITIES.pdf	States' homeland security priorities
University of North Florida	http://www.unf.edu/dept/ehs/documents/hazmatmanage.pdf	Publication: "Hazardous Materials Management Programs"
Rand Science and Technology Institute	http://www.rand.org/publications/CF/CF176/CF176.pdf	Protecting emergency responders

Food Vulnerability

Organization	Link/Reference	Description
FSIS Emergency Response Team (ERT)	http://www.fsis.usda.gov/OPPDE/rdad/FSISNotices/27-02.htm	General information for employees (good explanation of ERT)
Florida OPPAGA	http://www.oppaga.state.fl.us/reports/pdf/0264rpt.pdf	New security rules…aerial application industry

General References

Organization	Link/Reference	Description
AMA	http://www.amanet.org/research/pdfs/2002_CrisisMgmtSurvey.pdf	*Survey*—crisis management and security issues
AWWARF	http://www.awwarf.com/wwwsites/othersources.html	Water information sources, north america
ASIS	http://www.asisonline.org/glossary/glossary.html	Glossary of security terms
CIO.com	http://www.cio.com/online/102401_nasdaq.html	Article: "Nasdaq Lessons Learned from Sept. 11"
DoD Lock Program	http://locks.nfesc.navy.mil/Glossary.htm	Glossary of terms
EPA	http://www.energy.gov/security/index.html	Comprehensive links to security topics
EPA	http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ct-epro.html	EPA's role and authority in counterterrorism
EPA	http://www.epa.gov/ebtpages/emergencies.html	Extensive list of links to emergencies
FDLE and Florida Division of Emergency Management	http://www.fdle.state.fl.us/publications/anti-terrorism.pdf	Assessing Florida's antiterrorism capabilities, September 2001
FDLE	http://www.fdle.state.fl.us/osi/DomesticSecurity/reports.htm	Reports and publications related to domestic security

Organization	Link/Reference	Description
FDLE	http://www.fdle.state.fl.us/Publications/domestic_security/Domestic_Security_Nov_2002_Annual_Report.pdf	*"Strengthening Domestic Security*—Making Florida Safer," Annual Report, November 2002
Florida Division of Emergency Management	http://www.floridadisaster.org/bpr/EMTOOLS/	*Emergency management toolbox*—links to variety of resources general disaster issues
Florida Division of Emergency Management	http://www.dca.state.fl.us/bpr/EMTOOLS/Terrorism/Summit/terrorism.htm	Links to agencies and resources
Florida Division of Emergency Management	http://www.floridadisaster.org/bpr/EMTOOLS/Severe/terrorism.htm	General information and links to related sites
FEPA	http://www.emergencyemail.org/	Emergency preparedness e-mail notification service
Florida Initiative Against Homeland Terrorism (FIGHT)	http://www.flash.org/fight/employers.html	Employer information
Florida's Domestic Security Oversight Board—Terrorism and Domestic Preparedness	http://www.fdle.state.fl.us/Publications/domestic_security/Domestic_Security_Nov_2002_Annual_Report.pdf	"Strengthening domestic security in Florida, Making Florida Safer," November 2002, annual report
MyFlorida.com Domestic Security in Florida	http://www.myflorida.com/myflorida/domestic_security/index.html	*Domestic security in Florida*—links to information
National Academies	http://www.nap.edu/shelves/first/sites.html	Extensive links to security, terrorism-related sites
National Academies	http://stills.nap.edu/terror/	Terrorism and security collection publications (free online)
National Institute of Standards and Technology (NIST)	http://icat.nist.gov/vt_portal.cfm	ICAT Metabase is a searchable index of computer vulnerabilities that links users to a variety of publicly available vulnerability databases and patch sites
NIST	http://www.nist.gov/public_affairs/factsheet/homeland.htm	Technologies for improved homeland security
National League of Cities	http://www.nlc.org/nlc_org/site/files/reports/hsrp0902.pdf	Cities taking on security responsibilities
NGA Center for Best Practices	http://www.nga.org/center/1,1188,C_FAQ^D_359,00.html	Center services: identifying and sharing best practices
OSHA	http://www.osha.gov/SLTC/index.html	Extensive list of safety and health topics
The Infrastructure Security Partnership	http://www.tisp.org/	News, publications, discussion groups, newsletter
U.S. Department of Justice, Office of Justice Programs	http://www.ojp.usdoj.gov/terrorism/whats_new.htm	Lesson's learned 9/11

Information Technology

Organization	Link/Reference	Description
NIST	http://icat.nist.gov/icat.cfm	**ICAT** is a searchable index of information on computer vulnerabilities that provides search capability at a fine granularity and links users to vulnerability and patch information
CISSP (Open Study Guides Web Site)	http://www.cccure.org/Documents/HISM/ewtoc.html	A knowledge-rich site with a wide range of material for example: *Handbook of Information Security Management*
National Information Assurance Partnership (NIAP)	http://niap.nist.gov/cc-scheme/	Common criteria evaluation and validation scheme

Infrastructure

(Also see Assessments, Aviation, Technology, and Transportation)

Organization	Link/Reference	Description
AMWA	http://www.amwa.net/security/index.html	Water security resources
NIPC	http://www.nipc.gov/about/about.htm	Information on all areas of critical infrastructure
Canadian National Guide Survey by Center for Expertise and Research on Infrastructure in Urban Areas	http://www.infraguide.gc.ca/docs/SWW4E.pdf	Best Practices Survey: "How to Inspect, Assess, and Evaluate the Structure and Capacity of Storm Water and Waste Water Collection Systems"

Mail and Packages

Organization	Link/Reference	Description
BOMA Calgary	http://www.boma.ca/emergency.htm	Links to mail and package security
ATF, Treasury	http://www.atf.treas.gov/explarson/information/indic.htm	Suspect letter and package indicators
CDC, USPS FDLE	http://www.floridadisaster.org/bpr/EMTOOLS/Severe/package_guidelines.pdf	Information on suspicious packages
FDLE	http://www.myflorida.com/myflorida/domestic_security/MailroomSecurity.doc	"Addressing Biological & Chemical Threats and Mail Bombs (Mail Security)"
SMO	http://www.securitymanagement.com	"How and When a Company Should Scan Mail for Explosives or Bomb Components Depends on the Company's Own Profile"
USPS	http://www.usps.com/news/2001/press/mailsecurity/pr01_isbestprac.htm	"Security of the Mail: Best Practices"

Preparedness

Organization	Link/Reference	Description
Epidemiology Program Office, CDC	http://www.bt.cdc.gov/Documents/BTStratPlan.pdf	Recommendation: "Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response"
FEMA	http://www.fema.gov/library/bizindex.shtm	A step-by-step approach to emergency planning, response, and recovery for companies of all sizes
Florida Division of Emergency Management	http://www.floridadisaster.org/bpr/EMTOOLS/Severe/terrorism.htm	General information and links to related sites
NFPA	http://www.nfpa.org/BuildingCode/News/BuildingEvacuation/buildingevacuation.asp	Strategies in building evacuation messages
NFPA	http://www.nfpa.org/Research/NFPAFactSheets/Evacuations/Evacuations.asp	*Fact sheet*—Building Evacuations
NFPA	http://www.nfpa.org/Research/NFPAFactSheets/Emergency/Emergency.asp	*Fact sheet*—Developing a Preparedness Plan and Conducting Emergency Evacuation Drills
OSHA	http://www.osha.gov/Publications/osha3151.pdf	Publication: Assessing the Need for Personal Protective Equipment, a Guide for Small Businesses
SMO	http://www.securitymanagement.com	"How and When a Company Should Scan Mail for Explosives or Bomb Components Depends on the Company's Own Profile"

Protection Planning

Organization	Link/Reference	Description
AMA	http://www.amanet.org/sept_11/facilities_protection_plan.htm	Create a facilities protection plan
ARC	http://www.redcross.org/services/disaster/beprepared/hsas/business.pdf	Homeland Security advisory system recommended actions
BOMA, Calgary	http://www.boma.ca/Ontario%20Highrise%20Emergency%20Guide.pdf	Security and Emergency planning, "A Guide to Strengthen Emergency Management of High-Rise and High Risk Buildings"
FEMA	http://www.fema.gov/onp/introstate.shtm	Introduction to state and local EOP planning guidance
FEMA and Public-Private Partnership	http://www.fema.gov/pdf/library/bizindst.pdf	Publication: "A Step-By-Step Guide to Emergency Planning, Response, and Recovery for Companies of All Sizes"
IAAM Security Manager	http://www.iaam.org/Facility_manager/Pages/2002_May_Jun/legal.htm	Facility pre-employment information and verification, first level of security defense
NFPA	http://www.nfpa.org/Research/NFPAFactSheets/NFPAFactSheets.asp	*Fact Sheets*—Building Evacuations
NGA (Center for Best Practices)	http://www.nga.org/center/divisions/1,1188,T_CEN_HS^C_ISSUE_BRIEF^D_4362,00.html	"A Governor's Guide to Emergency Management Volume Two: Homeland Security"
NIOSH	http://atfp.nfesc.navy.mil/pdf/NIOSH%20Report.pdf	Guidance for protecting Building environments from airborne chemical, biological, or radiological attacks

Security Design

Organization	Link/Reference	Description
AIA	http://www.aia.org	Resource center on building security through design
NIBS	http://www.wbdg.org	Security-related design information
U.S. GSA	http://hydra.gsa/gov/pbs/pc/facilitiesstandards	Design standards and criteria for new buildings, alterations
WBDG	http://www.wbdg.org/design/resource.php?cn=2.7.4&cx=0&rp=28	Balancing security/safety and sustainability objectives

Security Officers

Organization	Link/Reference	Description
Shopping Center World	http://shoppingcenterworld.com/ar/retail_best_practices_security/index.htm	"Best Practices: Security at Front and Center"

Security Systems

Organization	Link/Reference	Description
Checkpoint Metro Canada, Inc.	http://www.retailcouncil.org/rpn/cctvtips.asp	CCTV Tips
Digital Technology	http://securitysolutions.com/ar/security_digital_revolution_continues/index.htm	Access control and security systems
NIJ, National Law Enforcement and Corrections Technology Center	http://www.nlectc.org/perimetr/handbook.htm	Perimeter security sensor technologies handbook (CD file, online)
GSA, Federal Technology Service	http://www.gsa.gov/Portal/content/offerings_content.jsp?contentOID=122778&contentType=1004	Fact sheets and IT security solutions
NIJ	http://www.ncjrs.org/school/home.html	"The Appropriate and Effective Use of Security Technologies in U.S. Schools"
NIST	www.nist.gov	Numerous and varied information for measurement, standards, and technology
Virginia Commonwealth University Police	http://www.vcu.edu/police/access.html	Comprehensive presentation of building access

Special Events/Venues

Organization	Link/Reference	Description
Crowdsafe	http://www.crowdsafe.com/	Web site dedicated to improving crowd safety at music events worldwide
IAAM Security Manager	http://www.iaam.org/CVMS/CVMSsafety.htm http://www.iaam.org/CVMS/CVMSlinks.htm	Articles, editorials, feature stories Extensive list of links for security for special events
IAAM	http://www.iaam.org/CVMS/TerrorismFacts.pdf	*Best practice protocols*—terrorism response planning
The Outback Bowl and Tampa Sports Authority	http://www.outbackbowl.com/tickets/security.html	"Stadium Security Policies"
Texas Tech	http://texastech.ocsn.com/sports/m-footbl/spec-rel/091002aaa.html	Jones SBC Stadium security guidelines

Threats

Organization	Link/Reference	Description
ATF	http://www.atf.treas.gov/press/breakingnews/threat.htm	Explosives, bomb threat, and detection resources
Crisis Response Planning Corporation	http://www.crpc.com/The%20Library.htm	*Crisis management case study*—bomb threats
IdeaByte	http://www.gigaweb.com/content/DR/RIB-092001-00095.pdf	Fact Sheet: "Best Practices in Security: Bomb Threats"
Florida Department of Emergency Management	http://www.dca.state.fl.us/FDEM/	Current threat level

Training

Organization	Link/Reference	Description
American Society for Training & Development (ASTD)	http://www.astd.org/index_IE.html	Link to training development tools and organization
International Association for Continuing Education and Training	http://www.iacet.org/	Nonprofit association dedicated to quality continuing education and training programs
Medical Device-Link Help Desk	http://www.devicelink.com/mddi/archive/97/07/012.html	Developing a successful employee training program
Longview Community College	http://www.kcmetro.cc.mo.us/longview/ctac/blooms.htm	"Bloom's Taxonomy and Critical Thinking"

Transportation

Organization	Link/Reference	Description
AASHTO	http://www.transportation.org/programs/services.nsf/homepage/overview	Links to programs and services
Florida Public Transportation Technical Assistance Training Program/Center for Urban Transportation	http://www.nctr.usf.edu/pdf/Transit%20Terrorism%20Resource%20Guide.pdf	Publication: "Anti-Terrorism Resource Guide" and extensive information and links to related sites
National Academies of Science	http://www.nas.edu/trb/publications/MarineBoard/2001SummerPorts/Session9Cross.pdf	PowerPoint presentation: "Seaport Security: Training, Equipment, and Research Needs," a commercially produced publication
Mineta Transportation Institute	http://gulliver.trb.org/publications/am/presentations/Session131-BrianMJenkins.pdf	Publication: "Best Security Practices" for Protecting Surface Transportation Against Terrorism and Serious Crime
U.S. Dept. of Transportation (DOT)	http://ntl.bts.gov/faq/sept11.html	Transportation security information