

Building Security Rating System

Checklists to Assess Risks, Consequences,
and Security Countermeasures

Building Security Rating System

This page intentionally left blank

ASCE Manuals and Reports on Engineering Practice No. 128

Building Security Rating System

Checklists to Assess Risks, Consequences, and Security Countermeasures

Prepared by the
Building Rating Security Committee (BRSC) of the
Architectural Engineering Institute (AEI) of the
American Society of Civil Engineers (ASCE)

Edited by
Mohammed M. Ettouney, Ph.D., P.E.

Library of Congress Cataloging-in-Publication Data

Building security rating system : checklists to assess risks, consequences, and security countermeasures / prepared by the Building Rating Security Committee (BRSC) of the Architectural Engineering Institute (AEI) of the American Society of Civil Engineers (ASCE) ; edited by Mohammed M. Ettouney, Ph.D., P.E., MBA, F.AEI, Dist.M.ASCE.

pages cm.—(ASCE manuals and reports on engineering practice ; no. 128)

Includes bibliographical references and index.

ISBN 978-0-7844-1334-0 (print)—ISBN 978-0-7844-7838-7 (pdf)

1. Buildings—Security measures—Evaluation. 2. Security systems—Evaluation. I. Ettouney, Mohammed. II. Architectural Engineering Institute. Building Rating Security Committee.

TH9705.B8465 2014

621.389'28—dc23

2014010558

Published by American Society of Civil Engineers

1801 Alexander Bell Drive

Reston, Virginia, 20191-4382

www.asce.org/bookstore | ascelibrary.org

Any statements expressed in these materials are those of the individual authors and do not necessarily represent the views of ASCE, which takes no responsibility for any statement made herein. No reference made in this publication to any specific method, product, process, or service constitutes or implies an endorsement, recommendation, or warranty thereof by ASCE. The materials are for general information only and do not represent a standard of ASCE, nor are they intended as a reference in purchase specifications, contracts, regulations, statutes, or any other legal document. ASCE makes no representation or warranty of any kind, whether express or implied, concerning the accuracy, completeness, suitability, or utility of any information, apparatus, product, or process discussed in this publication, and assumes no liability therefor. The information contained in these materials should not be used without first securing competent advice with respect to its suitability for any general or specific application. Anyone utilizing such information assumes all liability arising from such use, including but not limited to infringement of any patent or patents.

ASCE and American Society of Civil Engineers—Registered in U.S. Patent and Trademark Office.

Photocopies and permissions. Permission to photocopy or reproduce material from ASCE publications can be requested by sending an e-mail to permissions@asce.org or by locating a title in ASCE's Civil Engineering Database (<http://cedb.asce.org>) or ASCE Library (<http://ascelibrary.org>) and using the "Permissions" link.

Errata: Errata, if any, can be found at <http://dx.doi.org/10.1061/9780784413340>

Copyright © 2015 by the American Society of Civil Engineers.

All Rights Reserved.

ISBN 978-0-7844-1334-0 (paper)

ISBN 978-0-7844-7838-7 (PDF)

Manufactured in the United States of America.

22 21 20 19 18 17 16 15 1 2 3 4 5

Cover photo credit: Mr. Martin Denholm of the Smith Group, Washington, DC.

MANUALS AND REPORTS ON ENGINEERING PRACTICE

(As developed by the ASCE Technical Procedures Committee, July 1930,
and revised March 1935, February 1962, and April 1982)

A manual or report in this series consists of an orderly presentation of facts on a particular subject, supplemented by an analysis of limitations and applications of these facts. It contains information useful to the average engineer in his or her everyday work, rather than findings that may be useful only occasionally or rarely. It is not in any sense a “standard,” however; nor is it so elementary or so conclusive as to provide a “rule of thumb” for nonengineers.

Furthermore, material in this series, in distinction from a paper (which expresses only one person’s observations or opinions), is the work of a committee or group selected to assemble and express information on a specific topic. As often as practicable the committee is under the direction of one or more of the Technical Divisions and Councils, and the product evolved has been subjected to review by the Executive Committee of the Division or Council. As a step in the process of this review, proposed manuscripts are often brought before the members of the Technical Divisions and Councils for comment, which may serve as the basis for improvement. When published, each work shows the names of the committees by which it was compiled and indicates clearly the several processes through which it has passed in review, so that its merit may be definitely understood.

In February 1962 (and revised in April 1982), the Board of Direction voted to establish a series titled “Manuals and Reports on Engineering Practice,” to include the Manuals published and authorized to date, future Manuals of Professional Practice, and Reports on Engineering Practice. All such Manual or Report material of the Society would have been refereed in a manner approved by the Board Committee on Publications and would be bound, with applicable discussion, in books similar to past Manuals. Numbering would be consecutive and would be a continuation of present Manual numbers. In some cases of joint committee reports, bypassing of Journal publications may be authorized.

A list of available Manuals of Practice can be found at <http://www.asce.org/bookstore>.

This page intentionally left blank

BUILDING RATING SECURITY COMMITTEE (BRSC)

Mohammed Ettouney, Ph.D., P.E., MBA, Dist.M.ASCE, F.AEI
Principal, Weidlinger Associates, New York, NY
Chairman

Sreenivas Alampalli, Ph.D., P.E., MBA, F.ASCE, F.ASNT
Director, Structures Evaluation Services Bureau, New York State Department of Transportation,
Albany, NY

Scott Campbell, Ph.D., P.E.
President, Structural Analysis Consulting Group, Milwaukee, WI

Amar Chaker, Ph.D., F.AEI, F.EMI, F.ASCE
Director, Engineering Mechanics Institute, American Society of Civil Engineers, Reston, VA

Martin Denholm, F.AIA, LEED AP, BSCP
Vice President, Smith Group

Mark Hankewycz, CPP, M.AEI
President, Security Consulting and Design Services, M2H Protection, Middletown, MD

Milagros Kennett, M.AEI
Director, U.S. Department of Homeland Security, Washington, DC

Rober J. Lomb, Jr., CPP, RCDD, PSP, BSCP
Senior Security Engineer, Exp US Services Inc., Chicago, IL

Detective Arturo Mendez
NYPD/DHS Liaison, New York City Police Department , New York, NY

Paul Mlakar, Ph.D., P.E., Dist.M.ASCE
Senior Research Scientist, U.S. Army Research and Development Center, Vicksburg, MS

Hasan Aydin Pekoz, Ph.D., P.E., LEED AP
Senior Engineer, Weidlinger Associates, New York, NY

David C. Weggel, Ph.D., P.E., A.M.ASCE
Associate Professor of Civil Engineering, University of North Carolina at Charlotte

APPLIED RESEARCH ASSOCIATES

James Brokaw
Larry Bryant
Anthony DiGregorio
Douglas Fitzgerald
Douglas Hall
Joseph Smith
Joseph Stevens

BLUE RIBBON REVIEW PANEL

Sharada Alampalli
President, Prospect Solutions, Loudonville, NY

Peter DiMaggio, P.E.
Principal, Weidlinger Associates, New York, NY

Adam Hapj, P.E.
Senior Associate, Weidlinger Associates, New York, NY

Ali Memari, Ph.D., P.E., F.ASCE
Professor, Pennsylvania State University, University Park, PA

James Ruggieri, P.E.
President, General Machine Corporation, Fairfax Station, VA

ASCE / AEI STAFF

Carol Kurlancheek, P.E., LEED AP, M.ASCE
Verna Jameson, Aff.M.ASCE

CONTENTS

	Preface	xi
1.	Introduction	1
	1.1 Purpose	1
	1.2 Basis	1
	1.3 This Document	2
2.	Building Classification	3
	2.1 Overview	3
	2.2 Methodology: General	3
	2.3 General Classification Approach	4
	2.4 Primary Hazard Classification Factors	5
	2.5 Secondary Hazard Classification Factors	5
	2.6 Primary Impact/Consequence Classification Factors	8
	2.7 Secondary Impact/Consequence Classification Factors	9
	2.8 Mathematical Evaluation of Building Classification	10
3.	Countermeasure Evaluation	13
	3.1 Overview	13
	3.2 Countermeasure Levels	13
	3.3 Layout of Levels	13
	3.4 Required Countermeasures	18
	3.5 Not Applicable Countermeasures	18
	3.6 Interrelationships among Countermeasures	19
4.	Building Security Rating	21
	4.1 Overview	21
	4.2 Description of Rating Categories	21
	4.3 Rating System Philosophy	23
	4.4 Process of Rating Building Security	23
	4.5 Bonus Points	25
APPENDIX A	Classification and Impact Questions	27
APPENDIX B	Rating Class and Countermeasure Requirements for Each Rating Level	33
APPENDIX C	Innovations in Building Security	45
APPENDIX D	Countermeasure Commentary for Level 1, Rated	47
APPENDIX E	Countermeasure Commentary for Level 2, Bronze	57
APPENDIX F	Countermeasure Commentary for Level 3, Silver	77
		ix

APPENDIX G	Countermeasure Commentary for Level 4, Gold	103
APPENDIX H	Countermeasure Commentary for Level 5, Platinum	139
	References	159
	Index	165

PREFACE

This document presents a building security rating system (BSRS), which addresses security-related disciplines—from conceptual to design and development to operations and maintenance—and enables improved survivability of buildings and occupants subjected to terrorist attack. The BSRS rates buildings for their relative security using a rigorous system that (1) identifies physical and operational criteria that enhance building security and (2) compares building conformity with those criteria. The system includes the development and maintenance of a security-enhancing physical and operations rating protocol. Personnel training is the key to this end. This training includes, but is not limited to, continued adequate certification and education programs.

Conceptually, the BSRS is similar to the U.S. Green Building Council's Leadership in Energy and Environmental Design (LEED) system; both systems rate buildings according to an accepted set of rules for ensuring particular categories of performance in their respective fields. Technically, the building security rating system is based on the physical and operational features defined in FEMA 426 (2003a). FEMA 426 provides guidance for building stakeholders to reduce physical damage to buildings, related infrastructure, and people caused by terrorist assaults. This approach allows for the effective transfer of decades of federal and Department of Defense (DoD) research and experience to the broader building science community. The guidance of FEMA 426 is presented in the form of a comprehensive qualitative checklist that covers the essential 13 building security disciplines. In addition, FEMA 426 provides a complete commentary to all security items in the checklist to guide the user and ensure accurate implementation. The conceptual and technical basis of the system is described in Section 1.2 of Chapter 1.

The BSRS system is based on three pillars: building classification, security countermeasures, and the building security rating as shown in Fig. P-1. The three are interdependent, and their interdependency is accommodated in the rating system methodology. Note that Version 2.0, presented in this manual, covers only buildings; no other types of infrastructures are covered.

The building is classified, from a security viewpoint, into four classes. The classes (A, B, C, and D, from higher to lower security sensitivity) depend on both security exposure (hazard or threat) and consequence of loss (effects of loss). The classification system covers all important aspects of the hazards and the effects of terrorist attacks on buildings in a qualitative-to-quantitative method. The method is simple, based on a checklist and multiple-choice approach as detailed in Chapter 1. The multiple choices help in assigning quantitative values to the qualitative checklist. A simple method is then applied to quantify the final building security classification (A, B, C, or D). The multiple choice checklists for building classifications are given in Appendix A.

The second pillar of the rating system comprises the five rating categories. From the least secure to the most secure, the ratings are rated bronze, silver, gold, and platinum. Awarding a particular security rating category to a building depends on the building class (the first pillar) and existing security countermeasures (the third pillar). A description of the security rating categories is provided in Chapter 4.

The third pillar of the rating system is the security countermeasure (mitigation) evaluation. The basis of this step is that for each of the five security rating categories and the four building classes, a minimum level of security countermeasures must be implemented. The security countermeasure evaluation identifies 20 levels of countermeasures for the rating category–building class combinations. The different security countermeasures are subdivided by discipline (similar to FEMA 426). Given a desired security rating category, the building must achieve certain combinations of countermeasure levels. The procedures for achieving particular levels of countermeasures are detailed in Chapter 3. The actual checklists of all countermeasures are given in Appendix B.

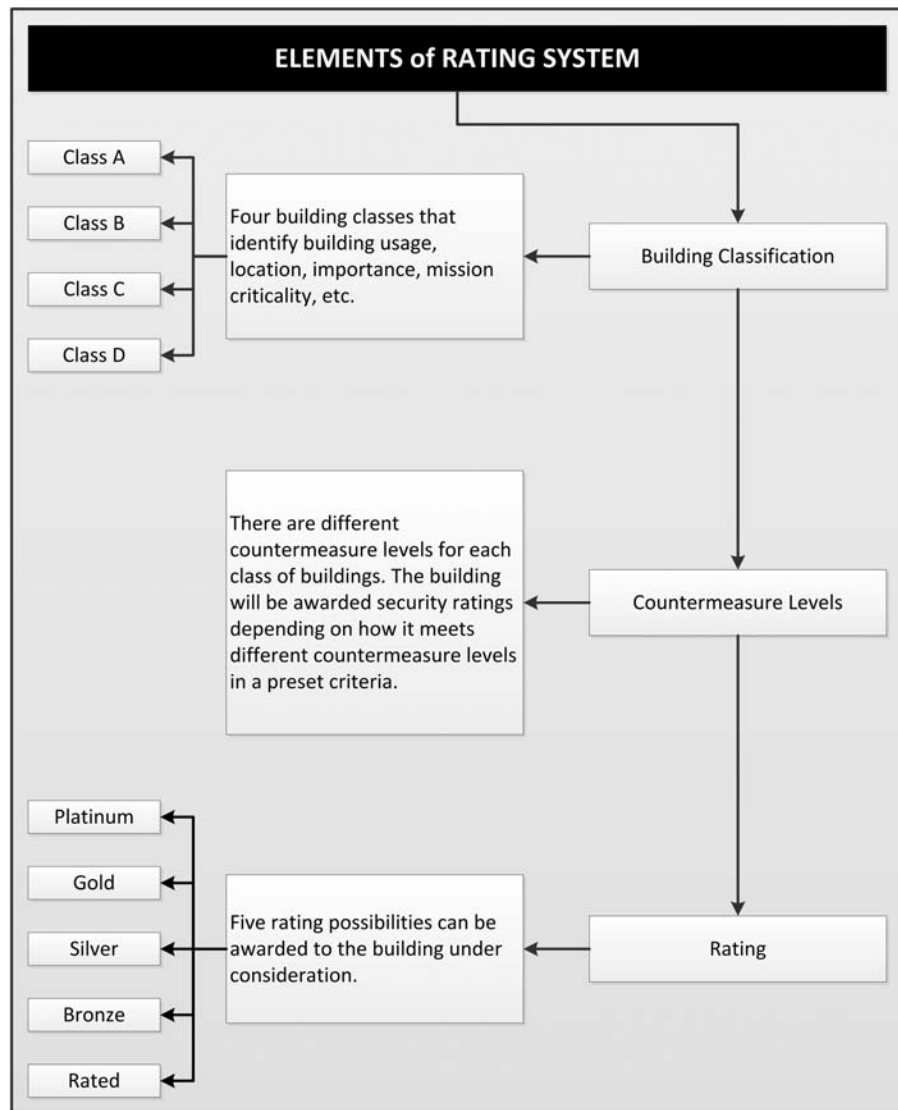


Fig. P-1. Elements of the Security Rating System.

To promote innovations in building security, the rating system includes extra points. Details are provided in Appendix C.

A security evaluation is a complex undertaking, because it covers several disciplines and relies heavily on the qualitative judgment of professionals. To help in standardizing and simplifying the rating system, comprehensive commentary is given in Appendixes D, E, F, G, and H. Finally, a comprehensive bibliography is supplied in the references.

In summary, this document describes a comprehensive method for rating building security. The method is straightforward and comprehensive and is based on the state of the art of building security. It is multidisciplinary, with appropriate representation of all disciplines factoring into building security. The methodology accounts for threat, effect, and mitigation as related to building security and, in doing so, provides a quantifiable measure of building security status: the building security rating. Knowledge of the building security rating can help building stakeholders assess the status of their building security in an objective manner. This rating will allow cost-effective building and public security improvements.

HISTORY OF THE BUILDING SECURITY RATING SYSTEM (BSRS)

Version 1.0 of the building security rating system was developed by Applied Research Associates, Inc., under the direction of the American Society of Civil Engineers (ASCE) Building Security Council (BSC) Rating System Development Committee.

Version 1.1 included several additions, changes, and rearrangements. The modifications were done as a result of the volunteer efforts of the BSC Rating System Development Committee. Version 1.1 was a draft document for review and testing. Versions 1.1 and 1.2 were used in a pilot-testing program.

Version 2.0 is the first version released to the public. Future versions will be issued by the AEI Building Rating System Committee (BRSC) as modifications dictate.

Both Versions 1.0 and 1.1 were named the PLUS system. In Version 2.0, the name of the system has been modified to *building security rating system (BSRS)*.

This page intentionally left blank

CHAPTER 1

Introduction

AEI, the Architectural Engineering Institute of ASCE, will develop and maintain a building security rating system (BSRS) that enables building owners to evaluate and improve the security of their facilities.

1.1 PURPOSE

The building security rating system was created to develop construction and operations criteria and a matching rating system to describe the relative security and safety of buildings and building systems, the objective being to enhance the security and safety of building mission and life safety services and thus the safety of building occupants. The rating system addresses the design, engineering, and construction disciplines (planning, architectural, structural, mechanical, electrical, heating, ventilation and air-conditioning, etc.) governing building design, development, and operations, while offering improved survivability of buildings and occupants when subjected to terrorist or criminal attacks involving nuclear, chemical, and biological agents or conventional explosives. The construction and operation criteria are part of a qualitative assessment engine used to govern building design and development, construction, and operations. The rating system is applicable to existing buildings and new building designs and guides owners and facility decision makers in improving survivability (or enhanced continued operations) after an attack. It also provides an indication of security value for facility owners and occupants that is analogous to the U.S. Green Building Council's LEED building rating system. Buildings are rated according to likely survivability, security, and safety given various degrees and types of terrorist or criminal assaults.

Note that in this rating system the term "security" is defined as *the capability to prevent terrorist or criminal attacks, reduce vulnerability to such events, and provide enhanced recovery from an event if one occurs. Consideration of life safety is at the forefront of prevention, mitigation, response, and recovery.*

1.2 BASIS

The rating system builds upon concepts present in other efforts and references.

1.2.1 LEED System

The former Building Security Council (BSC) was modeled after the U.S. Green Building Council (USGBC); however, it addressed security rather than sustainability. While the building security rating system maintains some elements of the LEED system, such as providing an indication of value for facility owners and occupants and categories named after precious metals, it diverges substantially by introducing risk and cost-benefit analysis into the rating methodology. The building security rating system recognizes that facilities have varying levels of risk and that all potential risk mitigation measures do not provide the same benefit. Therefore, the building security rating system introduces a sliding scale for rating a facility's security posture. Higher-risk buildings require more countermeasures in conjunction with the performance requirements of those countermeasures, based on the combined value of the countermeasures in mitigating the risk to the facility and the expense and/or effort required in implementing the countermeasures. This cost-benefit analysis provides a ranked countermeasure checklist with somewhat simple countermeasures at one end of the sliding scale and more complex countermeasures at the other, where the increased risk mitigation justifies the expense.

1.2.2 FEMA 426

The Federal Emergency Management Agency (FEMA) developed the *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings* (FEMA 426, 2003a) to provide information on how to mitigate the effects of potential terrorist attacks. The intended audience includes architects and engineers in private institutions and state and local

government officials working in the building sciences community. The objective of this manual is to reduce physical damage to structural and nonstructural components of buildings and related infrastructure and to reduce casualties during conventional bomb attacks and those using chemical, biological, and radiological (CBR) agents. Because of the similarity of goals, FEMA 426 was the primary reference for the building security rating system.

A fundamental difference, however, is that FEMA 426 asks a series of questions designed to determine a building's vulnerability, while the building security rating system provides countermeasures intended to measure a facility's security posture based on potential threats. The building security rating countermeasures are essentially answers to FEMA questions that are appropriate to a specific facility.

1.2.3 Other References

In addition to LEED and FEMA 426, many other references were used in developing the building security rating system. The countermeasures were developed based on references used across the security industry, the application of crime prevention through environmental design (CPTED) principles, and professional experience. These references supplemented and, in some cases, refined the countermeasures developed from FEMA 426 (2003a). Specific references used to determine countermeasures include

- FEMA risk management publications:
 - FEMA 426 (2003a),
 - FEMA 427 (2003b),
 - FEMA 452 (2005), and
 - FEMA 455 (2009);
- U.S. Department of Homeland Security (DHS) integrated rapid visual screening / risk assessment methodologies including
 - DHS (2009),
 - DHS (2011a)
 - DHS (2011b), and
 - DHS (2011c);
- Various risk assessment methodologies including
 - Federal security risk management (FSRM), and
 - Sandia National Laboratory's risk assessment methodology (RAM);

- Interagency Security Committee (ISC) security design criteria for new federal office buildings and major modernization projects; and
- Department of Defense (DoD) unified facilities criteria.

Most countermeasures used in the building security rating system appear in one or more of the reference documents and are common to the security and risk mitigation industry. However, the countermeasures do not always appear in these references with the same specificity and detail. For example, FEMA publications, various risk methodologies, and CPTED guidelines are intended for a general audience and, in most cases, do not provide specific performance requirements for recommended countermeasures. Federal design criteria provide specific performance requirements (based on risk) that are appropriate for federal or DoD facilities. In many cases, those countermeasures require substantial engineering design and analysis to implement.

The building security rating system seeks to strike a balance between the various reference documents and provides a simple-to-use checklist, appropriate for a wide variety of facilities, with a reasonable means of measuring adequacy. In some cases, where appropriate, the checklist includes the requirement for a more detailed risk or engineering level analysis to determine appropriate countermeasure development and performance.

While the building security rating system utilizes countermeasures from various federal and DoD references and criteria, the system is not a replacement for and does not constitute full compliance with any specific criteria.

1.3 THIS DOCUMENT

This document contains the complete description of the BSRS system. It includes a section on the methodology for classifying buildings according to potential threats and the consequences of an event, the list of specific countermeasures required for each level of relative security, the technique for determining the appropriate countermeasures for a specific building, and full commentary on the application of the countermeasures.

CHAPTER 2

Building Classification

The first step in the rating system is to classify buildings from a security viewpoint. All buildings are placed into one of four classes: A, B, C, or D. Four classes were chosen to provide a reasonable level of distinction between the threat to and impact of an event on different buildings without overly complicating the classification and, consequently, the rating process.

2.1 OVERVIEW

Class A facilities are typically large-occupancy, high-profile buildings that are attractive targets for a wide variety of attacks. They may also be one-of-a-kind facilities that would be difficult and/or impossible to replace in a reasonable timeframe. Additionally, these facilities are likely to be located in large metropolitan areas, near other high-profile targets or critical infrastructure, and face a high risk of collateral damage from one of these potential targets. Other attributes of Class A buildings might include being a public facility with many visitors or located in a high-crime area. Examples of Class A facilities include the New York Stock Exchange, the U.S. Capitol, or a facility that is a key piece of the U.S. power grid.

Class B facilities are usually slightly smaller and less populated than Class A buildings, or are less attractive targets. They may still exist in metropolitan areas and be located close to high-profile facilities, critical infrastructure, or industrial facilities. Examples of Class B facilities include a large federal building, a state capitol, a large hospital, or a nuclear power plant located in a rural area.

Class C facilities are generally moderate in size with limited occupancy (fewer than 450 occupants); are likely to be located in cities with fewer than 500,000 people; or do not present an attractive target for a large-scale attack. Examples of Class C facilities include commercial office buildings, apartment complexes, large shopping centers,

most large hotels and schools (unless they are close to other potential targets), local government buildings, and industrial plants in rural locations.

Class D facilities are typically small offices or buildings that are more likely to be targets of criminal activity such as burglary or vandalism. Examples of Class D facilities are an office with fewer than 100 people located in a city with fewer than 100,000 people, a small school located in a rural community, and a small shopping center.

The four building classes are used to determine the quantity and extent of the countermeasures required to protect the building and its occupants.

The following sections introduce how buildings are classified. The overall classification strategy is described first. Then classification system components are introduced. Finally, the mathematical description of the classification system is presented.

Currently, the rating system is limited to those structures specifically cited in the forward to FEMA 426 (2003a), namely, commercial office facilities, retail commercial facilities, light and industrial manufacturing facilities, health care facilities, local schools (K–12), and higher educational (university) facilities. Other infrastructure types, such as bridges, utilities, power generation plants, residential buildings, and places of public assembly such as stadia or amusement parks, are not covered by this rating system.

2.2 METHODOLOGY: GENERAL

Classifying buildings is a challenging task that must be performed as a part of an overall building evaluation scheme. In so doing, the following two questions must be asked:

1. What is the ultimate purpose of the building evaluation activity?
2. Are any other factors involved in the building evaluation, beyond the desired building classification?

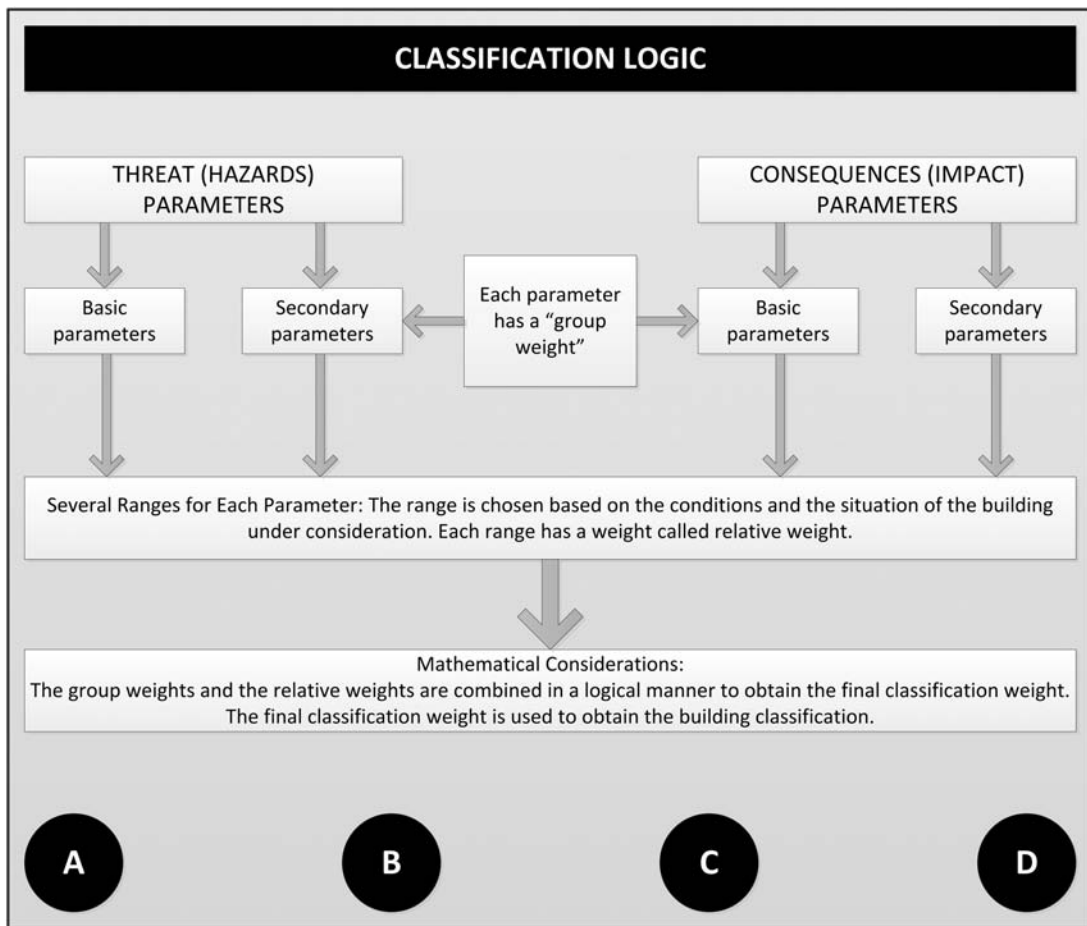


Fig. 2-1. Classification logic.

Based on the answers to these two questions, the building classification can be reasonably designated. For example, the evaluation of buildings for vertical loads in structural engineering is performed according to function (libraries, office buildings, residential buildings, etc.) and location (e.g., snow and wind loads) only. As soon as the building function is determined, the hazard (actual live load) and mitigation (acceptance limits) are determined. If the building function is a measure of the importance or impact of the building, it becomes clear that the process is an informal risk assessment. Within that process, the building classification represents only one part. In this structural engineering example, all three aspects (hazard, mitigation, and impact) are interconnected; that is, they are not independent.

In the field of building security, the interdependencies among these three parameters (hazard, mitigation, and impact) are not as tightly related as in the structural engineering example just provided. The current rating system subdivides the rating process into two parts: building classification and countermeasures. The countermeasures, obviously, provide mitigation parameters. The building

classification covers both the threat (hazard) and the consequence (impact) parameters. Although the parameters are generally discussed individually, they are interrelated, as will be discussed later. Fig. 2-1 shows the overall composition of the classification system.

2.3 GENERAL CLASSIFICATION APPROACH

The classification system is based on two parameters: the consequence (impact) parameter and the threat (hazard) parameter. The final classification considers the combined effect of both parameters. To determine both the level of impact and hazard for a particular building, a series of factors are evaluated. For each parameter, the factors are divided into primary (basic) and secondary groups. The primary group considers issues with a significant (or governing) effect on the level of impact or hazard. The secondary factors address issues of lesser significance to the impact or hazard. Each factor is evaluated with questions that have a range of answers. The possible answers vary by question from a simple binary choice (yes or no) to a long list of

building types. In addition, some questions require a numeric answer, while others are qualitative in nature and require considerable judgment on the part of the user.

An essential step in the classification system is converting the answers to numeric values. To do so, a relative weight that increases as the relative threat or consequence increases within the range is assigned to each possible choice for a given question. In addition, a group weight is assigned to factors under consideration. The total weight of the factor is the product of the relative weight times the group weight. Thus, for any given factor

$$\text{Factor weight} = \text{Relative weight} * \text{Group weight} \quad (2-1)$$

Note that the relative weight is chosen during the building's security assessment depending on the specifics of the property. The group weight is a preassigned weight that controls the overall relevancy of the factor under consideration. The preassigned group weights also reflect the difference between primary and secondary factors. Due to the essential nature of the primary factors, the group weights of the primary factors are considerably higher than the group weights of the secondary factors. Fig. 2-1 shows the logical relationships and hierarchy of the parameters, factors, and classification system.

2.4 PRIMARY HAZARD CLASSIFICATION FACTORS

Three factors are considered primary and thus have a significant effect on the hazard parameter:

1. **Building Functions (or Usage) and Threat Weights.**

Table 2-1 shows four building function categories based on the Building Occupancy Categories from ASCE 7-05 (2006). For each building function category, a hazard relative weight is assigned. Note that the weights range from 1 to 4, with a weight of 1 representing a low hazard level and a weight of 4 representing a maximum hazard level. The group weight is 18.75. Thus, the minimum weight of this factor is 18.75, while the maximum weight is 75. For buildings with multiple uses, select the building type corresponding to the most critical (highest relative weight) occupancy.

Note that Table 2-1 provides a general guideline only, and the relative weight values provided describe commonly held notions and assumptions for the given building type and function. For instance, typical assumptions for libraries, educational facilities, recreation centers, and such may distinguish these facilities as "vacant" during times of emergency and, correspondingly, might be assigned a somewhat low threat weight value. However, if the building is designated as a community emergency shelter, a higher threat weight must be assigned.

Recognizing that it would be impractical to describe every possible scenario, the Building Rating Security Committee (BRSC) determined that the rating would be optimized by the sound engineering judgment of the users. Therefore, it is the responsibility of the users to consider all operational and environmental factors and correspondingly validate and determine appropriate threat weight values.

When a need exists to deviate from the threat weights given in Table 2-1, the users need to keep a record of the following minimum information:

- a. Project identifiers;
- b. Users' identifiers and contact information;
- c. Affected table and item;
- d. Brief justification narrative; and
- e. Proposed value.

2. **Critical Infrastructure Association.** The second basic hazard factor is the building's association with critical U.S. infrastructures. Five qualitative choices are possible. They range from "very low" association to critical infrastructures to "very high" association to critical infrastructures, as shown in Table 2-2. Each association level is assigned a relative weight from 0 to 4 with the more critical infrastructure association assigned a higher weight. The group weight for this parameter is also 18.75. Thus, the maximum possible weight from this factor is 75 while the minimum weight is 0.

3. **Threat History.** This factor reflects the history of threats received the previous year and uses the number of those threats as an indication of the building's future threat exposure. Five weights are assigned, as shown in Table 2-3. Each range of threat values is assigned a relative weight from 0 to 4. If no threats occurred in the previous year, the relative weight is 0. If the number of threats in the previous year is 100 or more, the relative weight is 4. Because of the direct correlation between the actual threat and the threats received in the previous year, the group weight for this factor is also 18.75. Thus, the maximum possible weight for this factor is 75 while the minimum weight is 0.

2.5 SECONDARY HAZARD CLASSIFICATION FACTORS

Seven secondary hazard factors can have an effect on the final building classification. These secondary hazard factors are

1. **The VIP Factor.** The threat to a building increases as VIPs or celebrities reside, work in, or visit the building. Table 2-4 shows the binary (yes or no) possibilities and their relative weights (1 or 0). The group weight for this factor is 2.0. Thus, the minimum factor weight is 0, and the maximum weight is 2.

Table 2-1 Building Functions and Threat Weights

Building Type or Function	Categories / Relative Weight	Group Weight
All buildings except those listed in other categories.	1	
Buildings that represent a substantial hazard to human life in the event of failure, including, but not limited to • Buildings where more than 300 people congregate in one area; • Buildings with daycare facilities with a capacity greater than 150; • Buildings with elementary school or secondary school facilities with a capacity greater than 250; • Buildings with a capacity greater than 500 for colleges or adult education facilities; • Health care facilities with a capacity of 50 or more resident patients, but not having surgery or emergency treatment facilities; and • Jails and detention facilities.	2	
Buildings, not included in Category 3 or 4 (for simplicity, the value of relative weight is the same as the value of the building category), with potential to cause a substantial economic impact and/or mass disruption of day-to-day civilian life in the event of failure, including, but not limited to, telecommunication centers.		
Buildings not included in Category 3 or 4 containing sufficient quantities of toxic or explosive substances to be dangerous to the public if released, including, but not limited to, facilities that manufacture, process, handle, store, use, or dispose of such substances as hazardous fuels, hazardous chemicals, hazardous waste, or explosives.		18.75
Buildings and other structures designated as essential facilities, including, but not limited to • Hospitals and other health care facilities with surgery or emergency treatment facilities; • Fire, rescue, ambulance, and police stations and emergency vehicle garages; • Designated emergency shelters; • Designated emergency preparedness, communication, and operation centers and other facilities required for emergency response; • Public utility facilities required in an emergency; and • Buildings having critical national defense functions.	3	
Buildings containing highly toxic substances where the quantity of the material exceeds a threshold quantity established by the authority having jurisdiction, including, but not limited to, facilities that manufacture, process, handle, store, use, or dispose of such substances as hazardous fuels, hazardous chemicals, or hazardous waste.		
Buildings containing highly toxic substances shall be eligible for classification as Category 2 structures if it can be demonstrated by a hazard assessment that a release of the highly toxic substances does not pose a threat to the public. This reduced classification shall not be permitted if the buildings also function as essential facilities.		
Buildings with an essential national or local emergency response function.	4	

Table 2-2 Critical Infrastructure Association Factor

Infrastructure Association	Relative Weight	Group Weight
Very low	0	
Low	1	
Medium	2	18.75
High	3	
Very high	4	

Table 2-3 Threat History Factor

Number of Threats	Relative Weight	Group Weight
None	0	
1–5	1	
6–10	2	18.75
11–100	3	
>100	4	

Table 2-4 VIP Factor

VIP Factor	Relative Weight	Group Weight
Yes	1	2.0
No	0	

Table 2-5 Public Visitors Factor

Number of Public Visitors	Relative Weight	Group Weight
<20	0	1.5
20–49	1	
50–99	2	
100–300	3	
>300	4	

Table 2-6 City Population Factor

Population	Relative Weight.	Group Weight
<100,000	0	1.0
100,000–500,000	1	
500,001–1 million	2	
>1 million	3	

- Public Visitors Factor.** The threat to a building increases with an increased number of public visitors. Table 2-5 shows five ranges of weights corresponding to the number of public visitors to the facility, ranging from fewer than 20 to more than 300 per day. The relative weight ranges from 0 to 4. The group weight for this factor is 1.5. Thus, the minimum weight of this factor is 0, while the maximum weight is 6.
- City Population Factor.** The threat to a building increase as the city population increases. Table 2-6 shows four city population ranges, from a population of fewer than 100,000 to a population of more than 1 million. The relative weight is assigned in increasing order from 0 to 3. The group factor weight is 1.0. Thus, the minimum factor weight is 0, while the maximum weight is 3.
- Distance to Hazardous Materials/Transportation Routes.** The threat to a building increases if the building is located near a hazardous material storage site. Additionally, if the building or facility is located near a hazardous material transportation route, the threat to the facility increases. This is due to the possibility of hazardous material being released or bomb explosions from cars or trucks traveling along the transportation route. Table 2-7 shows five ranges of distances from

Table 2-7 Distance to Hazardous Materials/Transportation Routes Factor

Distance to Hazardous Materials or Trans. Rte. (ft)	Relative Weight	Group Weight
>1,000	0	1.0
501–1,000	1	
101–500	2	
6–100	3	
0–5	4	

Note: 1 ft = 0.3048 m.

Table 2-8 Distance to High-Profile Buildings Factor

Distance to High-Profile Buildings (ft)	Relative Weight	Group Weight
>1,000	0	1.0
501–1,000	1	
101–500	2	
10–100	3	
0–10	4	

Note: 1 ft = 0.3048 m.

- Distance to High-Profile Buildings.** The threat to a building increases if the building is located near one or more high-profile buildings. This is due to the possibility of collateral damage if the adjacent high-profile buildings are attacked. Table 2-8 shows five ranges of distances from the building site to a high-profile building. The distance ranges from 0 m to 305 m (0 ft to more than 1,000 ft). The relative weight ranges from 0 to 4. The group weight for this factor is 1.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 4.
- Gang Activities.** The threat (hazard) to the building increases if there is known gang activity in the area or if the building is located in a high crime area. For this factor (Table 2-9) the choices are binary (yes or no). The relative weights are 1 or 0, respectively. The group weight for this factor is 2.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 2.

Table 2-9 Gangs or Criminal Activities Factor

Gangs or Criminal Activities Parameter	Relative Weight	Group Weight
Yes	1	2.0
No	0	

Table 2-10 Proximity to Law Enforcement Factor

Law Enforcement Proximity	Relative Weight	Group Weight
Yes	1	4.0
No	0	

Table 2-11 National Symbolism or Prominence Factor

National Prominence	Relative Weight	Group Weight
Very low	0	18.75
Low	1	
Medium	2	
High	3	
Very high	4	

7. **Proximity to Law Enforcement Agencies.** If a building is located near a law enforcement agency such as a police station, the threat to the building increases. Also, if a law enforcement agency is a tenant in the building, the threat to the building increases. For this factor (Table 2-10) the choices are binary (yes or no). The relative weights are 0 or 1, respectively. The group weight for this factor is 4.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 4.

2.6 PRIMARY IMPACT/CONSEQUENCE CLASSIFICATION FACTORS

Four primary classification factors relate to the impact (or consequences) of losing building functions.

1. **National Symbolism or Prominence.** The first of these factors is the national symbolic function or the national prominence of the building. For example, the Statue of Liberty or the New York Stock Exchange would rank very high for this factor. As shown in Table 2-11, this factor has five relative weights. The values range from very low with a relative weight of 0 to very high with a relative weight of 4. The group

Table 2-12 National Political Significance Factor

National Political Significance	Relative Weight	Group Weight
Very low	0	18.75
Low	1	
Medium	2	
High	3	
Very high	4	

Table 2-13 Local Economic Significance Factor

Local Economic Significance	Relative Weight	Group Weight
Very low	0	18.75
Low	1	
Medium	2	
High	3	
Very high	4	

weight for this factor is 18.75. Thus, the maximum weight of this factor is 75, while the minimum weight is 0.

2. **National Political Significance.** The next primary factor is the national political significance of the building. For example, the White House in Washington, D.C., or an abortion clinic would rank very high. As shown in Table 2-12, this factor has five relative ranges. The values range from very low with a relative weight of 0 to very high with a relative weight of 4. The group weight of this factor is 18.75. Thus, the maximum weight of this factor is 75, while the minimum weight is 0.
3. **Local Economic Significance.** The next primary factor is the local economic significance of the building with respect to its primary function. For example, a large employer, financial institution, or tax revenue generator would rank very high. As shown in Table 2-13, this factor has five values. The values range from very low with a relative weight of 0 to very high with a relative weight of 4. The group weight of this factor is 18.75. Thus, the maximum weight of this factor is 75, while the minimum weight is 0.
4. **Infrastructure or Transportation Utility.** The final primary factor is the infrastructure or transportation utility of the building. For example, transportation hubs or control facilities of major bridges or tunnels would rank very high. As shown in Table 2-14, this parameter has five values. The values range from very

Table 2-14 Infrastructure or Transportation Utility Factor

Infrastructure or Transportation Utility	Relative Weight	Group Weight
Very low	0	18.75
Low	1	
Medium	2	
High	3	
Very high	4	

Table 2-15 Child Care Factor

Child Care Facility is Present	Relative Weight	Group Weight
Yes	1	1.0
No	0	

low with a relative weight of 0 to very high with a relative weight of 4. The group weight for this factor is 18.75. Thus, the maximum weight of this factor is 75, while the minimum weight is 0.

2.7 SECONDARY IMPACT/CONSEQUENCE CLASSIFICATION FACTORS

Six secondary impact or consequence factors can have an effect on the final building classification. These secondary factors are

1. **Child Care Factor.** The impact or consequence of the loss of the function of the building increases if the building is or includes a child care facility. For this factor, shown in Table 2-15, the choices are binary (yes or no). The relative weights are 0 or 1, respectively. The group weight for this factor is 1.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 1.
2. **Occupancy Factor.** The impact or consequence of the loss of a facility with high occupancy is much higher than that if the building or facility has a low occupancy. Table 2-16 shows four ranges of building occupancy, from fewer than 10 people (on average) to more than 450 people (on average). The relative weight ranges from 0 to 3. The group weight for this factor is 1.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 3.
3. **Building Size Factor.** The impact or consequence of the loss of a large facility (as measured by total floor area) is much higher than if the facility is small. Table 2-17 shows four ranges of building floor area,

Table 2-16 Occupancy Factor

Building Occupancy	Relative Weight	Group Weight
<10	0	1.0
10–150	1	
151–450	2	
>450	3	

Table 2-17 Building Size Factor

Building Area (sq ft)	Relative Weight	Group Weight
<2,500	0	1.0
2,501–80,000	1	
80,001–150,000	2	
>150,000	3	

Note: 1 sq ft = 0.0929 sq m.

Table 2-18 Public Visitors Factor

Number of Daily Public Visitors	Relative Weight	Group Weight
<20	0	1.5
20–49	1	
50–99	2	
100–300	3	
>300	4	

from an area less than 232 sq m (2,500 sq ft) to areas of more than 150,000 sq ft (13,935 sq m). The relative weight ranges from 0 to 3. The group weight for this factor is 1.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 3.

4. **Public Visitors Factor.** The impact or consequence of the loss of a facility increases when the number of public visitors increases. Table 2-18 shows five ranges of the number of public visitors to the facility, from fewer than 20 to more than 300 per day. The relative weight ranges from 0 to 4. The group weight for this factor is 1.5. Thus, the minimum weight of this factor is 0, while the maximum weight is 6. Note that this factor is also included as a secondary factor for the threat effects on building classification. This is in recognition that the presence of public visitors can be both a threat and a consequence.
5. **Historic Status Factor.** The impact or consequence of the loss of a historically designated building should be included in any building classification, because it would be difficult (in some cases impossible) to

Table 2-19 Historic Status Factor

Does the Building Have a Historic Designation?	Relative Weight	Group Weight
Yes	1	2.0
No	0	

Table 2-20 Overall Impact Factor

Overall Impact Parameter	Relative Weight	Group Weight
Low	0	2.0
Medium	1	
High	2	

replace such a building. For this factor, shown in Table 2-19, the choices are binary (yes or no). The relative weights are 1.0 or 0.0, respectively. The group weight for this factor is 2.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 2.

6. **Overall Impact Factor.** The purpose of this factor is to represent the overall impact on the major tenant organizations if the facility is destroyed or damaged beyond use for an extended period of time. A significant loss of business would carry a high weight. Table 2-20 shows three qualitative ranges (low, medium, and high) that describe the overall impact. The relative weight ranges from 0 to 2. The group weight for this factor is 2.0. Thus, the minimum weight of this factor is 0, while the maximum weight is 4.

2.8 MATHEMATICAL EVALUATION OF BUILDING CLASSIFICATION

The factors defined in the previous sections are evaluated and assigned numerical values. These values must be combined in a meaningful way to determine the building classification. This section explains the mathematical process by which the classification is obtained. For a given factor, i , and its range, j , the relative weight is defined as RW_{ij} . Similarly, the group weight is identified for the factor i as GW_i . Thus the total weight for each factor is computed as

$$TW_i = RW_{ij}GW_i \quad (2-2)$$

Note that Eq. (2-2) is the formal representation of Eq. (2-1).

Using Table 2-1 through Table 2-20, the total weight for each of the 20 factors, TW_i , can be calculated. Note that the subscript $i = 1 \dots 20$ is distributed as shown in Table 2-21.

The next step is to compute the aggregate weights of the primary hazard (threat) factors, secondary hazard (threat)

Table 2-21 Counters i and Their Uses

Counter	Comment
$i = 1 \dots 3$	Primary hazard (threat) factors (total of 3 factors)
$i = 4 \dots 10$	Secondary hazard (threat) factors (total of 7 factors)
$i = 11 \dots 14$	Primary impact (consequence) factors (total of 4 factors)
$i = 15 \dots 20$	Secondary impact (consequence) factors (total of 6 factors)

Table 2-22 Values of Scaling Factors

i	TWM_i
4	2
5	6
6	3
7	4
8	4
9	2
10	4
15	1
16	3
17	3
18	6
19	2
20	4

factors, primary impact (consequence) factors, and secondary impact (consequence) factors, PT , ST , PC , and SC , respectively, as follows:

$$PT = MAX(TW_1, TW_2, TW_3) \quad (2-3)$$

$$ST = 100 \frac{\sum_{i=4}^{i=10} TW_i}{\sum_{i=4} TWM_i} \quad (2-4)$$

$$PC = MAX(TW_{11}, TW_{12}, TW_{13}, TW_{14}) \quad (2-5)$$

$$SC = 100 \frac{\sum_{i=15}^{i=20} TW_i}{\sum_{i=15} TWM_i} \quad (2-6)$$

where TWM_i = the maximum possible total weight for a given i , as shown in Table 2-22.

Note that the use of the *MAX* function for the primary factors results in an equal effect for each factor. In such a case, the higher weight of the factor governs the value of the total weight. If a summation had been used instead, the lower factor weights would result in a lowering of the final weight, clearly an undesirable result.

The denominators in Eqs. (2-4) and (2-6) are scaling factors that contain the maximum possible value for each factor i as shown in Table 2-22. This results in a percentage score for the aggregate secondary threat and consequence factors. From Table 2-22, the value of the dominators in Eqs. (2-4) and (2-6) are 25 and 19, respectively.

Eqs. (2-4) and (2-6) can now be expressed as

$$ST = 100 \frac{\sum_{i=4}^{i=10} TW_i}{25} \quad (2-7)$$

$$SC = 100 \frac{\sum_{i=15}^{i=20} TW_i}{19} \quad (2-8)$$

The primary threat and consequence factors are combined using a square root of the sum of the squares (SRSS) approach, resulting in a primary parameter weight:

$$W_{PRIMARY} = MIN\left(100, \sqrt{PT^2 + PC^2}\right) \quad (2-9)$$

Table 2-23 Final Building Classification

Final Classification Weight, W_{FINAL}	Building Classification
$W_{FINAL} \geq 75$	A
$50 \geq W_{FINAL} < 75$	B
$25 \geq W_{FINAL} < 50$	C
$W_{FINAL} < 25$	D

The use of the *MIN* function in Eq. (2-9) limits the value of $W_{PRIMARY}$ to 100.

Given the uncertain nature of the variables and their occurrences, the SRSS method for combining the effects of *PT* and *PC* provides a reasonable empirical approach.

The secondary factors are combined in a similar fashion to obtain the secondary parameter weight:

$$W_{SECONDARY} = MIN\left(100, \sqrt{ST^2 + SC^2}\right) \quad (2-10)$$

The use of the *MIN* function in Eq. (2-10) limits the value of $W_{SECONDARY}$ to 100.

The final classification weight can then be expressed as

$$W_{FINAL} = 0.75W_{PRIMARY} + 0.25W_{SECONDARY} \quad (2-11)$$

The final classification of the building can then be obtained from the final classification weight, W_{FINAL} , using Table 2-23.

This page intentionally left blank

CHAPTER 3

Countermeasure Evaluation

As discussed in Chapter 2, the building classification system is based on three pillars. The first two are threat and impact or consequence. The third pillar of building security, mitigation measures or countermeasures, is the subject of this section.

3.1 OVERVIEW

Generally speaking, each building class has a corresponding security rating level of potential countermeasures used to evaluate the security posture of a facility. Because the building security rating system must represent a wide variety of buildings, the countermeasures represent some level of risk acceptance and are thus considered to be practically achievable within their respective classes. It is assumed that the facility owner has the ability to accomplish or implement all the countermeasures. Such measures as moving a facility, closing streets, protecting against aircraft attacks, and so on, are not included because they cannot be realistically implemented by all facility owners. Although these measures are not considered part of the official rating system, these measures and others like them are innovative examples that can be used to reward building owners and give them credit in meeting their security goals. Ultimately, the rating system and countermeasures listed here are performance based and are intended to achieve a desired security goal.

Fig. 3-1 shows the countermeasure checklist system. The overall level system is discussed first, followed by the levels of countermeasures. As noted in the Fig. 3-1, countermeasure level determined in this section is combined with building class discussed in Chapter 2 to determine building system rating (Rated, Bronze, Silver, Gold, or Platinum) described in Chapter 4.

3.2 COUNTERMEASURE LEVELS

Many security countermeasures can be applied to a building to enhance its security. Some of the countermeasures are

basic and suitable to building Class D. Some countermeasures are demanding and are needed only for more sensitive building classes, such as Class A. In recognition of this, the security countermeasures were divided into five levels, according to the degree of protection they provide. The most basic level is the rated level (level 1). A rated level provides a basic security protection for the building. The four additional levels of protection are levels 2 through 5; level 2 provides the lowest protection level (even though level 2 still provides higher protection than a rated level 1). Levels 3, 4, and 5 provide increasing levels of protection, with level 5 providing the maximum protection.

Countermeasure levels interact closely with building classifications in the building rating process. This interaction is described in the next section, which presents the layout of the countermeasure levels.

3.3 LAYOUT OF LEVELS

All five levels of countermeasures have a similar layout. Each level is subdivided by security discipline into 13 groups, as shown in Table 3-1.

The 13 checklist disciplines are the same as those of FEMA 426 (2003a) and are based on common physical security principles. Each discipline has a certain number of countermeasures that relate to the discipline. The countermeasures increase in their demands as the security level increases. For example, the rated level (level 1) covers the least demanding countermeasures; next, level 2 covers more demanding countermeasures, and so on. The most demanding level is level 5. Rating class, countermeasure requirements for each rating level, and corresponding countermeasure checklists are given in Appendix B.

The step-by-step procedure for each level is executed as follows:

1. For a given level and a given discipline, i , the professional evaluates each countermeasure, j . The result of the evaluation takes the form of a drop-down list with

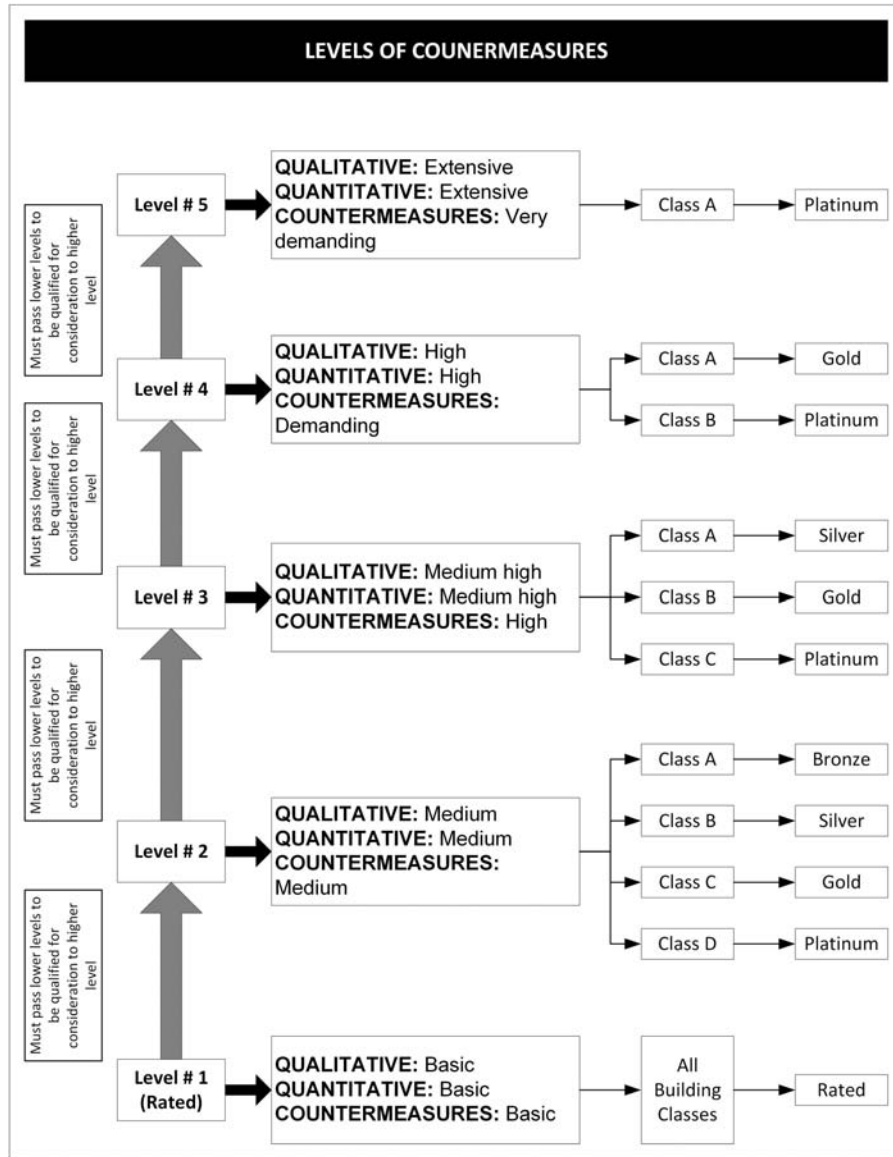


Fig. 3-1. Layout of the levels system.

preset choices; each choice has a preset weight, w_{ij} . Note that $0 \leq w_{ij} \leq 1.0$. In certain situations, no numerical value is given for the choice. One of these situations is when the countermeasure is *required*. The other situation is when the countermeasure is *not applicable* (N.A.) to the condition being investigated. Both situations will be discussed in more detail later in this section. Different preset drop-down lists and their preset weights, w_{ij} , are shown in Tables 3-2, 3-3, 3-4, and 3-5.

- Each countermeasure j has a constant, preassigned weight, W_{ij} , that reflects the relative importance of that countermeasure relative to other countermeasures in discipline i . The values for W_{ij} are shown in Tables

(3-6)–(3-10) for the five levels. Note that an R in a table indicates that the countermeasure is required for this level; as such the weight is considered infinite. The required countermeasures are discussed later in this section.

- The product $w_{ij}W_{ij}$ represents the relative weight of the j^{th} countermeasure in discipline i for the building being considered. The value W_{ij} represents the maximum possible relative weight that countermeasure j can attain (this implies $w_{ij} = 1.0$).
- For each discipline, i , there are two representative weights, the actual summation of the discipline weight, A_i , and the maximum possible summation of the discipline weight, T_i . They are computed as

Table 3-1 Disciplines of Each Countermeasure Level

Numbering System (Consistent with FEMA 426)	Discipline
1	Site
2	Architectural
3	Structural
4	Building envelope
5	Utilities
6	Mechanical
7	Plumbing and gas
8	Electrical
9	Fire
10	Communications and IT
11	Equipment operations and maintenance
12	Security systems
13	Security master plan

Table 3-2 Required Drop-Down List

Choice	w_{ij}
1 None	Fail
2 Full	Pass
3 N.A.	N.A.

Table 3-3 Binary Drop-Down List

Choice	w_{ij}
1 None	0
2 Full	1
3 N.A.	N.A.

Table 3-4 Three-Level Drop-Down List

Choice	w_{ij}
1 None	0
2 Medium	0.5
3 Full	1
4 N.A.	N.A.

Table 3-5 Five-Level Drop-Down List

Choice	w_{ij}
1 None	0
2 Low	0.25
3 Medium	0.5
4 High	0.75
5 Full	1
6 N.A.	N.A.

Table 3-6 Values of W_{ij} for Level 1 (Rated)

Discipline		Countermeasure Counter						
		1	2	3	4	5	6	7
1	Site	R	R	R	R	1	1	1
2	Architectural	1	1	1	1	1	1	
3	Structural	R	R	R				
4	Building envelope	2	2	4				
5	Utilities	R	R					
6	Mechanical	1	1	1				
7	Plumbing and gas	0						
8	Electrical	0						
9	Fire	0						
10	Communications and IT	0						
11	Equipment operations and maintenance	2						
12	Security systems	3	1	R	1	1		
13	Security master plan	R						

Table 3-7 Values of W_{ij} for Level 2

[illegible]

Table 3-8 Values of W_{ij} for Level 3

[illegible]

Table 3-9 Values of W_{ij} for Level 4

[illegible]

Table 3-10 Values of W_{ij} for Level 5

[illegible]

Table 3-11 Values of N_i for Different Disciplines and Levels

Discipline		Level 5	Level 4	Level 3	Level 2	Level 1 (Rated)	Total # of Countermeasures per Discipline
1	Site	3	9	2	11	7	32
2	Architectural	1	13	8	14	6	42
3	Structural	9	19	6	6	3	43
4	Building envelope	3	8	2	5	3	21
5	Utilities	4	11	6	2	2	25
6	Mechanical	14	7	3	4	3	31
7	Plumbing and gas	2	3	2	0	0	7
8	Electrical	0	0	4	1	0	5
9	Fire	1	5	6	0	0	12
10	Communications and IT	1	4	1	1	0	7
11	Equipment operations and maintenance	2	3	1	2	1	9
12	Security systems	4	10	18	10	5	47
13	Security master plan	2	5	6	2	1	16
Total number of countermeasures per level		46	97	65	58	31	297

$$A_i = \sum_{j=1}^{j=N_i} w_{ij} W_{ij} \quad (3-1)$$

$$T_i = \sum_{j=1}^{j=N_i} W_{ij} \quad (3-2)$$

The total number of countermeasures for the i^{th} discipline is N_i . The values of N_i are shown in Table 3-11.

5. Each discipline, i , within a security level has a preassigned relative weight. The purpose of the discipline relative weight, WDT_i , is to balance relative security countermeasures among different disciplines within the level. The relative actual weight and maximum possible weight for each discipline, i , are represented by the products $WDT_i A_i$ and $WDT_i T_i$, respectively. Table 3-12 shows the preassigned discipline weights for all levels.
6. The actual total building security score for the level under consideration, S_{ACTUAL} , and the maximum possible building security score for the same level, $S_{MAXIMUM}$, can be computed as

$$S_{ACTUAL} = \sum_{i=1}^{i=13} WDT_i A_i \quad (3-3)$$

$$S_{MAXIMUM} = \sum_{i=1}^{i=13} WDT_i T_i \quad (3-4)$$

The actual-to-maximum score ratio for the level

$$\alpha = \frac{S_{ACTUAL}}{S_{MAXIMUM}} \quad (3-5)$$

is of particular importance in the rating system. It is used in evaluating the adequacy of the security of the building within a particular security level. Note that $0 \leq \alpha \leq 1.0$. A higher security status is approached when $\alpha \rightarrow 1.0$. Conversely, when $\alpha \rightarrow 0.0$, a lower security status is approached.

It is important to discuss in more detail the *required* and the *not applicable* (N.A.) situations for a countermeasure.

3.4 REQUIRED COUNTERMEASURES

Several countermeasures in each level are required. A required countermeasure is an essential countermeasure that must be implemented to pass that level. Required countermeasures do not have assigned weights; thus, they do not contribute to the computations in Eqs. (3-1)–(3-5). However, if the building fails to satisfy any required countermeasure, the building will not pass that level; this makes any computation of a security score irrelevant. Table 3-13 shows the number of required countermeasures for different levels.

3.5 NOT APPLICABLE COUNTERMEASURES

The building rating system was developed to be as general as possible. In some situations, this generality results in countermeasures that do not apply to a particular building. The rating system accommodates these situations by introducing a not applicable (N.A.) choice for that particular countermeasure. An N.A. selection does not contribute

Table 3-12 Discipline Relative Weights, WDT_i

Numbering System (Consistent with FEMA 426)	Discipline	Level 5	Level 4	Level 3	Level 2	Level 1 (Rated)
1	Site	6	14	1	10	3
2	Architectural	3	17	5	17	7
3	Structural	11	43	12	9	0
4	Building envelope	6	15	13	14	8
5	Utilities	16	48	26	10	0
6	Mechanical	68	15	5	9	3
7	Plumbing and gas	2	5	2	0	0
8	Electrical	0	0	12	5	0
9	Fire	5	16	27	0	0
10	Communications and IT	5	20	2	5	0
11	Equipment operations and maintenance	2	5	3	3	2
12	Security systems	9	15	28	11	6
13	Security master plan	2	5	3	3	0

Table 3-13 Number of Required Countermeasures

Level 5	Level 4	Level 3	Level 2	Level 1 (Rated)
5	5	11	6	11

numerically to Eqs. (3-1)–(3-5). It is recommended that the N.A. selection be used carefully, because it can bias the final security rating. When selecting N.A. from the menu, a detailed written explanation should be provided.

3.6 INTERRELATIONSHIPS AMONG COUNTERMEASURES

Where a countermeasure requires a set parameter, such as setback distance, the user of the rating system may consider using that countermeasure if some direct action or design has been included that substitutes for the given parameter, such as structural hardening instead of setback distance. Future versions of the rating system will address this equivalence by linking appropriate countermeasures in an automatic and logical manner.

This page intentionally left blank

CHAPTER 4

Building Security Rating

The final step of the security rating system is combining the building classification and the security countermeasures. Such a combination ensures that the security rating accommodates all three important issues: threat, consequence (the components of the classification system), and countermeasures (the components of the countermeasure level system).

4.1 OVERVIEW

This chapter combines the building classification described in Chapter 2 and the security countermeasure levels described in Chapter 3 in a systematic fashion.

4.2 DESCRIPTION OF RATING CATEGORIES

The combined security rating system is subdivided into five categories: Platinum, Gold, Silver, Bronze, and Rated. Fig. 4-1 shows schematically the interaction among building security ratings, building classes, and countermeasure levels.

Note that for a given building class, say Class C, the countermeasure level increases as the building security rating increases. Similarly, for a given building rating category, say a Silver rating, the countermeasure level increases as the building classification increases.

4.2.1 Rated

This category is best described as a minimum baseline that is appropriate for all facilities regardless of the specific risk to that facility. Although only one countermeasure in the Rated category references a building code, the countermeasures in this category can be viewed in the same spirit as code requirements and should be considered the minimum standards that all building owners should strive to achieve.

Many countermeasures in this category are good safety and emergency planning practices that will improve pre-

paredness for a wide variety of scenarios (such as fire, natural hazards, and accidents) as well as security. Other countermeasures are considered to be relatively inexpensive crime prevention through environmental design (CPTED) measures. Overall, a minimum level of protection against forced entry (robbery and burglary), vandalism, and assault are achieved.

4.2.2 Bronze

In addition to increasing protection against the threats and tactics initially addressed in the Rated category, this category begins addressing some of the more severe terrorist tactics such as bombings and chemical, biological, and radiological (CBR) attacks. This category includes some of the more expensive CPTED measures, substantial site planning to control pedestrian and vehicular movement, and architectural planning to strategically locate building functions and systems. Additionally, more comprehensive emergency management planning measures are included in this category. Overall, a low level of protection against forced entry (robbery and burglary), vandalism, and assault are achieved and a minimum level of protection against threats such as hand-delivered bombs, mail bombs, vehicle bombs, hand-delivered weapons of mass destruction (WMDs), and airborne WMDs.

4.2.3 Silver

This category continues to incrementally increase the level of protection against the threats and tactics addressed by the previous categories. Specifically, intrusion detection systems become increasingly more detailed and comprehensive and facility hardening (against blast events) is first addressed. In this category, emergency management planning is optimized with the development of occupant emergency plans, command centers, and other preparedness and response planning. This category also substantially increases the

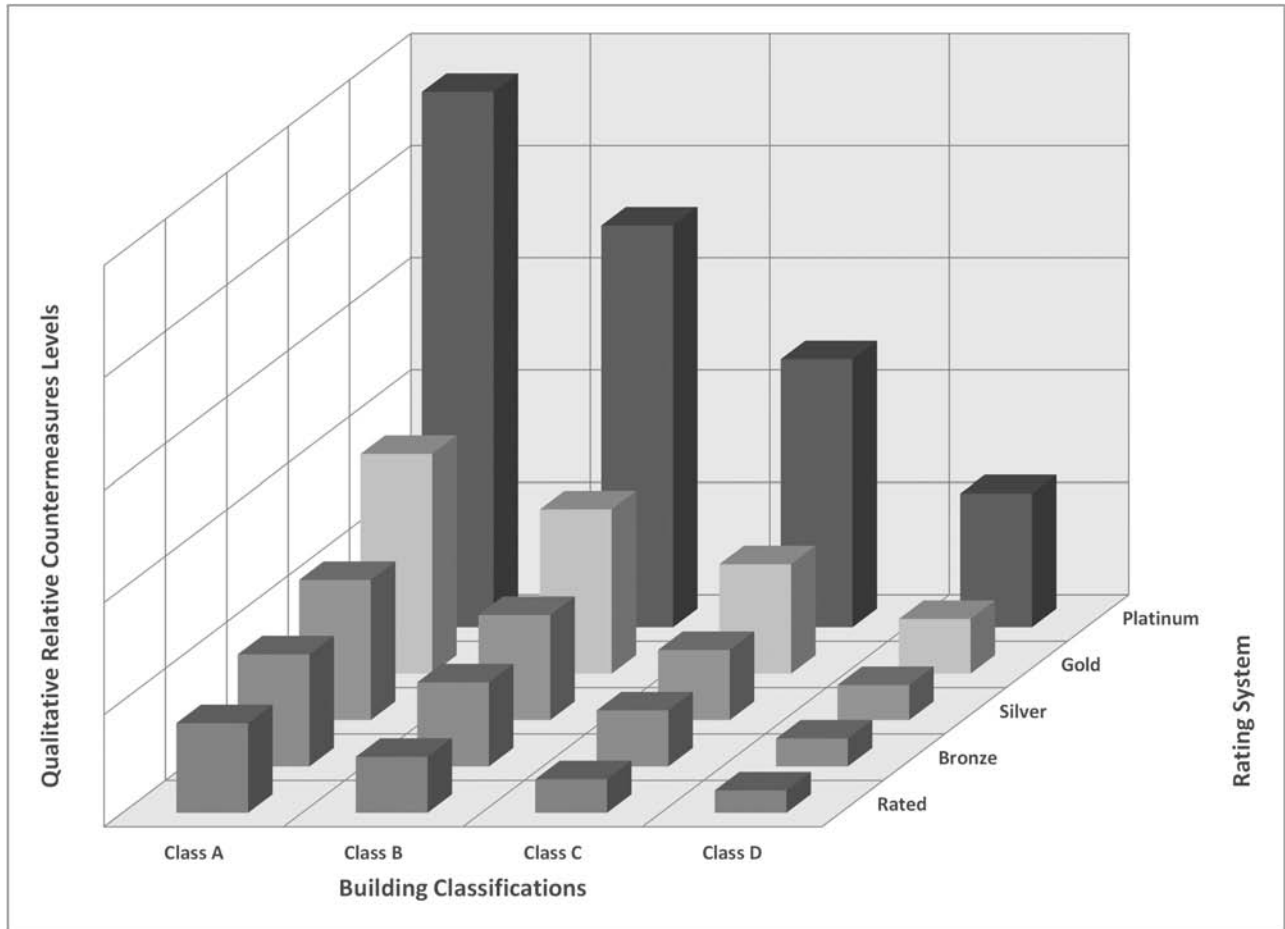


Fig. 4-1. Relationship among rating system categories, building classifications, and countermeasure levels; note: countermeasure axis is only schematic, not to scale.

security operational policies and procedures to support the increased physical countermeasures. Finally, this category requires a facility risk assessment, blast analysis, and fire analysis to quantify the consequences of potentially successful attacks and overall facility vulnerability. A medium level of protection against forced entry (robbery and burglary), vandalism, and assault and a low level of protection against threats such as hand-delivered bombs, mail bombs, vehicle bombs, hand-delivered WMDs, and airborne WMDs are achieved.

4.2.4 Gold

In this category, intrusion detection, access control, and closed-circuit television (CCTV) systems have been maximized for detection, surveillance, and assessment. The facility hardening has increased, and the available standoff has been protected. Security systems, operational procedures, and architectural features have been implemented to screen and control access of staff and visitors throughout the facility. Finally, the facility now employs some initial

countermeasures intended to mitigate the effects of waterborne contaminants. Overall, a high level of protection against forced entry (robbery and burglary), vandalism, and assault and a medium level of protection against hand-delivered bombs, mail bombs, vehicle bombs, hand-delivered WMDs, airborne WMDs, and waterborne WMDs are achieved.

4.2.5 Platinum

The Platinum rating should be considered an exemplary standard that is achieved by few facility owners other than the federal government in the higher building classifications. This is considered the highest level of security (based on risk) that building owners should be expected to achieve to protect the facility, the staff, and the visitors within. In this category the facility has been hardened to actual loads (based on the risk assessment) with the structural system specifically designed to protect against progressive collapse. Additionally, ballistic resistance is required for high-risk areas. A CBR analysis has been performed to optimize the

facility's protection against such attacks through additional countermeasures and operational procedures. Further, additional countermeasures to mitigate waterborne attacks have been implemented. Finally, all pedestrians and vehicles are controlled on the site and in the facility through additional physical countermeasures and operational procedures. Overall, a high level of protection has been achieved by the facility against credible threats and tactics.

4.3 RATING SYSTEM PHILOSOPHY

The rating categories are based on layers of security and are similar to the level of protection (LOP) designation required for the implementation of federal security design criteria such as the ISC Security Design Criteria and the Department of Defense (DoD) Unified Facilities Criteria. These criteria require the LOP to determine which countermeasures (or performance requirements of those countermeasures) are appropriate for a facility based on the specific risk to the facility. The building security rating system is similar in that as the building class and rating category increase, the number of required countermeasures increases in conjunction with the performance requirements of countermeasures.

The increase of ranking of the countermeasure rating system (Rated to Bronze, Bronze to Silver, Silver to Gold, and Gold to Platinum) is based on the combination of two factors:

- The benefit of the countermeasures in mitigating the risk to the facility, and
- The expense and/or effort required to implement the countermeasures.

Generally, this cost-versus-benefit analysis provides a ranked countermeasure checklist with somewhat inexpensive countermeasures at the Rated end of the spectrum and more expensive countermeasures at the Platinum end, where the increased risk mitigation justifies the expense.

The Rated category is a minimum baseline of security that all minimally secured buildings require. Beyond this, additional layers of security are provided in the higher categories to address increased risks. Class A facilities have inherently higher risks that create the need for additional layers of security, while the other classes require fewer layers of security. A Class D facility has adequate protection with two layers of security. In each class, determining an acceptable level of security for a building should be evaluated in the context of Rated, which is considered the minimum baseline appropriate for all facilities regardless of the specific risk to that facility. As noted earlier, the countermeasures in the Rated category should be considered the minimum standards that all building owners should strive to achieve while the Platinum rating should be considered an exemplary standard that would be achieved by few facility owners other than the federal government in the higher building classifications.

A Class A building with a Platinum rating has a very extensive list of countermeasures. The intermediate rating levels of Bronze, Silver, and Gold provide logical intervals within the spectrum to allow building owners to assess the risk and choose their desired security goals given a level of acceptable risk. Each interval contains a manageable number of countermeasures that will produce an appropriate level of protection for a reasonable expense. Moving down in building classification and building rating, the number of intervals decreases with the number of required countermeasures. Additionally, each category represents a general "level of protection" achieved against certain threats and tactics. However, it should be noted that certain threats and tactics can be mitigated at various degrees and that some level of protection against most threats and tactics exists in each category.

4.4 PROCESS OF RATING BUILDING SECURITY

This section will now discuss the actual process of rating a building with a given classification. Fig. 4-1 shows how the security rating relates to the building classification and the countermeasure levels. There are four building classifications, five countermeasure levels, and five possible security rating outcomes. All of these issues need to be related together in a logical manner.

The rating process starts with classifying the building (A through D). In addition the desired security rating (Rated through Platinum) is specified. Thus, two items are needed to start the process, CL_i and RT_j , the building classification ($i = 1, \dots, 4$) and the desired building security rating ($j = 1, \dots, 5$), respectively. For completeness, CL_i and RT_j are shown in Table 4-1 and Table 4-2.

For a building of class CL_i to attain a security rating of RT_j , it must achieve countermeasure level LV_{ij} . To achieve a specific countermeasure level (LV_{ij}), the first step is to recall that each countermeasure level has two specific components (see Chapter 3). Note that subscripts i and j were added for generality.

- Does the building for this LV_{ij} level pass all required countermeasures? (Yes or no)
- What is the value of the actual-to-maximum score ratio, α_{ij} ? (See Eqs. 3-3, 3-4, and 3-5)

Table 4-1 Building Classification, CL_i

Counter, i	CL_i
1	A
2	B
3	C
4	D

Two limiting values for α_{ij} are introduced as follows:

$$\text{Achieved actual-to-maximum score ratio} = \alpha_{ij}|_{\text{ACHIEVEMENT}} \quad (4-1)$$

$$\text{Advance actual-to-maximum score ratio} = \alpha_{ij}|_{\text{ADVANCE}} \quad (4-2)$$

The $\alpha_{ij}|_{\text{ACHIEVEMENT}}$ is the ratio that is needed so that the score satisfies (achieves) the required countermeasure for rating level under consideration. The $\alpha_{ij}|_{\text{ADVANCE}}$ is the ratio that is needed before the building is considered for the next rating level. Generally speaking,

$$\alpha_{ij}|_{\text{ACHIEVEMENT}} \leq \alpha_{ij}|_{\text{ADVANCE}} \quad (4-3)$$

The actual-to-maximum score ratio α_{ij} for the level LV_{ij} needs to satisfy

$$\alpha_{ij} \geq \alpha_{ij}|_{\text{ACHIEVEMENT}} \quad (4-4)$$

for a building of classification CL_i to achieve the desired building security rating RT_j .

Table 4-2 Desired Building Security Rating, RT_j

Counter, j	RT_j
1	Rated
2	Bronze
3	Silver
4	Gold
5	Platinum

Moreover, the actual-to-maximum score ratio α_{ij} for the level LV_{ij} needs to satisfy

$$\alpha_{ij} \geq \alpha_{ij}|_{\text{ADVANCE}} \quad (4-5)$$

for a building of classification CL_i to be eligible for consideration of an RT_{j+1} rating.

Thus, the rating process for a given classification CL_i starts at the least demanding rating level LV_{1j} (the Rated level). Three outcomes may result:

1. The building passes all *required* countermeasures of that level;
2. The equation $\alpha_{i1} \geq \alpha_{i1}|_{\text{ACHIEVEMENT}}$ is satisfied; and
3. The equation $\alpha_{i1} \geq \alpha_{i1}|_{\text{ADVANCE}}$ is satisfied.

If conditions 1 and 2 are not satisfied, then the building does not achieve the Rated rating. Obviously, it cannot advance to the next level. Also, if condition 3 is not met, then the building cannot advance to the next level. However, if the building satisfies all three conditions, then it is eligible for consideration for the next higher rating level LV_{2j} (i.e., the Bronze level). Again, three outcomes may result:

1. The building passes all required countermeasures of that level;
2. The equation $\alpha_{i2} \geq \alpha_{i2}|_{\text{ACHIEVEMENT}}$ is satisfied; and
3. The equation $\alpha_{i2} \geq \alpha_{i2}|_{\text{ADVANCE}}$ is satisfied.

The process continues as above until the building achieves the desired rating or gets to a point where the building cannot advance to the next level. Fig. 4-2 shows the flow-chart of the rating process. Table 4-3 shows the different

Table 4-3 Security Ratings as a Function of Class and Countermeasure Levels

Class	Rating	Countermeasure Level	$\alpha_{ij} _{\text{ACHIEVEMENT}}$ Needed to Achieve Rating (%)	$\alpha_{ij} _{\text{ADVANCE}}$ Needed to Advance (%)	Required Countermeasures
A	Platinum	Level 5	60.00	N.A.	5
	Gold	Level 4	60.00	90.00	5
	Silver	Level 3	60.00	90.00	11
	Bronze	Level 2	60.00	90.00	6
B	Platinum	Level 5	40.00	N.A.	2
	Gold	Level 4	40.00	50.00	2
	Silver	Level 3	50.00	60.00	9
	Bronze	Level 2	50.00	60.00	5
C	Platinum	Level 5	20.00	N.A.	0
	Gold	Level 4	30.00	50.00	0
	Silver	Level 3	40.00	40.00	6
	Bronze	Level 2	40.00	40.00	4
D	Platinum	Level 5	10.00	N.A.	0
	Gold	Level 4	20.00	20.00	0
	Silver	Level 3	30.00	30.00	3
	Bronze	Level 2	30.00	30.00	3

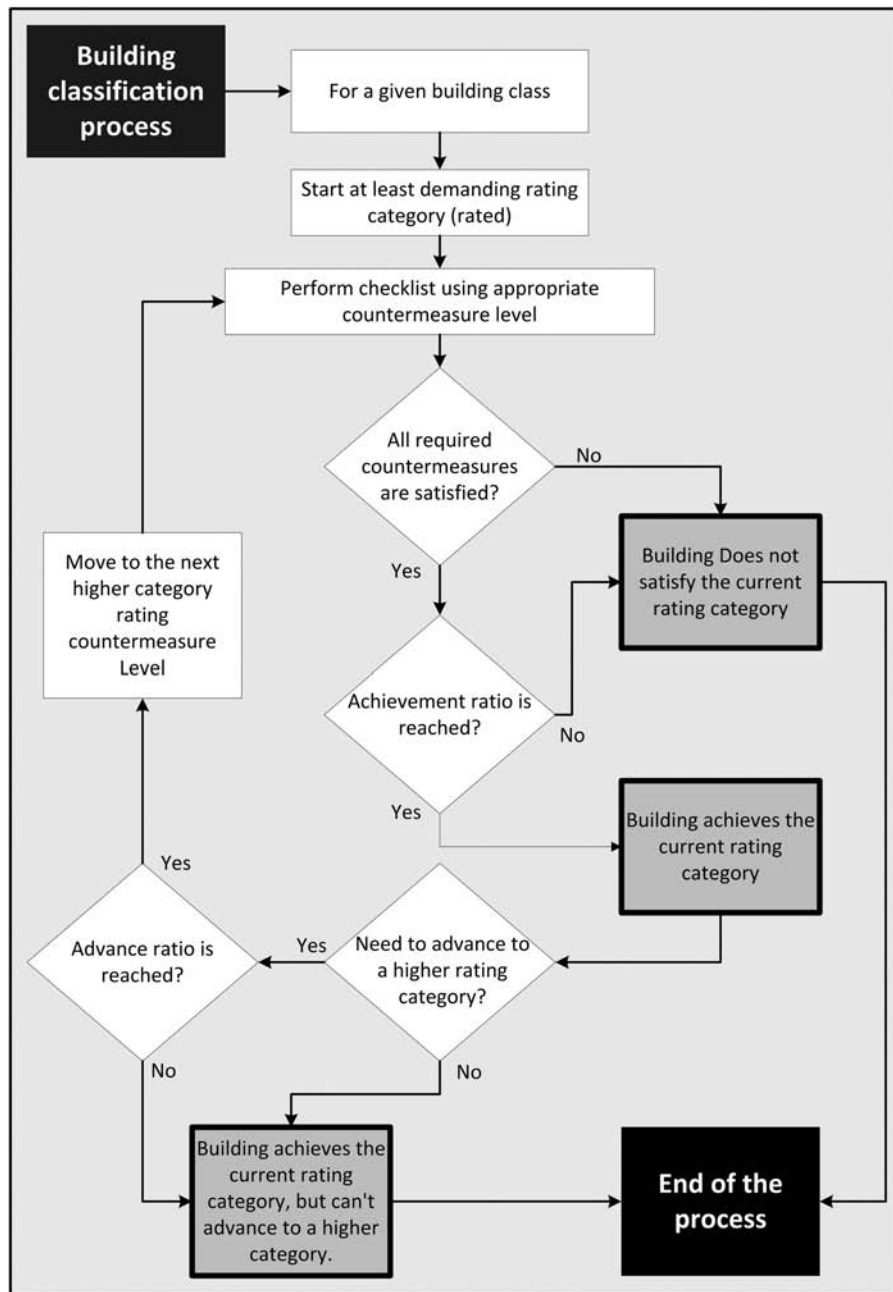


Fig. 4-2. Building security rating process.

values of $\alpha_{ij}|_{ACHIEVEMENT}$ (expressed in %); $\alpha_{ij}|_{ADVANCE}$ (expressed in %); and the number of required countermeasures for the four countermeasure levels, the different building classifications, and the different building security ratings.

One of the advantages of this process is that it systematically ensures that basic countermeasures in the lower security rating categories are not bypassed when attempting to achieve a higher security rating category.

4.5 BONUS POINTS

At the end of each rating category, there is a provision for awarding bonus points. These bonus points are awarded for innovative countermeasures not included in the checklist (see Appendix B) that provide a substantial benefit to building security. Some examples of innovation are given in Appendix C, Innovations in Building Security, but building owners are not restricted to just those listed.

Bonus points can be applied to obtain the rating in the category where awarded. In other words, bonus points may be used to help in satisfying Eq. (4-4) above. However, there are limits to the use of bonus points. For example, to move on to the next rating category, the required countermeasures and the required percentage of the applicable

listed countermeasure points to advance must still be met for the previous categories. Further, to move to the next category, the bonus points cannot be substituted for failure to meet countermeasure points in a previous category. In summary, the bonus points can't be used to satisfy Eq. (4-5) above.

APPENDIX A

Classification and Impact Questions

This appendix presents BSRS building classification questions and their corresponding group weights. Table A-1 contains threat questions and their possible multiple answers. Table A-2 contains impact questions and their possible mul-

iple answers. Details of the multiple possible choices for each question and the relative weights for these choices are shown in Table A-3 through Table A-22.

Table A-1 Threat Questions for Building Classification

Parameter Type	Threat Classification Question	Group Weight
Primary	What type of facility is being assessed? Please choose the option that best applies. These facility types provide a baseline risk level for the classification point system.	18.75
Primary	To what extent is the building associated with U.S. critical infrastructure, such as transportation, utilities, fuel, telecommunications, etc.? An essential operation to the infrastructure system would be considered high.	18.75
Primary	How many threats have been received at the facility in the last five years?	18.75
Secondary	Are there VIPs or other occupants that are attractive targets for criminals or terrorists?	2
Secondary	How many public visitors are in the building on average in a single day?	1.5
Secondary	What is the population of the city?	1
Secondary	What is the distance from the building to the hazardous material facility or transportation route?	1
Secondary	What is the distance from the building to the high-profile target?	1
Secondary	Are there regular instances of criminal or gang-related activity in the surrounding area?	2
Secondary	Are law enforcement agencies (i.e., police, FBI, ATF, U.S. Marshals Service, etc.) located in this facility?	4

Table A-2 Impact Questions for Building Classification

Parameter Type	Impact Classification Question	Group Weight
Primary	What is the national symbolic significance of the facility and its primary function? For example, the Statue of Liberty, Washington Monument, or New York Stock Exchange would be considered high.	18.75
Primary	What is the national political significance of the facility and its primary function? For example, the White House, the U.S. Capitol, or an abortion clinic would be considered high.	18.75
Primary	What is the local economic significance of the facility and its primary function? For example, major employer, financial institution, or large tax revenue creator would be considered high.	18.75
Primary	To what extent is the building associated with U.S. critical infrastructure such as transportation, utilities, fuel, telecommunications, etc.? An essential operation to the infrastructure system would be considered high.	18.75
Secondary	Does the facility contain a child care center?	1
Secondary	What is the facility occupancy?	1
Secondary	What is the square footage of the facility?	1
Secondary	How many public visitors are in the building on average in a single day?	1.5
Secondary	Is the facility a listed historic building?	2
Secondary	What is the overall impact to the major tenant organizations if this facility is destroyed or damaged beyond use for an extended period of time? A significant loss of business would be considered high.	3

Table A-3 Choices for Threat Question Number 1—To Be Used for Building Classification

Question	
What type of facility is being assessed? Please choose the option that best applies. These facility types provide a baseline risk level for the classification point system.	
Choice	Weight
Airport Terminals, Hangars, and Aviation-Related Structures	3
Ammunition and Explosive Storage Magazines	4
Apartments and Condominiums	2
Armories	4
Chemical Plants	4
Commercial Facilities	3
Community Services	1
Educational Facilities	2
Federal Courthouses	4
Federal Government	4
Financial Institutions	4
Gymnasiums, Recreation Centers, and Athletic Practice Facilities	1
Health Care Facilities	2
High-Rise Office Buildings	3
Hotels, Motels, and Resorts	2
Industrial Facilities	3
Land Ports of Entry	3
Libraries	1
Local Government	2
Maintenance Facilities and Equipment Buildings	1
Military	4
Monuments	2
Multistory Office Buildings	2
Museums	2
One-Story Office Buildings	1
Other Critical Infrastructure Facilities	4
Parking Facilities	1
Petroleum Plants	4
Power Plants	4
Religious Facilities	2
Research Facilities	3
Sea Ports of Entry	3
Shopping Centers and Retail	2
Single Family Dwellings	1
Stadiums, Arenas, Ballparks, and Entertainment Venues	3
State Government	3
Warehouses	2

Table A-4 Choices for Threat Question Number 2—To Be Used for Building Classification

Question	
Are there VIPs or other occupants that are attractive targets for criminals or terrorists?	
Choice	Weight
Yes	1
No	0

Table A-5 Choices for Threat Question Number 3—To Be Used for Building Classification

Question	
How many threats have been received at the facility in the last 5 years?	
Choice	Weight
None	0
1–5	1
6–10	2
11–100	3
>100	4

Table A-6 Choices for Threat Question Number 4—To Be Used for Building Classification

Question	
How many public visitors are in the building on average in a single day?	
Choice	Weight
<20	0
20–49	1
50–99	2
100–300	3
>300	4

Table A-7 Choices for Threat Question Number 5—To Be Used for Building Classification

Question	
What is the population of the city?	
Choice	Weight
<100,000	0
100,000–500,000	1
500,001–1 million	2
>1 million	3

Table A-8 Choices for Threat Question Number 6—To Be Used for Building Classification

Question	
What is the distance from the building to the hazardous material facility or transportation route?	
Choice	Weight
>1,000 ft (304.80 m)	0
1,000 ft (304.80 m)	1
500 ft (152.40 m)	2
100 ft (30.48 m)	3
0 ft (0.0 m)	4

Table A-9 Choices for Threat Question Number 7—To Be Used for Building Classification

Question	
To what extent is the building associated with the United States critical infrastructure such as transportation, utilities, fuel, telecommunications, etc.? An essential operation to the infrastructure system would be considered High.	
Choice	Weight
Very Low	0
Low	1
Medium	2
High	3
Very High	4

Table A-10 Choices for Threat Question Number 8—To Be Used for Building Classification

Question	
What is the distance from the building to the high profile target?	
Choice	Weight
>1,000 ft (304.80 m)	0
1,000 ft (304.80 m)	1
500 ft (152.40 m)	2
100 ft (30.48 m)	3
0 ft (0.0 m)	4

Table A-11 Choices for Threat Question Number 9—To Be Used for Building Classification

Question	
Are there regular instances of criminal or gang-related activity in the surrounding area?	
Choice	Weight
Yes	1
No	0

Table A-12 Choices for Threat Question Number 10—To Be Used for Building Classification

Question	
Are law enforcement agencies (i.e. police, FBI, ATF, U.S. Marshals Service, etc.) located in this facility?	
Choice	Weight
Yes	1
No	0

Table A-13 Choices for Impact Question Number 1—To Be Used for Building Classification

Question	
What is the national symbolic significance of the facility and its primary function? For example, the Statue of Liberty, Washington Monument, or New York Stock Exchange would be considered High.	
Choice	Weight
Very Low	0
Low	1
Medium	2
High	3
Very High	4

Table A-14 Choices for Impact Question Number 2—To Be Used for Building Classification

Question	
What is the national political significance of the facility and its primary function? For example, the White House, U.S. Capitol, or an abortion clinic would be considered High.	
Choice	Weight
Very Low	0
Low	1
Medium	2
High	3
Very High	4

Table A-15 Choices for Impact Question Number 3—To Be Used for Building Classification

Question	
What is the local economic significance of the facility and its primary function? For example, major employer, financial institution, or large tax revenue creator would be considered High.	
Choice	Weight
Very Low	0
Low	1
Medium	2
High	3
Very High	4

Table A-16 Choices for Impact Question Number 4—To Be Used for Building Classification

Question	
To what extent is the building associated with the United States critical infrastructure such as transportation, utilities, fuel, telecommunications, etc.? An essential operation to the infrastructure system would be considered High.	
Choice	Weight
Very Low	0
Low	1
Medium	2
High	3
Very High	4

Table A-17 Choices for Impact Question Number 5—To Be Used for Building Classification

Question	
Does the facility contain a child care center?	
Choice	Weight
Yes	1
No	0

Table A-18 Choices for Impact Question Number 6—To Be Used for Building Classification

Question	
What is the facility occupancy?	
Choice	Weight
<10	0
10–150	1
151–450	2
>450	3

Table A-19 Choices for Impact Question Number 7—To Be Used for Building Classification

Question	
What is the square footage of the facility?	
Choice	Weight
<2,500	0
2,500–80,000	1
80,001–150,000	2
>150,000	3

Table A-20 Choices for Impact Question Number 8—To Be Used for Building Classification

Question	
How many public visitors are in the building on average in a single day?	
Choice	Weight
<20	0
20–49	1
50–99	2
100–300	3
>300	4

Table A-21 Choices for Impact Question Number 9—To Be Used for Building Classification

Question	
Is the facility a listed historic building?	
Choice	Weight
Yes	1
No	0

Table A-22 Choices for Impact Question Number 10—To Be Used for Building Classification

Question	
What is the overall impact to the major tenant organizations if this facility is destroyed or damaged beyond use for an extended period of time? A significant loss of business would be considered High.	
Choice	Weight
Low	0
Medium	1
High	2

This page intentionally left blank

APPENDIX B

Rating Class and Countermeasure Requirements for Each Rating Level

This appendix shows different countermeasures for different security rating levels. Countermeasures for each level are categorized according to 13 building disciplines.

LEVEL 1 (RATED) COUNTERMEASURE CHECKLIST

Discipline	Count	Countermeasure
1—Site		
1	1	Vehicle and pedestrian entrances are lit for safety.
1	2	Perimeter vehicle and pedestrian circulation areas (including parking) are lit for safety.
1	3	Landscaping does not conceal and obstruct views near the perimeter of the facility.
1	4	Sufficient access to all fire hydrants is available.
1	5	Signage off site and at entrances is available to direct traffic.
1	6	Signage on site is available to direct vehicles and pedestrians.
1	7	Signage is clear to avoid confusion and direct users to their destinations efficiently.
2—Architectural		
2	1	Vehicle entry/exit points are kept to a minimum.
2	2	Employees and the public use the same building entrances if visitor screening is not present. (If present, separate entrances can be used.)
2	3	Openings for mail or express boxes and trash receptacles are small enough to prohibit insertion of packages.
2	4	Areas of refuge are identified, with special consideration given to egress.
2	5	High-value functions, critical assets, and officials are protected from public view and access.
2	6	Elevator lobbies are well lit and visible to both patrons in the parking areas and the public on the street.
3—Structural		
3	1	Vehicular or personnel proximity to transfer girders is not possible.
3	2	Simple supported load-carrying systems are not utilized.
3	3	Construction material is NOT light metal, wood, or nonreinforced bearing wall systems, or structural system is NOT accessible to pedestrian or vehicular traffic.
4—Building envelope		
4	1	Exterior walls and doors are designed to resist forced entry.
4	2	All door hinges and locking hardware are on the secure side of the door or window.
4	3	Building envelope (walls and roof) is anchored to the structural system.

Discipline	Count	Countermeasure
		5—Utilities
5	1	Emergency power for exit lights is provided.
5	2	Commercial central station is employed for after-hours monitoring or to supplement on-site monitoring.
		6—Mechanical
6	1	Exterior points of access to the building roof (ladders, adjacent structures, platforms, or buildings) cannot be used by unauthorized personnel to gain access.
6	2	Interior points of access to the building roof (hatches, doors, elevator, etc.) are kept locked to prevent access by unauthorized personnel.
6	3	Doors to utility or mechanical rooms are kept locked.
		11—Equipment operations and maintenance
11	1	Access to building information is restricted.
		12—Security systems
12	1	Facility has basic intrusion-detection devices (contacts for doors and operable first-floor windows) for entrances into the facility.
12	2	Ground-level pedestrian exits that open into nonsecure areas are used as emergency exits and are fitted with (only) panic bar hardware for exiting.
12	3	All security locking arrangements on doors used for egress comply with the requirements of NFPA 101, Life Safety Code (2012).
12	4	Self-contained battery lighting is provided in stairwells and for exit signs as backup in case of emergency generator lag time or failure.
12	5	Vaults or safes are located in secure rooms with no windows and a minimal number of doors.
		13—Security master plan
13	1	The facility has emergency evacuation plans updated annually, and evacuation drills are performed semi-annually.

LEVEL 2—BRONZE COUNTERMEASURE CHECKLIST

Discipline	Count	Countermeasure
		1—Site
1	1	Lighting supports visual or closed-circuit television (CCTV) surveillance.
1	2	Redundant routes are provided for emergency vehicle access and egress.
1	3	Attended booths or parking offices are located so that activity at pedestrian and vehicle entry points to the facility can be monitored.
1	4	Culverts, sewers, storm drains, concrete trenches, duct systems, and pipelines (that enter or go under the facility) have openings with no dimension greater than 6 in (15 cm).
1	5	Vegetation (bushes, trees, etc.) and other nonhardened landscape elements are used to control vehicle access.
1	6	Adjacent street curb lane parking is restricted to key employee parking.
1	7	Site is designed to clearly identify property lines.
1	8	Under-building access to crawl spaces and utility tunnels is restricted.
1	9	Security station or reception area is located where it is visible to the public and where the attendant can directly monitor entry/exit activity.
1	10	Design of stair towers and elevator lobbies ensures that people using these areas can be easily seen and can see out to reduce likelihood of assault.
1	11	Inside parking is restricted to selected employees only.

Discipline	Count	Countermeasure
2—Architectural		
2	1	Pedestrian walkways concentrate activity.
2	2	Parking facility has vehicular access control.
2	3	Security screening or fencing has been provided at openings to discourage anyone from entering the parking facility on foot.
2	4	Streets, sidewalks, and building entrances clearly indicate public routes and direct people away from private or restricted areas.
2	5	Access to private areas is discouraged with structural elements and limited access (no cut-through streets).
2	6	Shrubbery is less than 2 ft (60 cm) in height.
2	7	Lower branches of existing trees are kept at least 10 ft (3 m) off the ground.
2	8	Visitors (and their baggage) to facility are screened for weapons and explosives.
2	9	Circulation routes have unobstructed views of people approaching controlled access points.
2	10	Signage identifying high-risk areas is minimized.
2	11	Shelter-in-place locations are provided.
2	12	Sensitive areas are controlled by locks and physical barriers.
2	13	Staff areas are separated from the public by locked doors and barriers.
2	14	For lobby retail, control access to main building with separate entryways, access control, hardened partitions (against intrusion), and security operational measures is provided.
3—Structural		
3	1	Structural system is reinforced concrete (neither prestressed nor precast) or steel frame.
3	2	Structural system is braced frame, shear wall, or bearing wall.
3	3	Structural system is prestressed or precast reinforced concrete system (slabs, beams, and/or columns) and blast and/or progressive collapse analysis were performed.
3	4	Structural system is either wood or light metal, and blast and/or progressive collapse analysis were performed.
3	5	There are NO transfer girders within the structural system.
3	6	Loading zones are separate from public parking.
4—Building envelope		
4	1	The glazing has sufficient “bite.”
4	2	Exterior walls are framed curtain walls (metal).
4	3	Exterior walls are reinforced precast concrete panels or reinforced masonry.
4	4	Exterior walls are non-reinforced masonry or nonreinforced concrete panels.
4	5	Exterior walls are designed for high wind.
5—Utilities		
5	1	Restrooms are provided with emergency lighting.
5	2	Facility has an emergency power system or generator for life safety and security systems.
6—Mechanical		
6	1	Air intakes have been located on the roof or as high on the building as practical, or ground-level outdoor air intakes have a security zone established by fencing or grilling or other means of physical protection.
6	2	Ventilation equipment is located away from high-risk areas such as loading docks, garages, mailrooms, and lobbies.
6	3	Return air vent grilles are secured from general access.
6	4	Prerecorded message over the elevator cab speakers notifies passengers of an emergency and explains how to proceed.

Discipline	Count	Countermeasure
		10—Communications and IT
10	1	Mass communications system is used to make emergency announcements to building occupants.
		11—Equipment operations and maintenance
11	1	Up-to-date composite drawings indicate location and capacities of major systems (electrical, mechanical, and fire protection).
11	2	Updated operations and maintenance (O&M) manuals exist.
		12—Security systems
12	1	Parking facility and other remote areas have emergency intercom/duress buttons or assistance stations on structure columns, fences, other posts, and/or freestanding pedestals.
12	2	Emergency intercom/duress buttons or assistance stations are brightly marked with stripping or paint visible in low light.
12	3	Staff identification (ID) system is implemented, and ID checks are performed to control access into the facility.
12	4	Key control systems are in place and are well maintained.
12	5	There are areas of concealment for devices before screening points.
12	6	Potentially hazardous chemicals and combustible or toxic materials are stored on site in secure and monitored areas.
12	7	Duress buttons are located at key public contact areas and as needed in the offices of managers and directors, in garages, and other areas that are identified as high-risk locations.
12	8	Duress alarms are located in reception areas.
12	9	All security system documents include current as-built drawings.
12	10	Security system manuals are available.
		13—Security master plan
13	1	A written security plan exists for this site or building and has been communicated and disseminated to key management personnel and departments.
13	2	Security system as-built drawings have been generated.

LEVEL 3—SILVER COUNTERMEASURE CHECKLIST

Discipline	Count	Countermeasure
		1—Site
1	1	Design of the parking facility maximizes visibility and monitoring capability to the greatest extent possible.
1	2	Site lighting has been coordinated with the CCTV system.
		2—Architectural
2	1	High-risk and low-risk offices are housed separately.
2	2	Public and employee entrances include space for possible future installation of access control and screening equipment for higher threat periods.
2	3	Public access areas are separated from high-risk offices.
2	4	Mailroom is at the perimeter of the building.
2	5	Adequate room for explosive disposal containers and mail or package examination equipment is available in mailroom.
2	6	Distance of at least 25 ft (7.5 m) separates mailroom from facility main entrances, utilities, areas containing critical services, distribution systems, and important assets.
2	7	Entrances have been designed to avoid significant queuing.
2	8	The security console and control room is adequate in size and provides room for expansion.

Discipline	Count	Countermeasure
3—Structural		
3	1	Drive-up/drop-off areas restrict parking and are not located under inhabited portions of the building.
3	2	Rated vehicle crash barriers are installed to prevent driving into or under the facility.
3	3	Distance of at least 25 ft (7.5 m) separates main entrance, loading docks, shipping/receiving areas, vehicle circulation, and parking from utility mains, utility rooms, and other critical components and important assets.
3	4	Blast analysis has been performed to threat consistent with building classification. Acceptance limits are consistent with consequences used in the building classification.
3	5	Fire protection engineer has coordinated with the blast engineer on issues affecting life safety and building egress.
3	6	Progressive collapse analysis has been performed to threat consistent with building classification. Acceptance limits are consistent with consequences used in the building classification.
3	7	All hardened or protection systems are properly anchored to the ground.
4—Building envelope		
4	1	Measures such as window film, blast curtain, and blast shield have been implemented to mitigate secondary debris (primarily glass fragmentation) caused by abnormal loadings.
4	2	Interior glazing has been minimized and is shatter resistant where blast and/or forced entry threats exist, such as in lobbies, mailrooms, etc.
4	3	Antishatter or antiglare films on glazing are utilized.
4	4	All components of building envelope are attached to one another appropriately.
5—Utilities		
5	1	Incoming utility systems have been concealed and/or secured.
5	2	Manhole covers have locks.
5	3	Emergency generator fuel tank is located away from building.
5	4	Emergency generator fuel tank is secured with locked enclosure and/or intrusion detection.
5	5	Emergency generator is located away from loading docks, entrances, and parking.
5	6	Emergency generator is located away from areas prone to flooding.
6—Mechanical		
6	1	Air-handling system utilizes a high-efficiency particulate air (HEPA) filter or functional equivalent on all air-handling units (AHUs), including outside units, and in the supply air stream of recirculating AHUs.
6	2	Intrusion detection, CCTV, and/or security guards are implemented to protect air intakes.
6	3	Wiring for power and ventilation system controls is protected by conduit encasement.
7—Plumbing and gas		
7	1	Gas storage tanks (heating, cooking, medical, process) are located at least 50 ft (15 m) from personnel areas.
7	2	Exterior gas lines are piped below ground to the distribution system.
8—Electrical		
8	1	Emergency backup power exists for all critical areas.
8	2	There is redundancy of emergency power distribution to critical areas. Runs are separated.
8	3	Electrical distribution panels serving branch circuits are secured.
9—Fire		
9	1	Alarm and information systems (annunciator, radio system) are colocated.
9	2	Alarm and information systems are collected and mounted in separate conduits.
9	3	Facility has a fire command center (FCC).
9	4	Facility has a security control center (SCC).
9	5	There is a button in the FCC to recall elevators to an alternative floor if the elevators could safely be used to evacuate disabled persons or if the normal evacuation route would involve traveling through a high-risk area.

Discipline	Count	Countermeasure
9	6	Fire protection engineering analysis has been completed for fire suppression, evacuation capabilities, and secure locations.
		10—Communications and IT
10	1	The interior cameras are supported by an uninterruptible power supply source, battery, or building emergency power.
		11—Equipment operations and maintenance
11	1	Procedures and preventive maintenance schedules for cleaning and maintaining ventilation system components are in place.

LEVEL 4—GOLD COUNTERMEASURE CHECKLIST

Discipline	Count	Countermeasure
		1—Site
1	1	Design, site layout, or speed control measures prohibit a vehicle from approaching at significant speed.
1	2	CCTV surveillance system with recording capability is used to view activity within 50 ft (15 m) of the perimeter of the building.
1	3	System of fencing, grilles, doors, etc., to completely close down access to the entire site in unattended hours, or in some cases, all hours exists.
1	4	Vehicles are inspected at perimeter.
1	5	Pull-over lanes are available at checkpoints to inspect vehicles.
1	6	Vehicle control measures (sally port, etc.) are available to prevent tailgating.
1	7	Garage or service entrances that are not otherwise protected by site perimeter (crash) barriers are provided vehicle-arresting devices.
1	8	Emergency vehicle routes have vehicle barriers capable of allowing passage of large fire apparatus.
1	9	The uninterruptible power supply (UPS) is located in a secure area.
		2—Architectural
2	1	Vehicle standoff (based on blast assessment) is available for unscreened vehicles, defended by rated crash barrier systems.
2	2	Trash receptacles are placed at the perimeter of the facility, or they are hardened or removed from around the facility.
2	3	Potential hiding places are avoided or closed off.
2	4	Foyers have reinforced concrete walls, and interior and exterior doors are offset from each other.
2	5	Exterior hallways are not present in inhabited portions of the building to protect personnel from open exposure to large amounts of flying glass and debris.
2	6	Stairwells required for emergency egress are located away from areas where blast events might occur, such as lobbies, mailrooms, parking, and loading docks.
2	7	Stairwells required for emergency egress are designed to support the Occupant Emergency Plan (OEP).
2	8	Parking is prohibited underneath or within facility.
2	9	Public toilets, service spaces, and vertical circulation systems are located in secure areas behind security screening points.
2	10	Distance of at least 50 ft (15 m) separates main entrance, loading docks, shipping/receiving areas, vehicle circulation, and parking from utility mains, utility rooms, and other critical components and important assets.
2	11	Distance of at least 50 ft (15 m) separates mailrooms from utility mains, utility rooms, and other critical components and important assets.
2	12	Interior doors to high-risk offices are protected by door contacts.
2	13	Stairways are maintained with positive pressure, or other smoke control systems are present.

Discipline	Count	Countermeasure
3—Structural		
3	1	Surface or structured parking within 25 ft (7.5 m) (or based on risk and blast assessment) of the building is restricted to authorized vehicles.
3	2	Unrestricted vehicle and pedestrian access is not permitted under building overhangs.
3	3	Ceiling and lighting systems are designed to remain in place during hazard events.
3	4	All columns in the garage area are designed for an unbraced length equal to two floors, or three floors where there are two levels of parking.
3	5	If primary construction is unreinforced masonry, precast concrete frame, concrete frames with unreinforced masonry infill walls, steel frames with unreinforced masonry infill walls, or tilt-up, blast or progressive collapse analysis should be performed. The threat and acceptance limits should both be consistent with the levels that were used in defining the classification of the building.
3	6	If primary construction is braced steel frame, concrete shear wall, or reinforced masonry, then adequate ductile detailing away from the bracing system, shear wall, or reinforced masonry should be in place, as needed by the postulated threat.
3	7	If primary construction is steel or concrete, moment-resisting frames, or steel frames with cast-in-place concrete shear walls, then ductile detailing of all structural components should be constructed.
3	8	If primary construction is wood framing or light metal, then adequate ductile detailing should be constructed.
3	9	Symmetric steel reinforcement (positive and negative faces) exists in all floor slabs, roof slabs, walls, beams, and girders that may be subjected to rebound, uplift, and suction pressures (only applies to reinforced concrete structures).
3	10	Lap splices fully develop the capacity of the reinforcement (only applies to reinforced concrete structures).
3	11	Lap splices and other discontinuities are staggered (only applies to reinforced concrete structures).
3	12	Special shear reinforcement, including ties and stirrups, is available to allow large postelastic behavior (only applies to reinforced concrete structures).
3	13	Connections possess ductile details.
3	14	Moment connections are used (only applies to steel frame structures).
3	15	Column spacing is not greater than 30 ft (9.1 m) for a reinforced concrete-framed or steel-framed structure.
3	16	Floor heights are not greater than 16 ft (4.9 m) for a reinforced concrete-frame or steel-frame structure.
3	17	If exterior masonry walls are present, they are grouted and reinforced with at least 0.05% steel with spacing no less than 48 in. (1.2 m).
3	18	Facility is designed to prevent progressive collapse.
3	19	Where lobby retail exists, shared partitions are hardened against blast.
4—Building envelope		
4	1	Windows are designed to resist actual blast loads based on risk and blast assessments.
4	2	All exterior doors in inhabited areas open outward to ensure seating in door frames.
4	3	Enclosures for emergency egress are hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees.
4	4	Facility structure and exterior walls are designed to resist actual blast loads based on risk and blast assessments.
4	5	There is less than a 40% fenestration opening per structural bay.
4	6	Nonbearing masonry walls are reinforced.
4	7	Nonwindow openings have been designed to the level of protection required for exterior walls.
4	8	Security glazing meets the requirements of ASTM F1233 (1998) or UL 972 (2002).
5—Utilities		
5	1	Emergency generator system is access controlled.
5	2	Emergency generator system is protected by intrusion-detection devices.

Discipline	Count	Countermeasure
5	3	Utilities have redundant and separated paths for entering facility.
5	4	Incoming utility systems have blast protection, including burial or proper encasement.
5	5	Facility has a backup control center (BCC) for off-site monitoring of alarm, fire, and building maintenance systems.
5	6	There are alternate water supplies for fire suppression.
5	7	The sprinkler and standpipe connections are adequate and redundant.
5	8	Fire hydrant and water supply connections are near the sprinkler/standpipe connections.
5	9	Fire water pumps are redundant (e.g., one electric, one diesel).
5	10	The water pumps are located apart from one another.
5	11	Access to security system, emergency communication system, and associated systems' wiring and conduits is controlled, preferably by routing them through separate and secure closets.
6—Mechanical		
6	1	Automated access control system is provided to monitor access to mechanical, electrical, and telecommunication rooms.
6	2	Fire dampers are installed at all fire barriers.
6	3	Heating, ventilating, and air conditioning (HVAC) systems are isolated in lobbies, mailrooms, loading docks, and other locations where the significant risk of chemical, biological, and radiological (CBR) contamination exists.
6	4	Lobbies, mailrooms, and loading docks maintain negative pressure relative to the rest of the facility.
6	5	Gas adsorption filters are used on recirculated air and on outside air intakes.
6	6	Ventilation system is connected to an emergency power system.
6	7	CBR analysis has been performed using air-plume models to determine threat to facility.
7—Plumbing and gas		
7	1	Exterior water mains are looped and sectionalized to prevent disruption from damage.
7	2	Water supply has backflow preventers.
7	3	Water supply is protected from single-point interior failure, or redundant supply is provided.
9—Fire		
9	1	For enclosures, an automatic fire door or rolling fire shutter with an access door is employed so that the area is wide open during normal use.
9	2	Automated access control system is provided to monitor access to command and control center(s).
9	3	Doors and shutters are closed by a smoke detector when needed, instead of a fire-rated door that remains closed all the time.
9	4	Alternate methods, such as painting handrails, stair treads, signs, and doors with phosphorescent paint, are used to illuminate or delineate stairwells and emergency exits.
9	5	Facility has an area designated as the emergency command center (ECC), where building documents such as emergency instructions, Occupant Emergency Plan (OEP) manuals, and building plans are readily available.
10—Communications and IT		
10	1	Perimeter cameras are supported by an uninterruptible power supply, battery, or building emergency power.
10	2	Facility has a base radio communication system with antenna installed in the stairwell and portable sets distributed on floors.
10	3	A UPS is connected to the emergency power system for life safety and security systems.
10	4	Redundant communications system is provided.
11—Equipment operations and maintenance		
11	1	A computerized security incident reporting system is used to prepare reports and track security incident trends and patterns.

Discipline	Count	Countermeasure
11	2	Critical air systems have been rebalanced at least once a year.
11	3	Backup power systems are tested monthly under load.
		12—Security systems
12	1	Assistance stations within parking facilities or other remote areas have broadcast capability for emergency notification.
12	2	Cameras are oriented to record license plates of entering and departing vehicles and to record pedestrians exiting or entering via vehicle ramps.
12	3	Automated access control requires two inputs to verify ID (i.e., proximity card and personal identification number (PIN)).
12	4	Screening equipment, such as metal detectors, explosive detection equipment, or canines, is used at public entrances to supplement visual inspections.
12	5	Screening of packages and deliveries (for weapons, explosives, and CBR material) is performed at loading docks and shipping/receiving areas.
12	6	Backup motion detection sensors are located at all entrances/exits and accessible windows.
12	7	Delayed egress hardware is provided at egress doors, if permitted by governing code authorities.
12	8	Escort procedures have been implemented for visitors within staff areas.
12	9	Guards and employees receive emergency training in the proper reporting and response to fires and other emergencies and in the use of portable and built-in protection systems, including training in system maintenance.
12	10	The security plan addresses standardized security system construction specification documents.
		13—Security master plan
13	1	The security plan includes security implementation schedules established to address recommended security solutions.
13	2	The security plan addresses security operating and capital budgets.
13	3	Regulatory or industry guidelines or standards were followed in the preparation of the security plan.
13	4	The security plan addresses the following major components: access control, surveillance, response, building hardening, and protection against CBR and cyber-network attacks.
13	5	The security plan addresses qualifications for security consultants, system designers and engineers, installation vendors, and contractors.

LEVEL 5—PLATINUM COUNTERMEASURE CHECKLIST

Discipline	Count	Countermeasure
		1—Site
1	1	Facilities with similar threat levels have been clustered (if on campus).
1	2	Culverts, sewers, storm drains, concrete trenches, duct systems, and pipelines (that enter or go under the facility) have intrusion detection to detect unauthorized access.
1	3	Access to site is controlled by performing ID check and/or screening pedestrians entering the site.
		2—Architectural
2	1	Screening of mail, packages, and deliveries (for weapons, explosives, and CBR material) is performed off site.
		3—Structural
3	1	Adjacent buildings are spaced far enough away to prevent severe collateral damage.
3	2	Additional standoff for the facility has been created (based on risk and blast assessments) by eliminating street parking and/or closing streets.
3	3	Utility rooms, utility mains, and service entrances within 50 ft (15 m) of loading docks and shipping/receiving areas are hardened for blast.

Discipline	Count	Countermeasure
3	4	Building is structurally independent from any adjacent buildings.
3	5	Architectural or structural features that provide a minimum standoff of 150 mm (6 in.) from exposed primary load-bearing members have been implemented.
3	6	Mailrooms and unscreened retail spaces are designed to mitigate the effects of a blast on primary vertical or lateral bracing members.
3	7	Mailroom design contains provision for interior pressure relief or is hardened sufficiently to protect adjacent occupied space.
3	8	Queuing area is enclosed in blast-resistant construction within the building footprint.
3	9	Structural members and all mechanical system mountings and attachments will resist blast overpressures from infilling through nonwindow openings.
4—Building envelope		
4	1	Lobby doors and partitions are ballistic resistant.
4	2	Ballistic windows are used in the building for high-risk areas.
4	3	Ballistic glazing meets the requirements of UL 752 (2000).
4	4	Methods such as blow-out panels and window system designs that provide protection from blast pressure applied to the outside but that readily fail and vent if exposed to blast pressure on the inside are used to facilitate the venting of explosive forces and gases from interior spaces, including lobby, mailroom, and loading dock, to the outside of the structure.
5—Utilities		
5	1	Building air tightness is enhanced to prevent exterior CBR contamination.
5	2	Water supply has a central building water filtration and treatment system.
5	3	Connections for tertiary power source are provided.
5	4	The sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation.
6—Mechanical		
6	1	Results of analyses using air-plume models related to CBR clouds have been incorporated into the placement of intakes.
6	2	Low-leakage, fast-acting dampers are installed on the air intakes.
6	3	Space and access to AHU is provided for future installation of CBR-detection technology and large filter assemblies.
6	4	Smoke evacuation systems are installed.
6	5	Smoke removal equipment has stand-alone local control panels that can continue to individually function in the event the control wiring is severed from the main control system.
6	6	HVAC system has emergency shutoff switch to shut down air distribution except where interior pressures and airflow would prevent spread of contaminants.
6	7	HVAC control options can regulate airflow and pressures within a building on an emergency response basis.
6	8	Ducted return air systems are present.
6	9	There are redundancies in the air-handling system.
6	10	Critical areas can be served from other AHUs if a major system is disabled.
6	11	The air-handling system has purge capability.
6	12	Roof-mounted air-handling equipment is located at the center of the roof.
6	13	HVAC maintenance staff is trained in system operation, maintenance, and procedures for a suspected CBR agent release.
7—Plumbing and gas		
7	1	Interior standpipes are cross-connected on each floor.
7	2	Water supply has point-of-use filters.

Discipline	Count	Countermeasure
		9—Fire
9	1	Key fire alarm system components have fire- and blast-resistant separation.
		10—Communications and IT
10	1	Uninterrupted power supply is provided for critical life safety and security systems until emergency power is activated.
		11—Equipment operations and maintenance
11	1	The building has a policy or procedure for periodic recommissioning of major mechanical, electrical, and plumbing (M/E/P) systems.
11	2	Maintenance and service agreements exist for M/E/P systems.
		12—Security systems
12	1	Cameras have video motion detection capability.
12	2	Perimeter intrusion detection is provided to detect unauthorized access to the site using one or a combination of fence sensors, buried cables, microwave sensors, etc.
12	3	Alarm-actuated CCTV monitoring and recording are installed to monitor critical internal areas of the facility.
12	4	Alarm-actuated CCTV monitoring and recording are installed to monitor public/staff separation points within the facility.
		13—Security master plan
13	1	Three-dimensional (3D) evacuation modeling of the facility has been performed to facilitate ingress/egress associated with response to emergency events.
13	2	The security plan addresses existing security conditions from administrative, operational, managerial, and technical security systems perspectives.

This page intentionally left blank

APPENDIX C

Innovations in Building Security

The countermeasures listed in the five levels of the building security rating system pertain to either the physical configuration or layout of a building and its engineered systems or the operational aspects of security and emergency response. These countermeasures are considered to be reasonable and mainstream given the state of today's technology. However, the system also rewards and promotes innovations and advances in concepts and technologies that enhance building security by quantifying the contribution they make and awarding bonus points where the innovations improve a building's security score.

Examples of innovations in operational aspects of security and emergency response include digital IP (Internet protocol) video that allows the use of 360° video and video stitching of images from multiple cameras and 3D imaging

system, the use of artificial intelligence to detect abnormal patterns of behavior, and advanced sensors and detection systems for the detection of traces of explosives and toxic substances. Implementing innovative countermeasures such as these improves the situational awareness of security staff and the likelihood of early detection of abnormal circumstances.

Examples of innovative physical design countermeasures include hardened evacuation stairs, wider evacuation stairs allowing rapid full evacuation, separate stairs for firefighters, increased number of staircases, enhanced fireproofing of steel members, and refuge floors in high-rise buildings. While such measures are not required by today's building codes, they enhance building evacuation and survival of building occupants.

This page intentionally left blank

APPENDIX D

Countermeasure Commentary for Level 1, Rated

Discipline	Count	Countermeasure	Guidance
1—Site			
1	1	Vehicle and pedestrian entrances are lit for safety.	Adequate lighting in these areas provides a strong deterrent and is important to protect the facility from unauthorized access and attack. Vulnerability to personal attack (assault, robbery, rape, carjacking, or kidnapping) and violent acts by terrorists or militants at vehicle and pedestrian entrances can be reduced. Security protection can be successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, is critical. Illuminating Engineering Society of North America (IESNA) guidelines can be used: IESNA RP-20-98 (IESNA 1998), IESNA RP-33-99 (IESNA 1999), and ANSI/IESNA RP-8-00 (ANSI/IESNA 2000). Security lighting provided for overall site building illumination and the perimeter allows security personnel to maintain visual surveillance in darkness. Lighting is somewhat inexpensive to maintain and may reduce the need for security personnel by reducing opportunities for concealment and surprise by potential attackers. It facilitates detection of unauthorized personnel and makes the job of an attacker more difficult. A recommended effective lighting level at vehicular and pedestrian entrances is 160 lux (15 fc), horizontally maintained. Lighting level guidelines are provided to ensure that lighting complies with recognized standards for facility security protection. References include FEMA 426 (Table 1-22 and Section 1.20) (2003a), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
1	2	Perimeter vehicle and pedestrian circulation areas (including parking) are lit for safety.	Adequate lighting in these areas provides a strong deterrent and is important to protect the facility from unauthorized access and attack. Vulnerability to personal attack (assault, robbery, rape, carjacking, or kidnapping) and violent acts by terrorists or militants at vehicle and pedestrian circulation areas (including parking) can be reduced. Security protection can be successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, is critical. Illuminating Engineering Society of North America (IESNA) guidelines can be used: IESNA RP-20-98 (IESNA 1998), IESNA RP-33-99 (IESNA 1999), and ANSI/IESNA RP-8-00 (2000). Security lighting provided for overall site building illumination and the perimeter allows security personnel to maintain visual surveillance in darkness. Lighting is somewhat inexpensive to maintain and may reduce the need for security personnel by reducing opportunities for concealment and surprise by potential attackers. It facilitates detection of unauthorized personnel and makes the job of an attacker more difficult. Where practical, high-mast lighting is recommended, because it gives a broader, more natural light distribution; requires fewer poles and is thus less hazardous to drivers; and is more aesthetically pleasing than standard lighting. Effective lighting of the entry control point gives drivers a clear view of the gatehouse and gives security personnel a clear view of the drivers and vehicles. A recommended effective lighting level at perimeter and at vehicular and pedestrian circulation areas is 54 lux (5 fc), horizontally maintained. Where appropriate, perimeter lighting that is continuous and on both sides of the perimeter barriers, with minimal hot and cold spots, and that is sufficient to support surveillance, is effective. However, for safety reasons and/or for uses with CCTV, lower levels may be desirable. Other codes or standards may restrict site lighting levels. Lighting level guidelines are provided to ensure that lighting complies with recognized standards for facility security protection. References include FEMA 426 (Table 1-22 and Section 1.20), U.S. General Services Administration (2005), and ISC (2004).
1	3	Landscaping does not conceal and obstruct views near the perimeter of the facility.	Areas of concealment provided by landscaping features can assist an intruder and obstruct the view of security personnel and CCTV. Such areas could also be used to conceal the placement of an explosive device. Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, and newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages. A distance of 50 ft (15.2 m) is recommended to limit opportunities for concealment, detect the approach of unauthorized personnel, and provide sufficient standoff for a self-carried explosive device. However, 50 ft (15.2 m) may not be available or required for all facilities. The reviewer must determine an adequate clear zone exists for proper surveillance and to limit places of concealment. References include FEMA 426 (Table 1-22 and Section 1.19), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
1	4	Sufficient access to all fire hydrants is available.	Exterior sources of water for fire suppression are vital to the security and safety of the facility and its occupants. Just as vehicle access points to the site must be able to transit emergency vehicles, so too must the emergency vehicles have access to the buildings and, in the case of fire trucks, the fire hydrants. Thus, security considerations must accommodate emergency response requirements and not hinder access to fire hydrants. A fire protection engineer or local fire marshal shall have reviewed and approved fire hydrant access. References include FEMA 426 (Table 1-22 and Section 1.23) and U.S. General Services Administration (2005).
1	5	Signage off site and at entrances is available to direct traffic.	Signs are an important element of security. They are meant to inform potential intruders about the location of restricted areas; however, inadequate signs can create confusion and defeat their primary purpose. Adequate signage is an inexpensive countermeasure against confusion. Provide signage off site and at entrances. Signs can include • Entry control procedure signs, which explain current entry procedures for drivers and pedestrians; and • Traffic regulatory and directional signs, which control traffic flow and entry of vehicles to the site. Warning signs that are easy to understand posted along the physical barriers and at each entry point denote a facility's restricted area. If two or more languages are commonly spoken in the area, signs using both (or more) languages will be more effective. It is recommended that signs be posted at intervals of no more than 100 ft (30.4 m) along fences or other barriers. Mounting signs on fences equipped with intrusion-detection equipment is not advisable due to possible interference. References include FEMA 426 (Table 1-22 and Section 1.22), U.S. General Services Administration (2005), and ISC (2004).
1	6	Signage on site is available to direct vehicles and pedestrians.	Signs are an important element of security. They are meant to inform potential intruders about the location of restricted areas; however, inadequate signs can create confusion and defeat their primary purpose. Adequate signage is an inexpensive countermeasure against confusion. Provide on-site directional signs, parking signs, and cautionary signs for visitors, employees, service vehicles, and pedestrians. Signs can include • Signs that explain entry control procedures to limited, controlled, and exclusion areas. If two or more languages are commonly spoken in the area, signs using both (or more) languages will be more effective. • Traffic regulatory and directional signs, which control traffic flow of vehicles on the site. • Variable message signs, which give information on site/organization special events and visitors, located far inside site perimeters. By minimizing signs that identify critical utility complexes (e.g., power plants and water treatment plants) and high-risk buildings, site security is enhanced. Clear signs can be posted to minimize accidental entry by unauthorized personnel into sensitive critical asset areas; however, other standards may require signs that identify sensitive areas. References include FEMA 426 (Table 1-22 and Section 1.22), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
1	7	Signage is clear to avoid confusion and direct users to their destinations efficiently.	Confusion over on-site site circulation, parking, and building entrance/exit locations can contribute to reduced site security. The ability of users to navigate an unfamiliar environment en route to their destination is important on a day-to-day basis, but becomes critical in an emergency situation. Signs, in addition to other overt prompts such as landmarks, architectural elements, and maps, will enable facility personnel and visitors to select a path to safety. Signage that is simple and has the necessary level of clarity will be more effective. Signs can be used to clearly indicate exits and emergency evacuation routes and assembly areas. References include FEMA 426 (Table 1-22 and Section 1.22), U.S. General Services Administration (2005), and ISC (2004).
2—Architectural			
2	1	Vehicle entry/exit points are kept to a minimum.	Vehicles may be used to carry explosives and chemical, biological, and radiological (CBR) materials near or into a facility. Additionally, vehicles can support other threats such as kidnapping, robbery, and assault. Too many vehicle entrances can stretch security forces thin (to respond to incidents) and/or increase the expense of security force and equipment cost in controlling vehicle access. The first line of defense in limiting opportunities for aggressors to place vehicles close to a facility's buildings is at vehicle access points at the controlled perimeter, in parking areas, and at drive-up/drop-off points. Keep the number of access points to the minimum necessary for operational or life safety purposes. This will limit the number of points at which access may have to be controlled with barriers and/or personnel in increased threat environments. References include U.S. Department of Defense (DoD) (2002).
2	2	Employees and the public use the same building entrances if visitor screening is not present. (If present, separate entrances can be used.)	Ensuring that only authorized staff, visitors, vendors, and service personnel enter the facility is important to minimize vulnerability to threats associated with unauthorized access such as criminal or terrorist attacks against staff and visitors and critical facility components. Too many entrances can stretch security forces thin (to respond to incidents) and/or increase the expense of security force and equipment cost in controlling access. Unless visitors, vendors, and service personnel are screened at a separate entrance, better security is provided when only one entrance, with provisions for screening, is used for both employees and the public. Keep the number of access points to the minimum necessary for operational or life safety purposes. This will limit the number of points at which access may have to be controlled with equipment and/or personnel in increased threat environments. References include U.S. Department of Defense (DoD) (2002), FEMA 426 (Table 1-22 and Section 2.7), and ISC (2004).
2	3	Openings for mail or express boxes and trash receptacles are small enough to prohibit insertion of packages.	Mail or express boxes and trash receptacles represent potential areas of concealment for package-size explosive devices. Limiting the opening size and increasing the distance from the facility of these items can reduce the facility's vulnerability to attack with these weapons. The size of the trash receptacles and mailbox openings is restricted to prohibit insertion of packages, thus reducing vulnerability to a package bomb threat. Likewise, distancing street furniture, such as newspaper vending machines, or bringing them inside to a secure area can reduce vulnerability. References include FEMA 426 (Table 1-22 and Section 2.4), ISC (2004), U.S. Air Force (USAF) (1997), and DoD (2002).

Discipline	Count	Countermeasure	Guidance
2	4	Areas of refuge are identified, with special consideration given to egress.	Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards. These are generally used when evacuation is not recommended (e.g., for an exterior CBR release or a weather-related event such as a tornado). Establish internal and external areas of refuge (safe zones) for people to use during a toxic release. For an outdoor toxic release, people should remain indoors. “Shelter-in-place” rooms can be created or identified, where people can stay in the event of an outdoor release. These should be rooms with no or low air exchange with the outdoors and low air exchange with the rest of the building. The goal is to create areas where outdoor air infiltration is very low. Usually such rooms are in the inner part of the building (no windows to the outside) and away from areas at risk for a secondary attack (e.g., interior CBR release, bomb). They should have doors that are fairly effective at preventing airflow from the hallways; at a minimum there should be no gap around the edges of the door, and preferably there should be a gasket to completely seal the room. Pressurized stairwells can be another area of refuge. Bathrooms are usually a bad choice, because they often have an exhaust duct that leads directly to the outside. If the exhaust fan is turned off, then the duct, which leads directly outside, can allow toxin-bearing outside air to directly enter the bathroom, which could be very harmful during an outdoor release. Additionally, the stack effect can draw air into the bathroom from within the building, eventually contaminating the building during an indoor release. If the exhaust fan is left on, then air will be drawn into the bathroom from other parts of the building, which will eventually contaminate the bathroom. Exhaust fans for bathrooms and utility rooms are often controlled separately from the heating, ventilating, and air conditioning (HVAC) system. Opening and closing a conventional door can pump significant amounts of air into the safe room. Replacing the door with a sliding door, if practical, can substantially reduce this effect. Additionally, it may be possible to provide purified air to the safe area, depending on whether the pollutant can be removed by the building’s air-filtration system. Modifications to the HVAC system can add special chemical and biological filters to the air supply for the safe area. Pressurizing the safe zone with purified air will greatly reduce entry of contamination and will also reduce the importance of construction details such as the size of the cracks around the door. As circumstances change, it may be necessary to move the occupants of an area of refuge to another or to evacuate the building. For an exterior hazard, once the outdoor concentration has diminished to safe levels (as determined by emergency response teams), the building should be evacuated and flushed with outdoor air. After the contaminated plume passes, the concentration of contamination will actually be higher inside the building than outside, because the building will tend to retain contamination that managed to enter. The Occupant Emergency Plan (OEP) should delineate safe egress routes either to other areas of refuge or for building evacuation. Personnel should be trained for ingress to and egress from areas of refuge. References include FEMA 426 (Table 1-22 and Section 2.22), FEMA 386-7 (2002), and Lawrence Berkeley National Laboratory (2003).
2	5	High-value functions, critical assets, and officials are protected from public view and access.	Protection of high-value functions, critical assets, and officials is essential for the continued operation of the facility and performance of the organization’s mission. Place offices of vulnerable officials so that occupants cannot be seen from an uncontrolled public area such as a street. Offices facing courtyards, internal sites, or controlled areas can reduce vulnerability. Access to private and public space or restricted area space can be clearly defined through the design of the space, signage, use of electronic security devices, etc. Finishes and signage designed for visual simplicity work best. References include FEMA 426 (Table 1-22 and Section 2.8) and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	6	Elevator lobbies are well lit and visible to both patrons in the parking areas and the public on the street.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping) and exposure of vehicles and their contents to larceny and violent acts by terrorists or militants is increased when visual openness is increased. The following measures, as applicable, can help reduce vulnerability to these threats: • Stair tower and elevator lobby are as open as code permits. • Stair and/or elevator waiting areas are as open to the exterior and/or the parking areas as possible and well lit. • Impact-resistant, laminated glass for stair towers and elevators is used as a way to provide visual openness. • Potential hiding places below stairs are closed off. • Nooks and crannies are avoided or eliminated. • Dead-end parking areas are avoided or eliminated. References include FEMA 426 (Table 1-22 and Section 1.17), U.S. General Services Administration (2005), and ISC (2004).
3—Structural			
3	1	Vehicular or personnel proximity to transfer girders is not possible.	Transfer girders increase potential of progressive collapse in the building; a failure of a transfer girder can cause a disproportionate failure in the structure. The risk of this disproportionate collapse increases significantly when the girder is in close proximity to personnel or vehicles. There are two types of transfer girders: • Intermediate transfer girders, where the two ends of the girder are supported by columns; and • Cantilever type girders, where one end of the girder is free, and the girder rests on two interior supports. This type of girder is popular in driveways of public places because it protects cars and personnel from the elements (rain, snow, etc.). Cantilever-type girders are more risky than intermediate-type girders, because a cantilever beam is less redundant than a beam on two supports. References include FEMA 426 (Checklist).
3	2	Simple supported load-carrying systems are not utilized.	Simple supported load-carrying systems do not offer any redundancy beyond their own ultimate flexural capacity. These systems risk producing large displacements if the ultimate flexure of the system is reached. Simple supported load-carrying systems are generally not found in typical building frames. However, in some situations, such as trusses that cover large auditoriums, such systems might be found. References include FEMA 426 (Checklist).
3	3	Construction material is NOT light metal, wood, or nonreinforced bearing wall systems, or structural system is NOT accessible to pedestrian or vehicular traffic.	Structures made of certain materials, such as light metal, wood, or nonreinforced masonry are more vulnerable to blast and progressive collapse than other types of construction materials. These structures need special considerations to assess their resilience in case of bomb blasts. Similarly, all structural systems that are accessible to pedestrian or vehicular traffic need special considerations to assess their resilience in case of bomb blasts. References include FEMA 426 (Checklist).

Discipline	Count	Countermeasure	Guidance
4—Building envelope			
4	1	Exterior walls and doors are designed to resist forced entry.	Exterior walls and doors provide a physical barrier at the building envelope. The integrity of doors and walls is essential in preventing unauthorized access by an attacker. A variety of doors have been designed to resist forced entry and delay attempts to enter a building illegally. Although doors are obvious points at which forced entry may be attempted, walls and other building surfaces may also be vulnerable to penetration. The building is a box with a top, a bottom, and four sides. Applicable references for forced entry protection include, but are not limited to • Walls: U.S. Army (1994); • Swinging door assemblies: ASTM F476 (2014) (grade as directed by the facility risk assessment); • Child care center doors: ASTM F476 (grade as directed by the facility risk assessment); and • Horizontal sliding door assemblies: ASTM F842 (2014) (grade as directed by the facility risk assessment). References include ISC (2004), ASIS (2012), and U.S. Department of State (1997).
4	2	All door hinges and locking hardware are on the secure side of the door or window.	Doors and windows are obvious points at which physical controls are required to prevent unauthorized entry. If a door or window opens outward so that it seats against the inward frame, the hinges are on the nonsecure side of the door or window. If the hinge pins are removed, the door can be opened whether or not it is locked. If a door or window cannot be reconfigured to remove access to the hinges, this situation can be addressed by preventing removal of the hinge pins. Methods to ensure that hinge pins are secured include • Providing concealed hinges; • Peening (i.e., hammering to mushroom the end of the pin); • Installing a hinge with a nonremovable pin; • Inserting a pin or set screw through the hinge pin on the inside of the hinge leaves; and • Installing a safety stud hinge. References include USAF (1997).
4	3	Building envelope (walls and roof) is anchored to the structural system.	Adequate anchoring of building envelope to the structural system will ensure a continuous load path from blast source to the ground via the structural system. Those anchors must be analyzed and detailed according to acceptable analysis and design procedures. References include FEMA 426 (2003a).
5—Utilities			
5	1	Emergency power for exit lights is provided.	Visibility of exit lights and exit pathways is vital to life safety in the event of an emergency that requires evacuation of the facility during power outages. Exit lights should be connected to emergency power to ensure operability during emergencies. A regular maintenance program for stairway and exit sign lighting (all egress lighting) ensures functioning under normal and emergency power conditions. As an alternative, a floor-level evacuation lighting system may be more effective because a design event could fill corridors with dense smoke. Expect building codes to be updated as emergency egress lighting is moved from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured. References include FEMA 426 (Table 1-22 and Section 11.8), FEMA 386-7 (2002), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
5	2	Commercial central station is employed for after-hours monitoring or to supplement on-site monitoring.	Alarms (fire, intrusion, duress) and CCTV systems, if applicable, can be essential to the life safety and physical security of the occupants of the facility. The level of monitoring and the agency performing this duty vary with the level of protection, size, assets, complexity, and occupancy of the facility. Monitoring can be provided by a commercial central station, or an on-site security central control center can be provided during normal business hours. A more advanced measure of safety and security can be provided by monitoring at an on-site, proprietary security control center. To mitigate staffing requirements and annual operating costs, commercial central stations are sometimes used for after-hours monitoring or to supplement on-site monitoring. At the high end of the protection scale, security systems can be monitored by an on-site, 24-hour proprietary security control center. References include FEMA 426 (Table 1-22 and Section 12.32), U.S. General Services Administration (2005), and ISC (2004).
6—Mechanical			
6	1	Exterior points of access to the building roof (ladders, adjacent structures, platforms, or buildings) cannot be used by unauthorized personnel to gain access.	This countermeasure increases the level of protection of a facility by preventing access to criminal or terrorist intruders via the roof. Unwanted access to the roof increases the facility's vulnerability to threats such as burglary, attack upon occupants, and placement of CBR materials in or near a roof-mounted HVAC air intake. Vulnerability to the threat can be lowered by avoiding or removing fixed exterior ladders, platforms, and climbing aids. An alternative is to protect these features by cages or fencing. If adjacent buildings permit access to the facility's roof, protection can be provided by a barrier, such as a security fence. References include FEMA 426 (Table 1-22 and Section 2.14), U.S. General Services Administration (2005), CDC/NIOSH (2002), and ISC (2004).
6	2	Interior points of access to the building roof (hatches, doors, elevator, etc.) are kept locked and alarmed to prevent access by unauthorized personnel.	HVAC equipment and air intakes are frequently located directly on the roof of a building or in a mechanical room enclosed in a "penthouse." A risk exists that unauthorized personnel, including criminals or terrorists, might gain access to tamper with this equipment or to introduce CBR agents. Such access could also provide unauthorized personnel with entry through the roof to otherwise secure rooms or areas. Interior roof hatches with ladders and elevators and stairways with doors leading onto the roof or into a penthouse are avenues of access. Locks, elevator controls, alarms, and CCTV surveillance can be used to prevent unauthorized access to these areas. Authorized facility operations, maintenance, and management personnel can be granted unescorted access. To deter tampering by outside maintenance personnel, a building staff member can escort these individuals throughout their service visit and visually inspect their work before final acceptance of the service. Alternatively, building owners and managers can ensure the reliability of prescreened service personnel from a trusted contractor. References include FEMA 426 (Table 1-22 and Section 2.14), CDC/NIOSH (2002), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
6	3	Doors to utility or mechanical rooms are kept locked.	Closely related to the roof-top location of outdoor air intakes is the security of building mechanical areas. Mechanical areas may exist at one or more locations within a building. These areas provide access to centralized mechanical systems (HVAC, elevator, water, etc.), including filters, air-handling units, and exhaust systems. Such equipment is susceptible to tampering and may subsequently be used in a CBR attack. Access to mechanical areas can be strictly controlled by keyed locks, keycards, or similar security measures. Additional controls for access to keys, keycards, and key codes can be strictly maintained. Elevator controls, alarms, and CCTV surveillance can be used to prevent unauthorized access to these areas. Authorized facility operations, maintenance, and management personnel can be granted unescorted access. To deter tampering by outside maintenance personnel, a building staff member can escort these individuals throughout their service visit and visually inspect their work before final acceptance of the service. Alternatively, building owners and managers can ensure the reliability of prescreened service personnel from a trusted contractor. References include FEMA 426 (Table 1-22 and Section 6.2), CDC/NIOSH (2002), Lawrence Berkeley National Laboratory (2003), U.S. General Services Administration (2005), and ISC (2004).
11—Equipment operations and maintenance			
11	1	Access to building information is restricted.	Terrorists, militants, and criminals can use information about a facility to plan an attack that will accomplish the most harm. Information on building operation, ventilation system details, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel. If plans are provided to contractors for building work, they should be recovered after use whenever possible. Building managers and maintenance personnel should be wary of requests for information about details of the building's structure and HVAC, electrical, life safety, and security systems. References include FEMA 426 (Table 1-22 and Section 6.21), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).
12—Security systems			
12	1	Facility has basic intrusion-detection devices (contacts for doors and operable first floor windows) for entrances into the facility.	Every physical security system, regardless of size or complexity, consists of three elements: detection, delay, and response. Doors and windows are obvious points at which physical controls are required to prevent unauthorized entry. The physical security element of detection can be addressed at the building exterior by basic security detection devices for doors and operable first floor windows. Exterior door protection, especially at loading docks that have overhead or roll-up doors, can be provided by balanced magnetic contact switch sets. Likewise, balanced magnetic contact switch sets can be provided for operable first floor windows and upper floor operable windows that may be accessible from platforms or other building structures. References include ISC (2004).

Discipline	Count	Countermeasure	Guidance
12	2	Ground-level pedestrian exits that open into nonsecure areas are used as emergency exits and are fitted with (only) panic bar hardware for exiting.	Preventing intruders from gaining access to secure areas through emergency egress doors that open into nonsecure areas is important. A panic bar, also known as a crash bar, is commonly used on doors in the path of egress from structures with high occupancy. It automatically locks the door behind the person who is exiting. The nonsecure side of the door should have hardware, handles, or keyway with which to open the door. There should be no way to open the door from the nonsecure side. References include ISC (2004).
12	3	All security locking arrangements on doors used for egress comply with the requirements of NFPA 101 (2012).	The installation of exit devices requires a balance between life safety and physical security. An exit device, also known as a panic bar or crash bar, is commonly used on doors in the path of egress. Exit devices can be electrified to permit remotely controlled reentry via a push button or a card reader or keypad. The installation of emergency exit devices is mandated by NFPA (2012). References include FEMA 426 (Table 1-22 and Section 12.29), U.S. General Services Administration (2005), ISC (2004), and ASIS (2012).
12	4	Self-contained battery lighting is provided in stairwells and for exit signs as backup in case of emergency generator lag time or failure.	Visibility of exit lights and exit pathways is vital to life safety in the event of an emergency, such as a terrorist bomb attack, that requires evacuation of the facility. Self-contained battery lighting can be provided in stairwells and for exit signs as backup in case of emergency generator failure. A regular maintenance program for stairway and exit sign lighting (all egress lighting) ensures functioning under normal and emergency power conditions. Floor-level evacuation lighting systems may be effective because a design event may fill corridors with dense smoke. Expect building codes to be updated as emergency egress lighting is moved from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured. References include FEMA 426 (Table 1-22 and Section 8.6), U.S. General Services Administration (2005), and ISC (2004).
13—Security master plan			
13	1	The facility has emergency evacuation plans updated annually and evacuation drills are performed semi-annually.	Criminal, terrorist, or militant attacks such as bombing, arson, and CBR agent release can cause confusion, panic, injury, and death. This is also true for accidental emergencies such as fire, gas leaks, and natural disasters. Regardless of a facility's size or mission, some level of planning is necessary. Reasons for planning include • Mitigating the impact of the event; • Preparing staff, visitors, and assets; • Accelerating recovery of facilities and finance and administrative operations; • Allowing agency or institution to continue its mission, business, or operation; • Enhancing image with staff, customers, and community; and • Fulfilling moral responsibility. Emergency evacuation plans should be developed, posted, and updated annually. Evacuation drills should be performed semi-annually, if possible, to assess the continuing adequacy of the plans and the level of occupant response. References include FEMA 426 (Table 1-22 and Section 2.22), ISC (2004), and U.S. General Services Administration (2001).

APPENDIX E

Countermeasure Commentary for Level 2, Bronze

Discipline	Count	Countermeasure	Guidance
1—Site			
1	1	Lighting supports visual or closed-circuit television (CCTV) surveillance.	The vulnerability to intrusion through the perimeter and into restricted or controlled areas can be reduced by providing sufficient light for visual or CCTV surveillance. Sufficient lighting in roadway access and parking areas also provides a deterrent to terrorist or criminal activities. For surveillance to be effective, the facility needs sufficient lighting. Surveillance effectiveness can be achieved by coordinating site lighting with the method of surveillance in use. The following considerations apply when lighting systems are intended to support CCTV assessment or surveillance: field of view of the camera, lighting intensity levels, maximum light-to-dark ratio, scene reflectance, daylight-to-darkness transitions, camera mounting systems relative to lighting, spectral response of the camera, cold start time, and restrike time. In the most general sense, the TV camera will “see” the same things the eye sees in any scene. But the various hues and shades of color perceived by the eye will be displayed as shades of gray by a black and white TV camera. They can only be rendered accurately with color cameras and monitors. Also, TV camera imagers may pick up and use light in the ultraviolet or infrared bands that are not visible to humans. The most important factors in regard to scene viewing are the quality and quantity of useful light available. Quality of light means its compatibility with the type of image sensor in the television camera. In most cameras prior to the mid-1980s the imager would have been a vidicon or other type vacuum tube. Today the imager will more likely be a pixel (picture element) array in a charge-coupled device (CCD) camera. The characteristic differences between natural and artificial light and, in the latter class, between incandescent and fluorescent lights and mercury or sodium vapor lights, have an effect on the image picked up by the television camera. The differences are between the colors in the visible light emitted by each source. Different areas of the visible spectrum are emphasized, and the effect is termed the “spectral response.” It is important that the camera selected for a particular scene be capable of acquiring at least a usable image and preferably full video in the spectral response area of the scene lighting. Analysis of camera specifications is a first step, but the most convincing test is actually to sample the scene under the expected lighting conditions, using the specific camera being considered. Even more important than light quality is light quantity. The amount of light needed to produce a TV image at the monitor is most directly stated in terms of the amount of illumination on the image sensor (solid state type) or faceplate (tube type) of the camera. This measure is the most useful because it is an absolute value and does not depend upon factors outside the CCTV system itself, such as the amount of light falling on the scene or the reflecting characteristics of surfaces in the scene.

Discipline	Count	Countermeasure	Guidance
			The Illuminating Engineering Society of North America (IESNA) provides guidelines for this subject (IESNA 2014, IESNA RP-20-98, 1998, IESNA RP-33-99, 1999, and ANSI/IESNA RP-8-00, 2000). References include FEMA 426 (Table 1-22 and Section 1.20) (2003a), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).
1	2	Redundant routes are provided for emergency vehicle access and egress.	The goal is to have at least two access points to provide alternate routes for emergency vehicles if one of the access points becomes unusable. Two access points can also be used effectively to separate commercial, service, and delivery vehicles from passenger vehicles due to the different access procedures needed for each. Allowing too many points of access, however, can reduce the facility's control over entering and exiting vehicle traffic. References include FEMA 426 (Table 1-22 and Section 1.5) and USAF (1997).
1	3	Attended booths or parking offices are located so that activity at pedestrian and vehicle entry points to the facility can be monitored.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants increases when vehicular and pedestrian traffic entry and exit cannot be visually monitored by security personnel. The vulnerability to these threats can be reduced if personnel in attended booths or parking offices are able to observe traffic flow. Refer to countermeasures 1.1, 1.2, and 2.1 for further information concerning lighting for visual surveillance. References include ISC (2004).
1	4	Culverts, sewers, storm drains, concrete trenches, duct systems, and pipelines (that enter or go under the facility) have openings with no dimension greater than 6 in. (15 cm).	Unprotected utility tunnels, pipelines, manholes, stormwater runoff culverts, sewers, and concrete trenches can provide covert access and weapon concealment opportunities. This increases the facility's vulnerability to terrorist or criminal attack. Access to a building might be obtained through floor openings such as openings for shafts and ducts; utility tunnels or chases for heat, gas, water, electric power, and telephone; sewers and other types of drains; and other small service openings. To protect against unauthorized access via these routes, openings can be covered or secured. Various techniques and material can be used to give added protection to surface openings. Secure all penetrations with screening, grating, lattice work, or other similar devices such that openings do not allow intruder access. Expanded metal, wire fabric, grating, and fencing can be utilized. Manhole covers can be locked and periodically checked. Infrequently used manhole covers can be tack welded. Perimeter fencing should also be checked on a regular basis to find and repair washouts or other unwanted openings. References include FEMA 426 (Table 1-22 and Section 1.9) and USAF (1997).
1	5	Vegetation (bushes, trees, etc.) and other nonhardened landscape elements are used to control vehicle access.	Controlling vehicle access can reduce the facility's vulnerability to a vehicle bomb threat. Blast pressures from an exploding vehicle bomb decrease rapidly with distance from the explosion. Each foot of setback can be critically important. When a vehicle bomb is identified as a design threat, consider how the site design can offer maximum protection to the building, or whether site constraints require design modifications to the structure of the building. Setback is common terminology for the distance between a building and its associated roadway or parking. It is analogous to standoff between a vehicle bomb and the building. The benefit per foot of increased standoff between a potential vehicle bomb and a building is very high when close to a building and decreases rapidly as the distance increases. Landscape elements of various types and designs of buffers and barriers such as walls, fences, trenches, berms, ponds and water basins, plantings, trees, static barriers, sculpture, and street furniture can be used as a psychological deterrent to unauthorized vehicle access. References include U.S. General Services Administration (2005) and ISC (2004).

Discipline	Count	Countermeasure	Guidance
1	6	Adjacent street curb lane parking is restricted to key employee parking.	Controlling adjacent street curb lane parking in public rights-of-way can reduce the facility's vulnerability to a vehicle bomb threat. Where distance from the building to the nearest curb provides insufficient setback, restrict parking in the curb lane to key employees or prohibit parking in these areas. For typical city streets, this may require negotiating to close the curb lane. Note that the July 1, 1994, Americans with Disabilities Act Standards for Accessible Design states that required handicapped parking shall be located on the shortest accessible route of travel from adjacent parking to an accessible entrance. References include FEMA 426 (Table 1-22 and Section 1.3), U.S. General Services Administration (2005), and ISC (2004).
1	7	Site is designed to clearly identify property lines.	Territorial reinforcement is one of the design principles of the crime prevention through environmental design (CPTED) strategy. The CPTED process asks questions about territoriality, natural surveillance, and access control that can • Increase the effort to commit crime or terrorism, • Increase the risks to the perpetrator associated with crime or terrorism, • Reduce the awards associated with crime or terrorism, and • Remove the excuses as to why people do not comply with the rules and behave inappropriately. The CPTED process provides direction to solve the challenges of crime or terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods. Clearly identifying property lines can prevent unintentional intrusion and facilitate prosecution for criminal trespass. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
1	8	Under-building access to crawl spaces and utility tunnels is restricted.	Unprotected utility tunnels, pipelines, manholes, stormwater runoff culverts, sewers, and concrete trenches can provide covert access and weapon concealment opportunities. This increases the facility's vulnerability to terrorist or criminal action. Access can be gained through floor openings such as openings for shafts and ducts; utility tunnels or chases for heat, gas, water, electric power, and telephone; sewers and other types of drains; and other small service openings. To protect against unauthorized access via these routes, openings can be covered or secured. Various techniques and material can be used to give added protection to under-building openings, such as expanded metal, wire fabric, and fencing. Manhole covers can be locked and periodically checked. Infrequently used manhole covers can be tack welded. References include FEMA 426 (Table 1-22 and Section 1.9) and USAF (1997).
1	9	Security station or reception area is located where it is visible to the public and where the attendant can directly monitor entry/exit activity.	Territorial reinforcement is one of the design principles of the CPTED strategy. Maintaining awareness and control of visitors, vendors, and service personnel who request access to the facility is important. This can be accomplished by locating a contact person, such as a receptionist or security guard, at the entrance. A reception area or security station can also provide a deterrent to criminal activity. The receptionist can provide information, determine the purpose of the visit and the destination, and provide a sign-in/sign-out logbook and an identification tag or badge prior to access. Also, if the facility uses a system of escorted access, the receptionist can contact the staff member being visited or the maintenance department to request an escort. References include FEMA 426 (Table 1-22 and Section 2.7).

Discipline	Count	Countermeasure	Guidance
1	10	Design of stair towers and elevator lobbies ensures that people using these areas can be easily seen and can see out to reduce likelihood of assault.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants increases when visual openness decreases. The following measures, as applicable, can help to lower the vulnerability to these threats: • Stair tower and elevator lobby as open as code permits; • Stair and/or elevator waiting areas as open to the exterior and/or the parking areas as possible and well lit ; • Impact-resistant, laminated glass for stair towers and elevators as a way to provide visual openness; • Potential hiding places below stairs closed off; • Nooks and crannies avoided or eliminated; and • Dead-end parking areas avoided or eliminated References include FEMA 426 (Table 1-22 and Section 1.17), U.S. General Services Administration (2005), and ISC (2004).
1	11	Inside parking is restricted to selected employees only.	Uncontrolled parking inside or under the building could result in the introduction of a terrorist vehicle bomb into a highly vulnerable area. Parking restrictions help keep threats away from a building. In urban settings, however, inside or underground parking is often necessary and/or difficult to control. If underground or inside parking cannot be eliminated, the associated risks can be mitigated by various countermeasures dictated by the desired amount of protection for the building and its occupants. Among these are access control and barriers and structural hardening. The last countermeasure is usually quite expensive. For a lower level of protection, parking can be restricted to employees of the building. Higher levels of protection involve restricting parking to selected employees, or employees with a need for security, such as upper level management. Some form of access control is required at all protection levels. This may range from ID checks to some form of electronic control, such as card readers. References include FEMA 426 (Table 1-22 and Section 1.18), U.S. General Services Administration (2005), and ISC (2004). 2—Architectural
2	1	Pedestrian walkways concentrate activity.	Site planning and landscape design can provide natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities. This concept may also be used to prevent pedestrian access to parking areas other than via established entrances. Pedestrian paths can be planned to concentrate activity to the extent possible. For example, bringing all pedestrians through one portal rather than allowing them to disperse to numerous access points improves the ability to see and be seen by other users. References include FEMA 426 (Table 1-22 and Section 2.3), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	2	Parking facility has vehicular access control.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants increases when access to parking facilities is uncontrolled. On-site parking can be controlled with identification checks, security personnel, and access control systems. Inbound vehicle control can be either automated or semi-automated, or manual. In some locations both types are used, manual during busy periods and automated at other times. In the former, the driver utilizes a machine-readable device to open the gates or presents suitable identification to a remote control point via closed-circuit television (CCTV), audio transceiver, or both. In the manual control situation, a security person stationed at the point of entry makes the admittance decision. For large employee populations, especially when an identification card is already in use, installing card readers and mechanized gates may be an option. In smaller facilities or as an alternative to fully automated access controls, vehicle identification stickers and personnel at inbound gates can be used. To make this type of control effective against both unauthorized entry and removal of vehicles, a passive control device can be used at gates not staffed. References include FEMA 426 (Table 1-22 and Section 1.7), FEMA 386-7 (2002), ISC (2004), and Williams (2012).
2	3	Security screening or fencing has been provided at openings to discourage anyone from entering the parking facility on foot.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants increases when access to parking facilities is open to foot traffic. Security screening or fencing can be used to discourage pedestrian access to parking areas other than via established entrances. Expanded metal grilles can also be used to block off some openings. References include FEMA 426 (Table 1-22 and Section 2.3), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).
2	4	Streets, sidewalks, and building entrances clearly indicate public routes and direct people away from private or restricted areas.	Territorial reinforcement is one of the design principles of the CPTED strategy. It is useful in preventing unauthorized personnel from approaching private or restricted areas, thereby reducing the facility's vulnerability to unauthorized access and its attendant threats, such as attacks against personnel or critical facility components. The CPTED process asks questions about territoriality, natural surveillance, and access control that can • Increase the effort to commit crime or terrorism, • Increase the risks to the perpetrator associated with crime or terrorism, • Reduce the awards associated with crime or terrorism, and • Remove the excuses as to why people do not comply with the rules and behave inappropriately. The CPTED process provides direction to solve the challenges of crime or terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods. Employ design that distinguishes private or restricted spaces from public spaces using separation; landscape plantings; pavement designs (pathway and roadway placement); gateway treatments at lobbies, corridors, and door placement; and walls, barriers, signage, lighting, and CPTED fences. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	5	Access to private areas is discouraged with structural elements and limited access (no cut-through streets).	Natural access control is one of the design principles of the CPTED strategy. It is useful in discouraging access to private areas, thereby reducing the facility's vulnerability to unauthorized access and its attendant threats, such as attacks against personnel or critical facility components. The CPTED process asks questions about territoriality, natural surveillance, and access control that can • Increase the effort to commit crime or terrorism, • Increase the risks to the perpetrator associated with crime or terrorism, • Reduce the awards associated with crime or terrorism, and • Remove the excuses as to why people do not comply with the rules and behave inappropriately. The CPTED process provides direction to solve the challenges of crime or terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods. Public access cut-through streets or alleys provide easy access to the facility for vehicles and pedestrians and introduce threats from vehicle- and hand-carried bombs and weapons of mass destruction (WMDs). This is aggravated when the road separates multiple buildings or parts of buildings. Especially worrisome is the situation where a cut-through road or alley owned by the municipality passes through a tunnel or underpass between separate parts of the building or adjacent buildings. The situation can be improved if the owner works with municipal officials to eliminate public access by blocking the cut-through. If this is not possible, restricted access with owner control might be negotiated. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
2	6	Shrubbery is less than 2 ft (60 cm) in height.	Natural surveillance is one of the design principles of the CPTED strategy and is intended to prevent concealment of intruders or obstructing the view of security personnel and CCTV. The CPTED process asks questions about territoriality, natural surveillance, and access control that can • Increase the effort to commit crime or terrorism, • Increase the risks to the perpetrator associated with crime or terrorism, • Reduce the awards associated with crime or terrorism, and • Remove the excuses as to why people do not comply with the rules and behave inappropriately. The CPTED process provides direction to solve the challenges of crime or terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods. High shrubbery can conceal a standing or crouching intruder, allowing unobserved approach to the building envelope. Trimming shrubbery to a height of 2 ft (60 cm) or less decreases the facility's vulnerability to unauthorized access and the possible placement of an explosive device. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	7	Lower branches of existing trees are kept at least 10 ft (3 m) off the ground.	Natural surveillance is one of the design principles of the CPTED strategy and is intended to prevent concealment of intruders or obstructing the view of security personnel and CCTV. The CPTED process asks questions about territoriality, natural surveillance, and access control that can • Increase the effort to commit crime or terrorism, • Increase the risks to the perpetrator associated with crime or terrorism, • Reduce the awards associated with crime or terrorism, and • Remove the excuses as to why people do not comply with the rules and behave inappropriately. The CPTED process provides direction to solve the challenges of crime or terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods. Low tree branches can provide a concealment effect similar to high shrubbery, allowing unobserved approach to the building envelope. Trimming tree branches to 10 ft (3 m) or more off the ground decreases the facility's vulnerability to unauthorized access and the possible placement of an explosive device. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
2	8	Visitors (and their baggage) to facility are screened for weapons and explosives.	Screening visitors to the facility for weapons and explosives is important. This reduces the vulnerability to actions that accompany violent terrorist or criminal activity and acts related to domestic disputes. Without screening, facilities might be vulnerable to such threats as assault with a deadly weapon and hand-delivered bombs or WMDs. Screening policies and procedures, which have been reviewed and approved by legal counsel, are used to • Identify the personnel who will enforce the screening rules; • Train and periodically test the screening personnel; • Determine which situations will require participation of law enforcement personnel in the screening process; • Prescribe action to be taken when a visitor objects to screening; • Prescribe action to be taken upon discovery of weapons or explosives, including notification of bomb and hazardous material incident responders; and • Determine the disposition of weapons and contraband found, including legal and illegal weapons. Equipment that can be used in the screening process, in addition to visual inspection and baggage search, include walk-through and handheld metal detectors, X-ray inspection machines, explosives detectors, and, if the level of threat warrants, radiation detectors and chemical or biological agent detectors. If the nature of the threat warrants it, canines can be brought in to assist the inspectors. Most metropolitan police departments have canine units in which explosives detection animals are included. Bureau of Alcohol, Tobacco, Firearms, and Explosives (BATFE), the U.S. Customs Service, and the various military departments of the federal government also have explosives detection dogs. Airport law enforcement agencies in major gateway cities also use them. It is advisable to identify which nearby local or federal agencies have such animals and whether, in an emergency, they would be available for use in the private sector. References include FEMA 426 (Table 1-22 and Section 12.26) and Williams (2012).

Discipline	Count	Countermeasure	Guidance
2	9	Circulation routes have unobstructed views of people approaching controlled access points.	Obstructed views of the approach to controlled access points can give an advantage to an attacker intent on forcing entry past the control point or concealing an explosive or WMD device. The approaches to controlled access points should provide visual detection and monitoring of unauthorized personnel approaching controlled areas or occupied spaces. It can give security personnel the time to react to a suspicious person or object being carried. This countermeasure applies to perimeter entrances, building entrances, and critical areas within the building. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • Uninterruptible power source (UPS) systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Main refrigeration systems if critical to building operation; • Mechanical rooms containing heating, ventilating, and air conditioning (HVAC) equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms. References include FEMA 426 (Table 1-22 and Section 2.13), USAF (1997), and DoD (2002).
2	10	Signage identifying high-risk areas is minimized.	Signs can help an attacker (e.g., terrorist, militant, or vandal) identify potential targets. Eliminating or minimizing signage identifying high-risk, critical, and sensitive facilities can downplay their critical nature. However, there is a need for a balance between adequate signage to direct emergency responders, versus identifying the location of sensitive areas. One consideration in establishing a balance is to familiarize local emergency response personnel with these areas by conducting drills and walk-throughs, when feasible. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Main refrigeration systems if critical to building operation; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms. References include FEMA 426 (Table 1-22 and Section 1.22), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	11	Shelter-in-place locations are provided.	Protection of facility staff and visitors in some emergency situations, such as an exterior chemical, biological, and radiological (CBR) release by terrorists, or an unintentional hazardous material release, where people cannot be safely evacuated, may be best accomplished by the shelter-in-place concept. Shelter-in-place rooms or areas can be used for people to congregate in the event of an outdoor release. The advantage of sheltering in place is that it can be implemented rapidly. The disadvantage is that its protection is variable and diminishes with the duration of the hazard. Two distinct actions are required to be taken without delay: • Reduce the indoor–outdoor air exchange rate before the hazardous plume arrives; and • Increase the indoor–outdoor air exchange rate as soon as the hazardous plume has passed. The goal of sheltering in place is to create areas where outdoor air infiltration is very low. Such rooms will be in the inner part of the building in a room or area with no exterior windows (CDC/NIOSH 2002). Doors must be effective at preventing airflow; for example, sliding doors prevent pumping the large amounts of air into a room that a conventional swinging door allows. Supplies such as duct tape and plastic to further seal the area from hallways can be maintained in the room. The room should have emergency lighting. The locations of shelter-in-place rooms and when they should be used should be included in the facility Occupant Emergency Plan (OEP) or disaster management plan. References include FEMA 426 (Table 1-22 and Section 2.22), FEMA 386-7 (2002), and ISC (2004).
2	12	Sensitive areas are controlled by locks and physical barriers.	Locks and physical barriers can differentiate levels of security within a building and can deter and delay entry to high-risk, critical, and sensitive areas by an attacker (e.g., terrorists, militants, or vandals). While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Main refrigeration systems if critical to building operation; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms. References include FEMA 426 (Table 1-22 and Section 2.25) and USAF (1997).
2	13	Staff areas are separated from the public by locked doors and barriers.	Access controls between staff and public areas can slow down intruders. This can provide more time for security to react. Locks and physical barriers designed to resist forced entry and ballistic attack can be effective in this application. References include FEMA 426 (Table 1-22 and Section 2.25) and USAF (1997).

Discipline	Count	Countermeasure	Guidance
2	14	For lobby retail, control access to main building with separate entryways, access control, hardened partitions (against intrusion), and security operational measures is provided.	Permitting retail activities in nonsecured areas such as the building lobby is not advisable. However, the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting buildings. Consider separating entryways, controlling access, hardening shared partitions against intrusion (i.e., forced entry), and special security operational countermeasures such as guard patrols. References include FEMA 426 (Table 1-22 and Section 2.6), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
3—Structural			
3	1	Structural system is reinforced concrete (neither prestressed nor precast) or steel frame.	Structural frames, such as reinforced concrete or steel frames, offer higher redundancies than other structural systems. Connections must be detailed so as to offer high deformation capacity. The level of connection deformation must be consistent with the geometry of the building and the postulated threat. References include FEMA 426 (2003a).
3	2	Structural system is braced frame, shear wall, or bearing wall.	Shear walls or braced frames offer stiffer lateral behavior of the building. They also have an important function in providing stability to the whole building and need to be protected carefully. Because the number of bracing bays or shear walls are limited within the building plan, the redundancy level in this type of structural system is less than that of the framed structural system during a blast event. References include Ettouney et al. (2006).
3	3	Structural system is prestressed, or precast reinforced concrete system (slabs, beams, and/or columns) and blast and/or progressive collapse analysis were performed.	A progressive collapse or blast analysis of this class of buildings should include, but not be limited to, the effects of suddenly released energy due to the loss of prestressing in the damaged structural component(s), such as columns, beams, or slabs. In existing buildings, the condition of the prestressing tendons (for example, corrosion) must be accounted for in the analysis.

Discipline	Count	Countermeasure	Guidance
3	4	Structural system is either wood or light metal, and blast and/or progressive collapse analysis was performed.	A progressive collapse or blast analysis of this class of buildings should include, but not be limited to, (a) high-deformation behavior of connections, (b) flexibility of floor diaphragms, and (c) state of connectivity between structural members and nonstructural members such as partitions, envelope, and floors. In existing buildings, the condition of all components (for example, material properties, delamination, or loose connections) must be accounted for in the analysis.
3	5	There are no transfer girders within the structural system.	Lack of transfer girders in a structural system improves its resistance to progressive collapse.
3	6	Loading zones are separate from public parking.	Natural access control is one of the design principles of the CPTED strategy. The CPTED process asks questions about territoriality, natural surveillance, and access control that can • Increase the effort to commit crime or terrorism, • Increase the risks to the perpetrator associated with crime or terrorism, • Reduce the awards associated with crime or terrorism, and • Remove the excuses as to why people do not comply with the rules and behave inappropriately. The CPTED process provides direction to solve the challenges of crime or terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods. If public parking is allowed close to loading zones or docks, it increases the vulnerability to attack by terrorists, militants, or criminals via these areas. It also increases vulnerability to a vehicle bomb if the public parking area violates the facility's standoff requirements. Parking near such areas also allows undetected removal of material to vehicles. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
4—Building envelope			
4	1	The glazing has sufficient "bite."	A large glazing "bite" would ensure adequate anchoring between the glass and the supporting window framing. References include FEMA 426 (2003a) and FEMA 455 (2009).
4	2	Exterior walls are framed curtain walls (metal).	Curtain walls are light metal framed constructs. As such, they offer some ductile behavior during blast events. However, because of their light weight, they do not offer enough mass to slow the resulting accelerations. A proper dynamic analysis is needed to ensure adequate behavior during a postulated blast event, FEMA (2003).
4	3	Exterior walls are reinforced precast concrete panels, or reinforced masonry.	These types of walls offer some ductile behavior during blast events, when reinforced and anchored properly. Also, because of their heavier weights, they can offer some mass that can slow the resulting accelerations. A proper dynamic analysis is needed to ensure adequate behavior during a postulated blast event.

Discipline	Count	Countermeasure	Guidance
4	4	Exterior walls are nonreinforced masonry or nonreinforced concrete panels.	These types of walls offer negligible ductile behavior during blast events due to lack of reinforcements. If used, because of their brittle nature, the adequacy of their anchoring (including the anchor length) must be checked carefully during a postulated blast event.
4	5	Exterior walls are designed for high wind.	If the exterior walls are designed for high winds (such as tornado or hurricane conditions), their behavior during a blast event should be superior to other exterior walls.
5—Utilities			
5	1	Restrooms are provided with emergency lighting.	Emergency lighting in restrooms can facilitate evacuation and permit limited use during power outages when sheltering in place is required. Self-contained battery lighting in restrooms provides backup in case of emergency generator failure. A regular maintenance program for stairway and exit sign lighting (all egress lighting) ensures functioning under normal and emergency power conditions. References include FEMA 426 (Table 1-22 and Section 8.6), U.S. General Services Administration (2005), and ISC (2004).
5	2	Facility has an emergency power system or generator for life safety and security systems.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to life safety and security systems. Emergency power must be provided to essential building services, especially those required for life safety, evacuation, and sheltering in place, providing lighting and surveillance to deter and detect criminal activities and providing emergency communication. Such systems can include • Access control, • Alarms (intrusion detection), • Building control centers, • Communications, • Elevators, • Emergency lighting, • Fire suppression, and • HVAC (smoke removal). Besides installed generators to supply emergency power, portable generators or rental generators available under emergency contract can be quickly connected to a building with an exterior quick disconnect already installed. All emergency power systems must be tested on a regular basis. Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability. References include FEMA 426 (Table 1-22 and Section 5.18), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
6—Mechanical			
6	1	Air intakes have been located on the roof or as high on the building as practical, or ground-level outdoor air intakes have a security zone established by fencing or grilling or other means of physical protection.	One of the most important steps in protecting a building's indoor environment is the security of the outdoor air intakes. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system. Introducing CBR agents into the outdoor air intakes allows a terrorist to use the HVAC system as a means of dispersing the agent throughout a building. Publicly accessible outdoor air intakes located at or below ground level are at most risk—due partly to their accessibility (which also makes visual or audible identification easier) and partly because most CBR agent releases near a building will be close to the ground and may remain there. Securing the outdoor air intakes is a critical line of defense in limiting an external CBR attack on a building. Some buildings have air intakes that are difficult to access (e.g., on the roof, high on the building), but many others have intakes that are easily accessible and thus vulnerable. Physically inaccessible outdoor air intakes are the preferred protection strategy. When outdoor air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective alternative. Iron fencing or similar see-through barriers that will not obscure visual detection of terrorist activities or a deposited CBR source are preferred. The restricted area can also include an open buffer zone between the public areas and the intake louvers. Thus, individuals attempting to enter these protected areas will be more conspicuous to security personnel and the public. Effectively elevating intakes has practical limits. A plume or cloud of hazardous materials can reach intakes, particularly if the source is large and distant. For low-rise buildings (i.e., those having a width more than twice the height), a plume originating at ground level near the building will travel over the building rather than around it; thus, the wind will convey contaminants to the top of the building, with some dilution occurring. Various criteria and guidance sources give different heights above ground level for the preferred location of intakes; however, they agree on the basic principle of elevating the intakes. U.S. General Services Administration (2005) and ISC (2004) state that air intakes should be on the fourth floor or higher and, on buildings with three floors or fewer, they should be on the roof or as high as practical. Locating intakes high on a wall is preferred over a roof location. When choosing secure locations for intakes in urban areas, consider the vantage points offered to threats by nearby buildings and roofs. DoD (2002) states that, for all new inhabited buildings covered by this document, all air intakes should be located at least 3 m (10 ft) above the ground. CDC/NIOSH (2002) states, “An extension height of 12 feet (3.7 m) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes.” According to Lawrence Berkeley National Laboratory (2003), many large commercial buildings sometimes take in substantial amounts of outdoor air through what are intended to be the building exhausts. This phenomenon, which is contrary to the intent of the building designers and is often not recognized by building operators, is much more likely to occur during hot weather than at other times. DoD (2002) indicates that building exhaust registers may be more accessible to terrorists than building air intakes, because building designers often assume that there can be no inward flow through these registers and thus place them anywhere convenient. Common cases include exhaust registers located on or adjacent to loading docks or sidewalks. Setting the building HVAC for full exhaust will be highly effective in preventing a CBR agent from entering through the exhaust registers, once the release has been detected. However, preventing access to these registers in the first place, if it is practical to do so, would be a more effective measure for buildings that sometimes draw air through the exhaust registers. References include FEMA 426 (Table 1-22 and Section 6.1), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
6	2	Ventilation equipment is located away from high-risk areas such as loading docks, garages, mailrooms, and lobbies.	The continued operation of the mechanical system components during emergencies is an essential element of life safety, evacuation, refuge, and operations. Mailrooms, delivery areas such as loading docks, and areas with public access are the most likely locations for introducing toxic substances to a building. If the HVAC systems for these areas do not mix air into the rest of the building, the spread of the agent will be greatly reduced. Mixing into the general building air can be prevented either by providing a separate air-handling unit for these areas or by eliminating return air for these areas and exhausting them directly. In the event of a blast or event-related fires, the ventilation system may be essential to smoke removal, particularly in large, open spaces. In some facilities, a stairway pressurization system maintains positive pressure in stairways to minimize the entry of smoke and hazardous gases into stairways. This provides refuge and facilitates safe evacuation and access by firefighters. It is, therefore, important that ventilation equipment be located away from areas vulnerable to the introduction of an explosive device or airborne contaminant, such as loading docks, garages, mailrooms, and lobbies. If each of these areas with a significant risk for the introduction of airborne contaminants or explosive devices has a separate HVAC system, the effect of the event may be lessened. In some situations, these areas can be maintained at a negative pressure relative to the rest of the building but at a positive pressure relative to the outdoors. Physical isolation of these areas (well sealed floor to roof deck walls and sealed wall penetrations) is critical to maintaining the pressure differential. References include U.S. General Services Administration (2005), ISC (2004), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).
6	3	Return air vent grilles are secured from general access.	The return air system provides an avenue for dispersion of contaminants throughout the facility. The vulnerability to the threat of a terrorist chemical or biological attack from inside the building increases if the public has access to return air vent grilles. It is important that the air supply both to and from critical areas is inaccessible to the public, especially if the ductwork runs through the public areas of the building. Having a ducted air-handling system versus sharing hallways and plenums above drop ceilings for return air is also more secure. Nonducted systems provide greater opportunity for introducing contaminants. Return air grille protective measures include • Relocating return air grilles to inaccessible yet observable locations; • Increasing security presence (human or CCTV) near vulnerable return air grilles; • Directing public access away from return air grilles; and • Removing furniture and visual obstructions from areas near return air grilles. A terrorist who wants to maximize the casualties from an indoor chemical or biological attack, or to target specific people, can use knowledge of the building's ventilation system, such as how many ventilation zones the building has and which air vents serve which rooms, etc. The easiest way to determine these facts is from the building plans. Therefore, information on building operation, ventilation system details, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel. If plans are provided to contractors for building work, they should be recovered after use whenever possible. Building managers and maintenance personnel should be wary of requests for information about ventilation system details. References include FEMA 426 (Table 1-22 and Section 6.12), U.S. General Services Administration (2005), ISC (2004), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
6	4	Prerecorded message over the elevator cab speakers notifies passengers of an emergency and explains how to proceed.	Occupants of elevators may panic if they hear an emergency alarm. This can lead to injury and loss of life. In other cases, elevator occupants may not know of an emergency that has occurred. A prerecorded message can be delivered from the building fire control or security control rooms, via the elevator cab speakers, notifying passengers of an emergency and explaining how to proceed. Part of the message could instruct elevator occupants to use the elevator phone to make their presence known. This is particularly important if the elevator has stopped between floors. Provisions must be made for an override of recorded message with a live transmission with directions for a specific emergency. References include FEMA 426 (Table 1-22 and Section 6.20), U.S. General Services Administration (2005), and ISC (2004).
8—Electrical			
8	1	Emergency and normal electric panels, conduits, and switchgear are installed separately, at different locations, and as far apart as possible.	To ensure that emergency power is available for the protection of occupants during a terrorist attack or natural emergency, the emergency power equipment and distribution must be as far separated from the normal power supply as possible. This will prevent an act or incident from disabling both systems (i.e., a single point of failure). Emergency and normal electric panels, conduits, and switchgear should be installed separately, at different locations, and as far apart as possible. Electric distribution should also run at separate locations, not using the same conduits or chases. References include FEMA 426 (Table 1-22 and Section 5.18), U.S. General Services Administration (2005), and ISC (2004).
10—Communications and IT			
10	1	Mass communications system is used to make emergency announcements to building occupants.	In the event of a terrorist attack or other life-threatening emergency, a mass communications system that reaches all building occupants is necessary to provide warning and alert information, avoid panic, and inform occupants of actions to take before and after an incident. Mass communications systems can include a public address system, pager, cell phone, computer override, or a combination of these resources. Equipment redundancy and a source of emergency power are necessary to ensure adequate emergency communication with the occupants. References include FEMA 426 (Table 1-22 and Section 10.15), DoD (2002), and ISC (2004).
11—Equipment operations and maintenance			
11	1	Up-to-date composite drawings indicate location and capacities of major systems (electrical, mechanical, and fire protection).	A terrorist, criminal, or militant attack on the facility will require that critical infrastructure components function to mitigate its consequences. These include critical systems, if applicable, such as: • Electrical distribution; • Emergency electrical supply; • Telecommunications; • Mass communications; • Water supply (fire suppression and domestic water); • Wastewater removal; • HVAC; • Smoke removal (if separate from HVAC); • Security (intrusion detection, CCTV, communications, and automated access control); and • Life safety (fire alarm and suppression and emergency lighting). Within critical infrastructure protection at the building level, up-to-date composite drawings indicating location, current configuration, and capacity of all critical systems must be understood to ensure they meet emergency needs. These are also important aspects of operations and maintenance (O&M) and operations, security, and life safety training. References include FEMA 426 (Table 1-22 and Section 11.1) (2003a).

Discipline	Count	Countermeasure	Guidance
11	2	Updated operations and maintenance (O&M) manuals exist.	Arson, accidental fire, explosion, CBR contamination, and accidental hazardous material release are threats that could cause an emergency requiring manipulation of the HVAC system. The operation of mechanical system components during emergencies is an essential element of life safety, evacuation, refuge, and operations. Continuity of this system can be provided by an adequate O&M program. Within critical infrastructure protection at the building level, the current configuration and capacity of all critical systems must be understood to ensure they meet emergency needs. Manuals must also be current to ensure operations and maintenance keep these systems properly functioning. The system must function during an emergency unless directly affected by the hazard incident. References include FEMA 426 (Table 1-22 and Section 11.1) (2003a).
12—Security systems			
12	1	Parking facility and other remote areas have emergency intercom/duress buttons or assistance stations on structure columns, fences, other posts, and/or freestanding pedestals.	To reduce both the real exposure and the perceived risk of drivers and passengers to personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants, alarm devices can be installed at selected lot and garage locations. Alarm devices are basically switches, easily seen and activated, that transmit a signal to a remote monitoring point, or activate local features such as audible and visible alarms, or both. A mushroom-type button, installed on a lighting stanchion in open lots or on a post or pillar within an enclosed garage structure, transmits the alarm. Intercoms must be integrated and used to identify the emergency. For isolation and area identification purposes, assistance stations must be zoned in some fashion. In addition to the remote central monitoring of emergency alarm points, local enunciation at the point can alert others who might then be in the parking facility. A hum or other audible signal at the point where the device was actuated can be used. Another local device could be a strobe or flashing light. The visible signal would attract local attention and, in situations where a number of devices were zoned in common for remote enunciation, would permit patrol guard response directly to the location of the incident. References include FEMA 426 (Table 1-22 and Section 12.4), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).
12	2	Emergency intercom/duress buttons or assistance stations are brightly marked with striping or paint visible in low light.	To reduce both the real exposure and the perceived risk of drivers and passengers to personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants, alarm devices can be installed at selected lot and garage locations. Alarm devices are basically switches, easily seen and activated, that transmit a signal to a remote monitoring point, or activate local features such as audible and visible alarms, or both. A mushroom-type button, installed on a lighting stanchion in open lots or on a post or pillar within an enclosed garage structure, transmits the alarm. Intercoms and duress buttons can either be separate or integrated and used to identify the emergency. For isolation and area identification purposes, assistance stations must be zoned in some fashion. In addition to the remote central monitoring of emergency alarm points, local enunciation at the point can alert others who might then be in the parking facility. A hum or other audible signal at the point where the device was actuated can be used. Another local device could be a strobe or flashing light. The visible signal would attract local attention and, in situations where a number of devices were zoned in common for remote enunciation, would permit patrol guard response directly to the location of the incident. References include FEMA 426 (Table 1-22 and Section 12.4), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).

Discipline	Count	Countermeasure	Guidance
12	3	Staff identification (ID) system is implemented, and ID checks are performed to control access into the facility.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, hand-delivered bombs, and WMDs. Facilities maintain an identification system to facilitate access control, thereby ensuring that only authorized personnel enter controlled areas. Usually a facility-issued form of identification is employed. The employer or facility owner has the responsibility of making identification documents as reliable as the level of exposure demands. To the extent the document serves any purpose, it should be distinctive, not easily available, and not readily duplicated or counterfeited. The type of document to be issued depends in part upon the foreseeable circumstances in which it will be used for controlled access, inventory control, time and attendance, cashing checks, or charging meals or merchandise. Generally, access control is provided through main entrance points for employees and visitors and may range from visual identification by a guard (personal recognition) to electronic access control equipment using readers for • Magnetic coding, • Proximity or contact, • Resonant circuits, • Radio frequency, • Biometric technology, • Optical character, and • Smart card technology. The identification and access control system should consist of written policies concerning badge identification, badge replacement, and badge production. Badge identification: Important employee responsibilities, such as displaying a badge, must be part of the company security policy and adhered to by all levels of management. To have a meaningful personal identification system requires that all personnel display their badges when on the premises. This is the only method under which employees feel free to challenge personnel who are not displaying a badge. Facilities that only require visitors to display a badge are not effective. A visitor who removes the badge looks like a new employee, and no one will challenge him or her. Badge replacement: It is good practice to impose a charge for the issuance of replacement badges and make repeated badge losses without a satisfactory explanation a disciplinary infraction. If cards are replaced free of charge, you will find some employees with several cards in their briefcases. Rather than admit they have forgotten a badge, some employees will report it lost and have a new one issued. This can pose additional problems if the badge is not the photo type and is used to gain access to employee parking areas and to the facility interior. Badge production: An identification card can easily become an identification badge if it is originally designed with both functions in mind. Most medium and large companies purchase card production material, camera, and film and produce badges on site and as needed. If it is necessary to issue a large quantity of badges, such as for the initial installation of a badge system or replacement of all badges, there are badge production companies that will come to the facility with all the necessary equipment, supplies, and personnel to perform this service. Some of the basic requirements for a secure badge are • Resistive to surreptitious changes, • Use of holography, • Use of photograph for personal recognition, and • Lamination. Visitors, vendors, and service personnel should be issued temporary badges with sign-in/ sign-out requirements. Alternatively, stick-on badges are available, which are light sensitive and which, over a measured time period, display the word "VOID" and become illegible when exposed to light. The period during which the card will remain stable after exposure to light is brief, usually not more than eight hours. References include FEMA 426 (Table 1-22 and Section 2.7) and Williams (2012).

Discipline	Count	Countermeasure	Guidance
12	4	Key control systems are in place and are well maintained.	The mechanical lock and key has been the traditional access control system. Another mechanical locking system that can be used is based on use of a numeric combination rather than a key. Whether it is a mechanical lock and key system or a combination-based system, the benefits will be negated if the locking system is not professionally planned and administered. A system based upon a written policy can be used to • Require that a systematic approach be taken to the use of locks for security purposes, including key storage and check-out/check-in and combination control; • Assign specific responsibility for the development and maintenance of the locking program; • Make all persons who will use or have access to keys, locks, or combination information responsible for compliance with the program requirements; and • Ensure that all security locking arrangements on doors used for egress comply with NFPA 101 (2012). Some elements of a key control system that should be considered include • Authorization for possession of keys, master keys, and locks, including the period of time in possession; • Duplication of keys, including approved locksmith or on-site lock shop; • Reporting of lost or stolen keys, including authorization for replacement; • Disposition of keys upon employee transfer or termination; • Control of combinations to locking devices, including original setting of combinations, changes in setting of combination locking devices, and possession of combinations for locking devices; and • Use of locking devices, including restrictions on personal use. References include FEMA 426 (Table 1-22 and Section 12.29), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).
12	5	There are no areas of concealment for devices before screening points.	A risk exists that a terrorist or militant might conceal an explosive device that could injure or kill persons queued for screening. By avoiding features that can be used for concealment, such as mail or express boxes or trash receptacles, or restricting the size of the openings of these features in the areas before screening points, the vulnerability to concealed explosive packages can be reduced. Planters with dense foliage can also offer concealment; therefore removing them, or trimming the foliage, would also reduce vulnerability. References include ISC (2004) and Williams (2012).
12	6	Potentially hazardous chemicals and combustible or toxic materials are stored on site in secure and monitored areas.	Potentially hazardous chemicals and combustible or toxic materials stored on site represent an opportunity for a terrorist release of these materials. An intruder need not bring the material into the building if it is already there and accessible. This material could also be a source for increasing the severity of a primary attack with bombs and incendiaries. The storage, use, and handling locations should also be kept away from other high-risk areas that could be attacked, such as loading docks, mailrooms, and lobbies. Storage areas should be located to provide visual observation by security personnel and facility staff. References include FEMA 426 (Table 1-22 and Section 12.30).

Discipline	Count	Countermeasure	Guidance
12	7	Duress buttons are located at key public contact areas and as needed in the offices of managers and directors, in garages, and other areas that are identified as high-risk locations.	A potential for violence exists anywhere there is contact between facility staff and the public. Therefore, it is expedient to have a means of notifying the security force when it appears that a situation might get out of control. This can be accomplished by the use of a duress alarm system (also known as a panic alarm or hold-up alarm). A risk management assessment can identify locations that require this alarm system. One location, previously discussed in 12.1, is a parking facility assistance station containing a duress alarm. Duress alarm systems may be either hardwired or portable, using a radio frequency or microwave transmission to alert the security force or local law enforcement. The level of monitoring and the agency performing this duty vary with the level of protection, size, assets, complexity, and occupancy of the facility. Monitoring can be provided by a commercial central station, or an on-site security central control center can be provided during normal business hours. A more advanced measure of safety and security can be provided by monitoring at an on-site, proprietary security control center. To mitigate staffing requirements and annual operating costs, commercial central stations are sometimes used for after-hours monitoring or to supplement on-site monitoring. It is useful, when possible, to have CCTV coverage of the areas where duress buttons are located so that security control room personnel can appraise the situation that necessitated the alarm and direct security or law enforcement responders. References include FEMA 426 (Table 1-22 and Section 12.4), U.S. General Services Administration (2005), and ISC (2004).
12	8	Duress alarms are located in reception areas.	A potential for violence exists anywhere there is contact between facility staff and the public. Therefore, it is expedient to have a means of notifying the security force when it appears that a situation might get out of control. Reception areas are one location where such notification is recommended. References include FEMA 426 (Table 1-22 and Section 12.4), U.S. General Services Administration (2005), and ISC (2004).
12	9	All security system documents include current as-built drawings.	Drawings are critical to the consideration and operation of security technologies, including overall design and engineering processes. These historical reference documents outline system specifications and security devices used, including their application, location, and connectivity. They are a critical resource tool for troubleshooting system problems and replacing and adding other security system hardware and software products. Such documents should be an integral component to new and retrofit construction projects. Security system documents such as O&M manuals and training materials should include current as-built documents. References include FEMA 426 (Table 1-22 and Section 12.44).
12	10	Security system manuals are available.	A terrorist, criminal, or militant attack on the facility will require that security system components function to mitigate its consequences. Security systems also must operate on a normal daily basis. Manuals are required to facilitate operations, maintenance, and repair of systems and for training security personnel. Security systems that require up-to-date manuals include • Electronic access control, • Intrusion detection, • Duress alarm, • CCTV, • Communication, and • Active vehicle barrier. If security system maintenance is not performed by facility personnel, maintenance service agreements, including requirements for service employee background checks, should be in place for all security systems. References include FEMA 426 (Table 1-22 and Sections 12.47, 12.48).

Discipline	Count	Countermeasure	Guidance
13—Security master plan			
13	1	A written security plan exists for this site or building and has been communicated and disseminated to key management personnel and departments	The development and implementation of a written security master plan provides a roadmap that outlines the strategic direction and vision and operational, managerial, and technological mission, goals, and objectives of the organization's security program. The security plan should include requirements for • Employee and visitor building access control processing; • Elevator access and controlled usage; • Use and control of fire; • Emergency/disaster management; • Access to utilities and mechanical and machine rooms; • Shipping and receiving procedures; • Package control; • Company-wide standards; • Security's mission, reflecting that of the organization; and • Any other security objective that could be advanced through a design approach. The plan should apply the following concepts: • Deter: Visual evidence of a comprehensive security program will induce some perpetrators to look for other facilities where access would be less risky. • Detect and annunciate: Security's primary function is to prevent losses. The first step is to detect unauthorized intrusion and inform security that a penetration has occurred. • Delay: Once an intrusion has been detected, the perpetrator must be delayed for sufficient time to allow a response force to prevent a loss. • Deny access: Provide physical barriers to prevent access to assets at risk. • Apprehend: If possible the perpetrator should be apprehended in time to prevent malfeasance or recovery of assets and to deter future perpetrators. The security plan should be part of the building design so that the construction or renovation of the structure integrates with the security procedures to be used during daily operations. To be effective, the security plan must be enforced by all levels of management and department supervision. This requires that the plan, and any updates, be communicated and disseminated throughout the organization. An attitude may exist among employees that security measures are the exclusive task of the security department. Most organizations—almost all large ones that have formal security programs—devote at least some time to security orientation or security awareness. Yet knowing that a security program exists is not the same as playing an active role. There are specific activities that nonsecurity personnel can and should do in their own day-to-day routines that will enhance the entire security effort. Every department has a necessary role to play in the identification, prevention, and reduction of losses. The whole process of security vulnerability assessment involves both physical and the human elements. Once employees understand that they have a stake in the success of the security program, its ultimate success is much more likely. Some security programs are ineffective because the need for complete management support has not been efficiently stressed. When senior management delegates complete protection responsibility to lower level managers without top-level backing, the results are usually unsatisfactory. The program must be fully understood and supported at the top level in the enterprise, and senior management must be interested enough to ensure that all personnel follow the established requirements. The example, good or bad, set by senior executives in complying with requirements will permeate the organization. References include FEMA 426 (Table 1-22 and Sections 13.1, 13.2) and Williams (2012).
13	2	Security system as-built drawings have been generated.	Drawings are critical to the consideration and operation of security technologies, including overall design and engineering processes. These historical reference documents outline system specifications and security devices used, including their application, location, and connectivity. Current as-built drawings are necessary to avoid costly and possibly harmful mistakes when troubleshooting system problems and replacing and adding other security system hardware and software products. Such documents should be an integral component to new and retrofit construction projects. References include FEMA 426 (Table 1-22 and Section 12.39).

APPENDIX F

Countermeasure Commentary for Level 3, Silver

Discipline	Count	Countermeasure	Guidance
1—Site			
1	1	Design of the parking facility maximizes visibility and monitoring capability to the greatest extent possible.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants increases when visual openness decreases. The following measures, as applicable, can help to lower the vulnerability to these threats: • Stair tower and elevator lobby as open as code permits; • Stair and/or elevator waiting areas as open to the exterior and/or the parking areas as possible and well lit; • Impact-resistant, laminated glass for stair towers and elevators as a way to provide visual openness; • Potential hiding places below stairs closed off; • Nooks and crannies avoided or eliminated; and • Dead-end parking areas avoided or eliminated. References include FEMA 426 (Table 1-22 and Section 1.17) (2003a), U.S. General Services Administration (2005), and ISC (2004).
1	2	Site lighting has been coordinated with the CCTV system.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs. The vulnerability to intrusion through the perimeter and into restricted or controlled areas can be reduced by providing sufficient light for visual or closed-circuit television (CCTV) surveillance. Sufficient lighting and CCTV coverage in roadway access and parking areas also provides a deterrent to terrorist or criminal activities. For CCTV systems to be effective, the facility needs sufficient lighting. CCTV effectiveness can be achieved by coordinating site lighting with the CCTV system in use. The following considerations apply when lighting systems are intended to support CCTV assessment or surveillance: field of view of the camera, lighting intensity levels, maximum light-to-dark ratio, scene reflectance, daylight-to-darkness transitions, camera mounting systems relative to lighting, spectral response of the camera, cold start time, and restrike time.

Discipline	Count	Countermeasure	Guidance
			In the most general sense, the TV camera will “see” the same things the eye sees in any scene. But the various hues and shades of color perceived by the eye will be displayed as shades of gray by a black and white TV camera. They can only be rendered accurately with color cameras and monitors. Also, TV camera imagers may pick up and use light in the ultraviolet or infrared bands not visible to humans. The most important factors in regard to scene viewing are the quality and quantity of useful light available. Quality of light means its compatibility with the type of image sensor in the television camera. In most cameras prior to the mid 1980s, the imager would have been a vidicon or other type of vacuum tube. Today the imager is more likely to be a pixel (picture element) array in a charge-coupled device (CCD) camera. The characteristic differences between natural and artificial light and, in the latter class, between incandescent and fluorescent lights and mercury or sodium vapor lights, have an effect on the image picked up by the television camera. The differences are between the colors in the visible light emitted by each of the sources. Different areas of the visible spectrum are emphasized, and the effect is termed the “spectral response.” It is important that the camera selected for a particular scene be capable of acquiring at least a usable image and preferably full video in the spectral response area of the scene lighting. Analysis of camera specifications is a first step, but the most convincing test is to sample the scene under the expected lighting conditions, using the specific camera being considered. Even more important than light quality is light quantity. The amount of light needed to produce a TV image at the monitor is most directly stated in terms of the amount of illumination on the image sensor (solid state type) or faceplate (tube type) of the camera. This measure is the most useful because it is an absolute value and does not depend upon factors outside the CCTV system itself, such as the amount of light falling on the scene or the reflecting characteristics of surfaces in the scene. IESNA (2014), IESNA RP-20-98 (1998), IESNA RP-33-99 (1999), and ANSI/IESNA RP-8-00 (2000) provide guidelines for this subject. References include FEMA 426 (Table 1-22 and Section 1.20), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).
			2—Architectural
2	1	High-risk and low-risk offices are housed separately.	Terrorists or militants may identify some targets based on their symbology, visibility, ideology, political views, potential for publicity, or simply the consequences of their loss. Offices considered to be high risk (more likely to be targeted) should not be colocated with lower risk tenants. For example, a post office or supply center or room should not be located adjacent to a childcare center. Collateral damage may be incurred by low-risk offices if high-risk offices are attacked. If high-risk and low-risk offices are already housed together, they can be separated using gateway treatments such as walls, barriers, signage, and lighting at lobbies, corridors, and door placement. References include USAF (1997) and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	2	Public and employee entrances include space for possible future installation of access control and screening equipment for higher threat periods.	As discussed in countermeasures 2.5, 2.7, 12.5 and 12.6 of this table, screening for weapons and explosives is important because it reduces the vulnerability to violent terrorist or criminal activity and acts related to domestic disputes. Without screening, facilities might be vulnerable to such threats as assault with a deadly weapon and hand-delivered bombs or weapons of mass destruction (WMDs). If the facility does not currently perform such screening, or only screens visitors, it may become necessary in the future, under heightened levels of threat and alert, to introduce screening of visitors and/or staff. The entrances should be configured or remodeled to allow enough space for screening operations and equipment. Such equipment might include turnstiles, walk-through metal detectors, X-ray devices, chemical, biological, and radiological (CBR) detectors, search stations (with privacy partitions), and other technologies that may be developed. References include FEMA 426 (Table 1-22 and Section 2.10), U.S. General Services Administration (2005), and ISC (2004).
2	3	Public access areas are separated from high-risk offices.	High-risk offices that are not separated from public areas are at greater risk for attacks by criminals, terrorists, or militants because these elements can approach and enter with ease. Threats include assault, assault with a deadly weapon, assassination, kidnapping and hostage taking, robbery, and hand-delivered bombs. High-risk offices can be separated from public access areas using access control; gateway treatments, such as walls, barriers, and signage; and lighting at lobbies, corridors, and door placement. References include FEMA 426 (Table 1-22 and Section 2.17), USAF (1997), and ISC (2004).
2	4	Mailroom is at the perimeter of the building.	Mailrooms and mail-handling areas are vulnerable to the threat of a mail or package bomb sent by criminals, terrorists, or militants. Explosives in packages delivered through the mail can cause significant localized damage, injuries, and fatalities if they detonate inside a building. The mailroom should be located on the perimeter of the building. By locating the mailroom on the building perimeter, there is an opportunity to modify it in the future if a mail bomb threat is identified. Where mailrooms are located in the interior of buildings, few retrofit options are available for mitigating the mail bomb threat. References include FEMA 426 (Table 1-22 and Section 2.20), U.S. General Services Administration (2005), ISC (2004), DoD (2002), and USAF (1997).
2	5	Adequate room for explosive disposal containers and mail or package examination equipment is available in mailroom.	Screening deliveries from the U.S. mail and commercial package delivery services entering the facility for weapons and explosives is important. This reduces the vulnerability to actions that accompany violent terrorist or criminal activity. Without screening, facilities might be vulnerable to assault with a deadly weapon, assassination, mail or package bombs, or CBR agent release. A need may exist for explosive disposal containers in the event explosives are found. Disposal containers are used to contain a potential explosion, thus protecting the mailroom until the bomb squad arrives. The bomb squad can remove the container to a safe place for investigation and disposal of the suspicious item. Without disposal containers, the facility, occupants, and bomb squad members are exposed to the risk of a detonation if the mail or package does contain an explosive device. This inspection and disposal equipment can occupy significant space; therefore, adequate space for its accommodation should be provided. Future technology may provide additional inspection devices. Additional space for these should be considered. References include FEMA 426 (Table 1-22 and Section 2.21), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	6	Distance of at least 25 ft (7.5 m) separates mailroom from facility main entrances, utilities, areas containing critical services, distribution systems, and important assets.	Utility systems and other critical assets can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Distribution systems; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • Uninterruptible power supply (UPS) systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Mechanical rooms containing heating, ventilating, and air conditioning (HVAC) equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms and equipment. Mailrooms and mail-handling areas are among the most susceptible to the delivery of explosive materials. Maintaining distance between these areas and utilities, critical components, and important assets will reduce their vulnerability to bomb attack. A distance of 25 ft (7.5 m) is the generally accepted margin for the highest level of protection contained in the source criteria and guidance documents. However, 25 ft may not be available or required for all facilities. The reviewer must determine whether a separation exists between the mailrooms and assets. References include FEMA 426 (Table 1-22 and Sections 2.15, 8.3), DoD (2002), and ISC (2004).
2	7	Entrances have been designed to avoid significant queuing.	Excessive queuing at entrances can have adverse effects. Crowded conditions can conceal covert activity such as the placement of a hand-carried bomb, which, if detonated, could result in significant casualties. Long queues can result in a tendency to hurry the screening process, which might provide unauthorized access to people and weapons. If sufficient space exists inside the entrance, the queuing will occur within the building footprint. An adequate number of security personnel and sufficient inspection equipment should be provided to facilitate rapid processing of visitors and staff, especially at the opening of business, lunchtime, and close of business. The process can be facilitated by colocating or combining visitor and staff entrances. If space inside the entrance is insufficient, queuing should be expected outside the building, and a rain cover should be provided. References include FEMA 426 (Table 1-22 and Section 2.5), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	8	The security console and control room is adequate in size and provides room for expansion.	The security control center (SCC) is where security personnel monitor information, signals, and alarms from the security systems installed in and around the building. These include exterior and interior CCTV systems, intrusion-detection systems, and access control systems. The SCC can be used for remote operation of the equipment in these systems. It serves as a central location for decisions and actions that are required in security emergency situations. For example, additional forces can be dispatched from the SCC to the point of intrusion or duress. The SCC also serves as the control point for security personnel briefing and postassignment. The SCC should have an area where the following building documents will be readily available: • General, special, and post orders; • Emergency instructions; • Occupant Emergency Plan (OEP) manuals; • Building plans; • Alarm system plans and manuals; and • Fire codes. Whether it is a separate area or colocated with the fire command center and operations control center (which can enhance the ability to communicate in emergency situations), the security control area should be large enough to support all activities and have room for expansion in the event of future technological advances. The SCC should have adequate environment controls (e.g., air-conditioning (A/C), lighting, heating, air circulation, and backup power) to maximize functionality; it should be ergonomically designed to enhance the performance of the SCC personnel. References include FEMA 426 (Table 1-22 and Section 12.33) and Williams (2012).
3—Structural			
3	1	Drive-up/drop-off areas restrict parking and are not located under inhabited portions of the building.	Some facilities require access to areas for dropping off or picking up people or loading or unloading packages and other objects. Examples that may require drive-up/drop-off include, but are not limited to, medical facilities, hotels, childcare centers, and banks. A vehicle containing an explosive device could be especially destructive to inhabited portions of the building above the drive-up/drop-off area, possibly causing progressive collapse and casualties. Where operational or safety considerations require drive-up or drop-off areas or drive-through lanes near buildings, ensure those areas or lanes are clearly defined and marked and that their intended use is clear to prevent parking of vehicles in those areas. Do not allow unattended vehicles in drive-up or drop-off areas or drive-through lanes. Horizontal barriers or low ceilings can be used to prohibit entry by large vehicles. Do not allow drive-through lanes or drive-up/drop-off areas to be located under any inhabited portion of a building. References include ISC (2004) and DoD (2002).

Discipline	Count	Countermeasure	Guidance
3	2	Rated vehicle crash barriers are installed to prevent driving into or under the facility.	A terrorist vehicle bomb attack where the vehicle is driven into or under the building could result in catastrophic structural damage, injury, and death. Vehicle barriers of various types are designed to stop a vehicle before it can penetrate the perimeter of the building or the defended setback. The stopping power or rating is based on the weight of the vehicle and the maximum speed it can attain prior to striking the barrier. The desired barrier rating for a particular facility is based on the required level of protection identified in the risk assessment. Active barriers for entrances include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. Any barrier system proposed must meet impact requirements and be tested or otherwise certified by an independent testing lab or firm to meet or exceed the required vehicle size and impact velocity. Without proper site-specific design there is no assurance that such barriers will perform as required. References include FEMA 426 (Table 1-22 and Section 1.10), U.S. General Services Administration (2005), and ISC (2004).
3	3	Distance of at least 25 ft (7.5 m) separates main entrance, loading docks, shipping/receiving areas, vehicle circulation, and parking from utility mains, utility rooms, and other critical components and important assets.	Utility systems and other critical assets can suffer significant damage when subjected to the shock of an explosion. Some of these utilities and critical components may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Distribution systems; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms and equipment. Loading docks, shipping/receiving areas, vehicle circulation, and parking areas are among the most susceptible to the delivery of explosive materials. Maintaining distance between these areas and utilities, critical components, and important assets will reduce their vulnerability to bomb attack. A distance of 25 ft (7.5 m) is the generally accepted margin for a moderate level of protection contained in the source criteria and guidance documents. However, 25 ft may not be available or required for all facilities. The reviewer must determine a separation exists between delivery areas and critical areas.

Discipline	Count	Countermeasure	Guidance
3	4	Blast analysis has been performed to threat consistent with building classification. Acceptance limits are consistent with consequences used in the building classification.	Blast analysis involves the structural analysis of the building and related systems using advanced blast models and applications to determine the facility's vulnerability to the threat identified in the risk assessment. The blast analysis will help determine the necessary performance requirements of mitigation measures such as required standoff and facility hardening to meet the required level of protection. A blast analysis typically includes analysis of structural framing, exterior walls, roof systems, and window systems to determine the necessary performance of the structure under blast loads produced by the identified threat. The analysis must be performed by a qualified blast consultant. References include FEMA 426 (Table 1-22 and Section 3.5) and U.S. General Services Administration (2005).
3	5	Fire protection engineer has coordinated with the blast consultant on issues affecting life safety and building egress.	A fire protection engineering analysis should be done whenever a blast analysis is required. A fire protection engineer should coordinate with the blast engineer on issues affecting life safety and building egress. Use performance-based fire protection as outlined in NFPA (2000). The fire protection analysis should be performed by a qualified fire protection consultant. Fire safety is an important consideration in blast-resistant window design. A fire protection engineer should evaluate the performance requirements for all security glazing materials proposed for a facility. Normal tools carried by firefighters, such as a pick head axe, halligan tool, or similar device, may not readily overcome ordinary glazing barriers. If the use of more specialized tools, such as a rabbit tool, a k-tool, circular saws, rams, or similar devices is necessary to break through the glazing barrier or if the glazing itself is hardened so that high pressures may not blow out the windows, alternative methods or systems to ensure that smoke from an incident is not trapped inside the building must be implemented. References include FEMA 426 (Table 1-22 and Section 3.5) and ISC (2004).
3	6	Progressive collapse analysis has been performed to threat consistent with building classification. Acceptance limits are consistent with consequences used in the building classification.	Progressive collapse is defined as a situation whereby failure of a primary structural component leads to the collapse of adjoining members, which in turn leads to additional collapse. Hence, the extent of total damage is disproportionate to the original cause. Another way of describing progressive collapse is a chain reaction, or propagation of failures, following damage to a relatively small portion of a structure. Such damage may result in upper floors of a building collapsing onto lower floors. Progressive collapse can be initiated by a variety of events including the following: • Accidental or deliberate impact: Several cases of progressive collapse have been caused by accidental impact. An example of this type of abnormal loading is an automobile striking a key load-bearing member in a structure (i.e., building, bridge, etc.). The aircraft that impacted the Pentagon and the World Trade Center towers on September 11, 2001, are examples of deliberate impacts that initiated collapse of the target structures. • Faulty construction practice: In several instances, poor construction practices have led to progressive collapse. A notable example of this was the collapse of the Skyline Plaza apartment building in Fairfax County, Virginia. This failure was attributed to the premature removal of supporting forms, which initiated localized failure followed by a progressive collapse of the northwest corner of the structure. • Foundation failure: Failure of a small section of a structure's foundation can result in a loss of primary structural support. This failure may be the result of erosion, geology, overload, etc. If the remainder of the structure is unable to redistribute this change in load, damage to the structure could be much larger than the initial foundation failure. • Violent change in air pressure: An extreme change in air pressure can stem from many sources such as explosions created by gas or TNT. An example of progressive collapse that resulted from a severe change in air pressure was the 1995 terrorist bombing of the A.P. Murrah Federal Building in Oklahoma City, Oklahoma.

Discipline	Count	Countermeasure	Guidance
			Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-02 (2003). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted. An analysis determines the susceptibility of a building to progressive collapse. Structures must be analyzed according to requirements for new construction, and a written report must clearly state the potential vulnerability of the building to progressive collapse. This report should be used as a planning tool to reduce risk. Findings of the design analysis must be incorporated into the facility's risk assessment and include the methodology, the details of the progressive collapse analysis, retrofit recommendations, cost estimates, and supporting calculations. The analysis methods are too complex to be discussed in this guide. For details and references concerning progressive collapse analysis, refer to Section 8 of U.S. General Services Administration. (2005). References include FEMA 426 (Table 1-22 and Section 3.6), U.S. General Services Administration (2005), and DoD (2005).
3	7	All hardened or protection systems are properly anchored to the ground.	A continuous and adequately stiff and strong load path from the loading source to the ground needs to be analyzed and detailed properly. This includes the analysis of the pertinent foundation system and the underlying soil.
4—Building envelope			
4	1	Measures such as window film, blast curtain, and blast shield have been implemented to mitigate secondary debris (primarily glass fragmentation) caused by abnormal loadings.	A terrorist vehicle bomb driven near or into the building or a hand-carried bomb placed close to the building creates secondary debris when detonated. In past explosive events where there was no building collapse, a large number of injuries resulted from flying glass fragments and debris from walls, ceilings, and fixtures (nonstructural features). The glass used in most windows breaks at very low blast pressures, resulting in hazardous, daggerlike shards. Minimizing those hazards by reducing window numbers and sizes and enhancing window construction has a major effect on limiting mass casualties. Hazardous fragments may also include secondary debris such as that from barriers and site furnishings. The performance of the glass depends on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened, or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to less than 40% of the building envelope's vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows, an architect may favor window curtain walls, building codes require so much fenestration per measure of floor area, fire codes require a prescribed window opening area if the window is a designated escape route, and the building owner has cost concerns.

Discipline	Count	Countermeasure	Guidance
			Measures that can be used to reduce glass fragmentation include • Using laminated glazing; • Providing protection with an antishatter (fragment retention) film, a minimum of 7-mil thick film, or specially manufactured 4-mil thick film; • Applying structural silicone to glazing systems with a 1/2-in. (3/4-in. is better) bite; • Ensuring the window system design on the exterior façade is balanced (i.e., glazing, frames, and anchorage to supporting walls) to mitigate the hazardous effects of flying glazing following an explosive event; and • Using window treatments such as a blast curtain or shield. Ideally, an owner would want 100% of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat/weapon size at the expected standoff distance). However, economics and geometry may allow 80 to 90% due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher). References include FEMA 426 (Table 1-22 and Section 4.2), DoD (2002), U.S. General Services Administration (2005), and ISC (2004).
4	2	Interior glazing has been minimized and is shatter resistant where blast and/or forced entry threats exist, such as in lobbies, mailrooms, etc.	A terrorist hand-carried bomb placed close to areas with interior glazing, or a mail/package bomb within the building creates secondary debris when detonated. In past explosive events where there was no building collapse, a large number of injuries resulted from flying glass fragments and debris from walls, ceilings, and fixtures (nonstructural features). The glass used in most windows breaks at very low blast pressures, resulting in hazardous, daggerlike shards. Interior glazing should be avoided in enclosures of critical functions next to high-risk areas. References include FEMA 426 (Table 1-22 and Section 2.27), U.S. General Services Administration (2005), and ISC (2004).
4	3	Antishatter or antiglare films on glazing are utilized.	Antishatter or antiglare films on glazing would provide additional strength to otherwise highly brittle glazing. A proper anchoring between the glazing and the supporting frame needs to be provided in this situation. References include FEMA 426 (2003a) and FEMA 455 (2009).
4	4	All components of building envelope are attached to one another appropriately.	Building envelopes can have several components, such as glazing, frames, adhesives, and/or anchors. For proper behavior during blast events, all of those components must be capable of transferring the blast loading adequately to the supporting structural system.
5—Utilities			
5	1	Incoming utility systems have been concealed and/or secured.	Protecting utility systems, locating them away from vulnerable areas, and restricting access help ensure that services will facilitate life safety and operations support after an event such as a terrorist attack or other emergency. For the greatest protection within building and property lines, conceal incoming utility systems by means such as burial or proper encasement, wherever possible. Utility systems should be located away from loading docks, entrances, and parking. Underground service is preferred. Typically, inside the building the service entrance is a locked room, inaccessible to the public. Refer to 2.2 and 2.6 for information on protecting service entrances. References include Table 1-22 and Section 5.17 of FEMA 426 (2003a), ISC (2004), and FEMA 455 (2009).

Discipline	Count	Countermeasure	Guidance
5	2	Manhole covers have locks.	Unprotected manholes for utility tunnels, pipelines, stormwater runoff culverts, sewers, and concrete trenches can provide covert access and weapon concealment opportunities. This increases the facility's vulnerability to terrorist or criminal attack. To protect against unauthorized access to the perimeter and building via manholes, covers can be locked and periodically checked. Infrequently used manhole covers could be tack welded. References include FEMA 426 (Table 1-22 and Section 1.9) and USAF (1997).
5	3	Emergency generator fuel tank is located away from building.	An explosion of the fuel tank, whether accidental or as a result of a terrorist attack, could severely damage the building and injure its occupants. The fuel tank should be located as far as practicable from the building. References include FEMA 426 (Table 1-22 and Section 5.11), U.S. General Services Administration (2005), and ISC (2004).
5	4	Emergency generator fuel tank is secured with locked enclosure and/or intrusion detection.	An explosion of the fuel tank as a result of a terrorist attack could severely damage the building and injure its occupants. Access to the main fuel tank and day tank should be restricted and protected (e.g., locks on caps and seals). The appropriate intrusion-detection system(s), depending on the location, should be provided. References include FEMA 426 (Table 1-22 and Section 5.11), U.S. General Services Administration (2005), and ISC (2004).
5	5	Emergency generator is located away from loading docks, entrances, and parking.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to life safety and security systems. Emergency power must be provided to essential building services, especially those required for life safety, evacuation, and shelter in place, providing lighting and surveillance to deter and detect criminal activities and providing emergency communication. Such systems can include, if applicable, • Access control, • Alarms, • Building control centers, • Communications, • Elevators, • Emergency lighting, • Fire suppression, and • HVAC (smoke removal). The emergency generator should be located away from loading docks, entrances, and parking. These are high-risk areas for a vehicle bomb. Also, entrances are high-traffic areas that could facilitate placement of a hand-carried bomb or tampering with the generator. More secure locations include the roof, protected grade level with adequate drainage, and protected interior areas. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a), U.S. General Services Administration (2005), and ISC (2004).
5	6	Emergency generator is located away from areas prone to flooding.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to life safety and security systems. Emergency power must be provided to essential building services, especially those required for life safety, evacuation, and shelter in place, providing lighting and surveillance to deter and detect criminal activities and providing emergency communication. The generator should not be located in any areas that are prone to flooding. More secure locations include the roof, protected grade level with adequate drainage, and protected interior areas. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
6—Mechanical			
6	1	Air-handling system utilizes a high-efficiency particulate air (HEPA) filter or functional equivalent on all air-handling units (AHUs), including outside units, and in the supply air stream of recirculating AHUs.	Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern are the airflow patterns and dynamics in buildings, specifically in the building heating, ventilating, and air conditioning (HVAC) systems. These systems can become an entry point and a distribution system for hazardous contaminants, particularly CBR agents. Most building HVAC systems have some type of particle filter. Substitution of a more effective filter (particularly for small particle sizes) can reduce the risk of spreading a biological agent through the building via the HVAC system. Most airborne biological agents are between 1 and 10 µm in diameter, and virtually all are between 0.5 µm and 15 µm. Most ventilation filters are very effective at removing particles larger than 10 µm, and some filters are very effective at removing particles between 3 and 10 µm, while only the best filters are very effective at removing particles smaller than 3 µm. The American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) has developed a standard test procedure for classifying filters using a minimum efficiency reporting value (MERV)—the higher the MERV, the better the filter. A filter with a MERV rating of 13 or higher, located so that it filters both recirculated air and air from the outdoor air intakes, will eliminate most biological agents from the HVAC supply air, if they are introduced upstream of the filter. A filter with a MERV rating of 9 or higher will be very effective at removing particles larger than about 5 µm, but the effectiveness falls off quickly with smaller sizes, and about 80% of 1 µm particles will pass through a filter rated 8 and below. Filters below MERV 13 should be upgraded to HEPA filters. In the size range of airborne biological agents, each step upward in MERV rating has substantial benefits, up to about MERV 13. Beyond that, there is little benefit to filters with a higher MERV rating (including HEPA filters). Increasing filter efficiency is one of the few measures that can be implemented in advance to reduce the consequences of both an interior and exterior release of a particulate CBR agent. However, the decision to increase efficiency should be made cautiously, with a careful understanding of the protective limitations resulting from the upgrade. The filtration needs of a building should be assessed with a view to implementing the highest filtration efficiency that is compatible with the installed HVAC system and its required operating parameters. In general, increased filter efficiency will provide benefits to the indoor environmental quality of the building. However, the increased protection from CBR aerosols will occur only if the filtration efficiency increase applies to the particle size range and physical state of the CBR contaminant. It is important to note that particulate air filters are used for biological and radiological particles and are not effective for gases and vapors typical of chemical attacks. These types of compounds require adsorbent filters (i.e., activated carbon or other sorbent-type media) and result in substantial initial and recurring costs. More effective filters can lead to a significant pressure drop, which can pull unfiltered air around the filter or through leaks in ducts between the filter and the fan. To minimize or eliminate increases in pressure drop, deep pleated filters or filter banks with larger inlet area can be used if space allows. Improved filters can provide significant protection from a biological release, but they should be installed correctly and duct leaks should be sealed to reduce air bypass. Installing new filters may also require changes in other equipment (e.g., fan capacity may need to be increased) to maintain air quality and comfort and may increase energy use, so it should be done only after careful evaluation. For a low level of protection, use of a MERV 13 filter is acceptable. For moderate to high levels of protection, a HEPA filter or functional equivalent should be used on all air-handling units (AHUs), including outside ones and in the supply air stream of recirculating AHUs. One functional equivalent may be ultraviolet germicidal irradiation (UVGI) lamps in combination with MERV 13 filters, when UVGI lamps meet performance standards. (Current research must be further developed and tested to support this technology.) Where no recirculating AHUs exist (e.g., when local fan coil units or heat pumps are used), install HEPA filters in the outside AHUs only. For greatest protection, recirculating AHUs are required. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a), CDC/NIOSH (2002), Lawrence Berkeley National Laboratory (2003), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
6	2	Intrusion detection, CCTV, and/or security guards are implemented to protect air intakes.	One of the most important steps in protecting a building's indoor environment is the security of the outdoor air intakes. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system. Introducing CBR agents into the outdoor air intakes allows a terrorist to use the HVAC system as a means of dispersing the agent throughout a building. Publicly accessible outdoor air intakes located at or below ground level are at most risk—partly because of their accessibility (which also makes visual or audible identification easier) and partly because most CBR agent releases near a building will be close to the ground and may remain there. Securing the outdoor air intakes is a critical line of defense in limiting an external CBR attack on a building. Some buildings have air intakes that are difficult to access (e.g., on the roof or high on the building), but many others have intakes that are easily accessible and thus vulnerable. Physically inaccessible outdoor air intakes are the preferred protection strategy. When outdoor air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective alternative. Iron fencing or similar see-through barriers that will not obscure visual detection of terrorist activities or a deposited CBR source are preferred. The restricted area can also include an open buffer zone between the public areas and the intake louvers. Thus, individuals attempting to enter these protected areas will be more conspicuous to security personnel and the public. Monitoring the buffer zone with security guards, CCTV, security lighting, or intrusion-detection sensors will enhance this protective approach. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a), CDC/NIOSH (2002), Lawrence Berkeley National Laboratory (2003), U.S. General Services Administration (2005), ISC (2004), and DoD (2002).
6	3	Wiring for power and ventilation system controls is protected by conduit encasement.	Access to any component of the building automation and control system could compromise the functioning of the system, increasing vulnerability to a hazard or precluding its proper operation during a hazard incident. A terrorist with access to a building's HVAC equipment can quickly contaminate the entire building, or at least an entire ventilation zone, with a chemical or biological agent. The rooms that contain HVAC equipment should be locked and keyed so that they can be opened only by authorized staff. Power and control wiring for HVAC equipment should be encased in metal conduit. The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a), FEMA 386-7 (2002), and Lawrence Berkeley National Laboratory (2003).
7—Plumbing and gas			
7	1	Gas storage tanks (heating, cooking, medical, process) are located at least 50 ft (15 m) from personnel areas	The concern is that gas tanks and piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher risk area. A potential explosion or fire should not be allowed to impact personnel areas. A standoff distance of 50 ft (15 m) is considered by ISC (2004) to offer a high level of protection from collateral damage associated with attack on high-risk areas such as loading docks and other delivery vehicle loading/unloading areas. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a) and ISC (2004).
7	2	Exterior gas lines are piped below ground to the distribution system.	Similar to gas storage tanks, aboveground gas piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher risk area. Gas supply lines should be piped to the distribution system underground. Parts of the gas distribution system close to the building that are exposed (e.g., meters or valves) should be protected with antiram barriers and enclosures (e.g., fencing or expanded metal cages). Gates to enclosures should be secured with locks and access to keys strictly controlled. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a).

Discipline	Count	Countermeasure	Guidance
8—Electrical			
8	1	Emergency backup power exists for all critical areas.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to critical areas of the facility. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Main refrigeration systems if critical to building operation; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a), U.S. General Services Administration (2005), and ISC (2004).
8	2	There is redundancy of emergency power distribution to critical areas. Runs are separated.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to critical areas of the facility. The nature of the incident could affect the emergency power distribution system either directly or collaterally. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Main refrigeration systems if critical to building operation; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms. There should be redundant emergency power distribution to these critical areas. No single critical node should allow both the emergency backup power supply and redundant emergency backup power supply to be affected by a single incident. Two or more emergency backup power distribution systems should be separated as much as possible. The redundant distribution systems for emergency backup power should be separated as much as possible from the normal electrical distribution system. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a).

Discipline	Count	Countermeasure	Guidance
8	3	Electrical distribution panels serving branch circuits are secured.	Single runs of electrical distribution are at risk for single-point failure if subjected to a terrorist attack or an accident. Multiple electric distribution runs, separated as much as possible and not located near high-risk areas, should be used. In addition, critical electrical systems should not be colocated with other building systems. Critical electrical systems should not be located in areas outside of secured electrical areas. Colocation concerns include rooms, ceilings, raceways, conduits, panels, and risers. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a).
8	4	Electrical distribution panels serving branch circuits are secured.	Electrical power is essential for operating systems and equipment to mitigate the impact of a terrorist, militant, or criminal attack. Electrical distribution panels serving branch circuits should not be located in areas accessible to the public. Panels should be locked or in locked rooms with access to keys strictly controlled. Refer to countermeasures 2.3 and 12.4 in this table for a discussion of key control. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a). 9—Fire
9	1	Alarm and information systems (annunciator, radio system) are colocated.	Receipt of an alarm signal from, for example, a perimeter intrusion by terrorists, criminals, or militants intent on harming the facility, calls for action on the part of security personnel. Likewise, receipt of a fire alarm calls for immediate action. Colocating a radio system, telephone, or other information communication system with the alarm annunciator reduces the reaction time in summoning the appropriate response forces. References include Table 1-22 and Section 8.5 in FEMA 426 (2003a).
9	2	Alarm and information systems are collected and mounted in separate conduits.	As discussed in countermeasure 9.1, colocating alarm annunciators with information communication systems is essential to providing a fast reaction time. However, to avoid the possibility of a single failure occurrence disrupting both the alarm and communication systems, transmission lines for these signals should be collected separately and mounted in separate conduits. References include FEMA 426 (Table 1-22 and Section 9.3).
9	3	Facility has a fire command center (FCC).	An FCC is where information, signals, and alarms from the fire alarm and suppression systems installed in the building are monitored. The FCC can be used for remote operation of the equipment in these systems. It serves as a central location for decisions and actions that are required in blast or fire situations. For example, if the smoke removal system is not part of the HVAC system, it can be operated to mitigate a terrorist bomb or incendiary attack or a fire incident. The FCC should have redundant capability for voice and data transmission and mass communication. A backup power source should be provided. An area in the fire command center should be designated where the following building documents will be readily available: • Emergency instructions, • OEP manuals, • Building plans, • Fire suppression plans and manuals, and • Fire codes. Colocation with the operations control center and security control center, if applicable, can enhance the ability to communicate in emergency situations. References include FEMA 426 (Table 1-22 and Section 10.16), ISC (2004), and Williams (2012).

Discipline	Count	Countermeasure	Guidance
9	4	Facility has a security control center (SCC).	The SCC is where security personnel monitor information, signals, and alarms from the security systems installed in and around the building. These include exterior and interior CCTV systems, intrusion-detection systems, and access-control systems. The SCC can be used for remote operation of the equipment in these systems. It serves as a central location for decisions and actions that are required in security emergency situations. For example, additional forces can be dispatched from the SCC to the point of intrusion or duress. The SCC also serves as the control point for security personnel briefing and postassignment. The SCC should have redundant capability for voice and data transmission and mass communication. A backup power source should be provided. An area in the security control center should be designated where the following building documents will be readily available: • General, special, and post orders; • Emergency instructions; • OEP manuals; • Building plans; • Alarm system plans and manuals; and • Fire codes. Colocation with the fire command center and operations control center, if feasible, can enhance the ability to communicate in emergency situations. References include FEMA 426 (Table 1-22 and Section 10.16), ISC (2004), and Williams (2012).
9	5	There is a button in the FCC to recall elevators to an alternative floor if the elevators could safely be used to evacuate disabled persons or if the normal evacuation route would involve traveling through a high-risk area.	In a fire emergency, people are generally directed to use the stairways rather than elevators. However, in some emergencies the elevators could be safely used to evacuate disabled persons or if the normal evacuation route would involve traveling through a high-risk area. Consistent with the facility's OEP, a button can be provided on the FCC console to recall elevators to an alternative floor if the elevators could safely be used. An OEP may prefer that elevators not discharge personnel on the first floor (lobby) during some events. The requirements of ASME (2011) must be considered. References include FEMA 426 (Table 1-22 and Section 6.20), U.S. General Services Administration (2005), and ISC (2004).
9	6	Fire protection engineering analysis has been completed for fire suppression, evacuation capabilities, and secure locations.	Fire, whether arson or accidental, can be catastrophic, resulting in injury, loss of life, and property destruction. A fire protection analysis should be completed for fire suppression and evacuation capabilities. The analysis should include all fire protection and life safety systems, including but not limited to building construction, occupancy classifications, means of egress, water supply, fire alarm system(s), water-based fire extinguishing systems, non-water-based fire extinguishing systems, fire dynamics calculations, egress calculations, and smoke-control calculations. A range of scenarios may result from some of the design events. For example, simultaneous fires may break out on multiple floors, or the electronic fire protection system, communications, and sprinkler system may be disabled. Some events may require coordination of fire and CBR protective measures; sheltering in place, as opposed to evacuation, may be required. Consider the risks associated with occupants utilizing exit stairs that are infiltrated by heat, smoke, and fire gases due to an unwanted event. One possible solution may be to incorporate smokeproof enclosures within the facility to limit the infiltration of heat, smoke, and fire gases from a fire in any part of the building. The smokeproof enclosures may be permitted to be created by using natural ventilation, by using mechanical ventilation incorporating a vestibule, or by pressurizing the exit stair enclosure.

Discipline	Count	Countermeasure	Guidance
			The water supply, dual fire pumps, and standpipe connection should be protected and/or located away from vulnerable areas to help ensure that services will provide life safety and operations support after an event. The fire protection analysis must be performed by a qualified fire protection consultant. For design basis events, use performance-based fire protection as outlined in NFPA (2000). Fire analysis is consistent with building codes and applies only to the design basis events. References include FEMA 426 (Table 1-22 and Section 5.6), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
			10—Communications and IT
10	1	The interior cameras are supported by an uninterruptible power supply source, battery, or building emergency power.	CCTV can be a valuable tool for deterring terrorists, criminals, and militants from attacking a facility or identifying an intrusion or potential attack (i.e., alarm assessment). CCTV systems are also useful for monitoring egress through emergency exits. They are also used for automating and monitoring access to mechanical, electrical, gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms. Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power should be provided to security systems, including the interior CCTV systems. Various sources of emergency power can be UPS systems, including batteries, power conditioners, and emergency generators. References include FEMA 426 (Table 1-22 and Section 12.18).
			11—Equipment operations and maintenance
11	1	Procedures and preventive maintenance schedules for cleaning and maintaining ventilation system components are in place.	All buildings should have current emergency plans to address fire, weather, and other types of emergencies. In light of past U.S. experiences with anthrax and similar threats, these plans should be updated to consider CBR attack scenarios and the associated procedures for communicating instructions to building occupants; identifying suitable shelter-in-place areas (if they exist); identifying appropriate use and selection of personal protective equipment (i.e., clothing, gloves, and respirators); and directing emergency evacuations. The effectiveness of CBR protective measures depends on proper installation and maintenance, including changing filters regularly. Procedures and preventive maintenance schedules should be implemented for cleaning and maintaining ventilation system components. Replacement filters, parts, and so forth should be obtained from known manufacturers and examined prior to installation. Maintaining and cleaning ventilation systems according to the manufacturer's specifications is important. To do this requires information on HVAC system performance, flow rates, damper modulation and closure, sensor calibration, filter pressure loss, filter leakage, and filter change-out recommendations. These steps are critical to ensure that protection and mitigation systems, such as particulate filtration, operate as intended. Periodic training of HVAC maintenance staff in system operation and maintenance should be conducted. This training should include the procedures to be followed in the event of a suspected CBR agent release. Training should also cover health and safety aspects for maintenance personnel and the potential health consequences to occupants of poorly performing systems. Development of current, accurate HVAC diagrams and HVAC system labeling protocols should be addressed. These documents can be of great value in the event of a CBR release. References include FEMA 426 (Table 1-22 and Section 11.5), CDC/NIOSH (2002), Lawrence Berkeley National Laboratory (2003), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
12—Security systems			
12	1	Alarm-actuated CCTV cameras monitor and record assistance stations.	To reduce both the real exposure and the perceived risk of drivers and passengers to criminal or terrorist activities such as personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants, alarm devices (assistance stations) are installed in the parking garage or at parking lot locations. The efficiency of monitoring multiple screens decreases as the number of screens increases. Integrating the alarm system to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Alarm-actuated (or activated) CCTV coverage of assistance stations can assist the security force in identifying the situation and determining response requirements. For deterrence and to aid postincident investigations, assistance stations should be video recorded. The use of digital video systems should be considered by the designer. References include FEMA 426 (Table 1-22 and Section 12.2) and ISC (2004).
12	2	CCTV cameras with recording capability are placed at vehicle entrances and exits.	CCTV cameras with recording capability can be used to reduce both the real exposure and the perceived risk of drivers and passengers to criminal or terrorist activities such as personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants. CCTV cameras placed at vehicle entrances and exits to parking garages and lots should be used mainly to record security events for subsequent review, investigation, and prosecution. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. For deterrence and to aid postincident investigations, entrances and exits should be video recorded. The use of digital video systems should be considered by the designer. References include FEMA 426 (Table 1-22 and Section 12.2) and ISC (2004).
12	3	Site is capable of implementing temporary vehicle barrier systems during high threat periods or as required.	Threats to a facility can change due to several factors such as increased terrorist or criminal activity. Consideration should be given to the improvement of a defensive posture should threat levels increase. A number of temporary or semipermanent measures may be effective. Expedient methods include blocking access routes with heavy vehicles or temporarily blocking roads surrounding a building to create a form of controlled access area. If a secured area requires a limited exclusion area on a temporary or infrequent basis, it may not be possible to use physical structural barriers. Temporary barriers (including temporary fences, Jersey barriers, and vehicles) can be used. Also consider the use of removable bollards. References include ISC (2004).
12	4	Automated access control is implemented at all public/staff separation points.	High-risk offices that are not separated from public areas are at greater risk for attacks by criminals, terrorists, or militants because these elements can approach and enter with ease. Threats include assault, assault with a deadly weapon, assassination, kidnapping and hostage taking, robbery, and hand-delivered bombs. Automated access control is provided at high-use public/staff separation points for employees and can include electronic access control equipment using readers for • Magnetic coding, • Proximity/contact, • Resonant circuits, • Radio frequency, • Biometric technology, • Optical character, and • Smart card technology.

Discipline	Count	Countermeasure	Guidance
			The optimum value of these systems will be ensured only if all the following are observed: • The coding system is not easily decoded and duplicated. For example, on magnetic strip cards the magnetic coding is susceptible to transfer to another magnetic strip and later decoding or duplication. Low coercivity cards (the typical credit and debit cards) are particularly vulnerable. • The system can be modified from a remote location, quickly and at any time, even during heavy system use, to delete (or add) a user. • All the access level features are used. For systems that permit portal control by individual name, day of the week (or year), and clock hours (or shift), such features should be incorporated into the selection of the appropriate access level for each user. And these parameters should be updated immediately when that user's status changes. • Each protected portal in very secure applications requires not only that the correct card be used but that a remembered value (personal identification number, or PIN) be keyed in as well. Alternatively, biometric readers may be used. These require more elaborate readers at higher unit cost, but for truly secure applications, they will ensure that a lost or purloined card cannot be used before its loss has been discovered and reported. Automated control eliminates the need for guards at staff/public separation points. It provides electronic tracking of entrances and exits. References include FEMA 426 (Table 1-22 and Section 12.20).
12	5	Screening of mail (for weapons, explosives, and CBR material) is performed.	Screening deliveries from the U.S. mail and commercial package delivery services that enter the facility for weapons and explosives is important. This reduces the vulnerability to actions that accompany violent terrorist or criminal activity. Screening policies and procedures are used to • Identify the personnel who will perform the screening; • Train and periodically test the screening personnel; • Prescribe action to be taken upon discovery of weapons, explosives, and CBR agents, including notification of bomb and hazardous material incident responders; and • Determine the disposition of weapons, explosives, and CBR agents found. Equipment that can be used in the screening process include X-ray inspection machines, explosives detectors, and, if the level of threat warrants, radiation detectors and chemical/biological agent detectors. If the nature of the threat warrants it, canines can be brought in to assist the inspectors. Most metropolitan police departments have canine units that include explosives detection animals. BATF, the U.S. Customs Service, and various military departments of the federal government also have explosives detection dogs. Airport law enforcement agencies in major gateway cities also use them. It is advisable to identify which nearby local or federal agencies have such animals and whether, in an emergency, they would be available for use in the private sector. Written procedures should be available to mailroom screening personnel to explain the required actions in the event weapons, explosives, or CBR materials are discovered. References include FEMA 426 (Table 1-22 and Section 12.26), U.S. General Services Administration (2005), ISC (2004), Williams (2012), and DOC/CIAO (1998).

Discipline	Count	Countermeasure	Guidance
12	6	Staff (and their baggage) of facility are screened for weapons and explosives.	For high-risk facilities and heightened threat levels screening staff for weapons and explosives is important. This reduces the vulnerability to actions that accompanies violent terrorist activity, employee violence such as assault, assault with a deadly weapon, and hand-delivered bombs or WMDs. Screening policies and procedures, which have been reviewed and approved by legal counsel, are used to • Identify the personnel who will enforce the screening rules; • Train and periodically test the screening personnel; • Determine which situations will require participation of law enforcement personnel in the screening process; • Prescribe action to be taken when a visitor objects to screening • Prescribe action to be taken upon discovery of weapons or explosives, including notification of bomb and hazardous material incident responders; and • Determine the disposition of weapons and contraband found, including legal and illegal weapons. Equipment that can be used in the screening process, in addition to visual inspection and baggage search, include walk-through and handheld metal detectors, X-ray inspection machines, explosives detectors, and, if the level of threat warrants, radiation detectors and chemical/biological agent detectors. If the nature of the threat warrants it, canines can be brought in to assist the inspectors. Most metropolitan police departments have canine units that include explosives detection animals. BATFE, the U.S. Customs Service, and various military departments of the federal government also have explosives detection dogs. Airport law enforcement agencies in major gateway cities also use them. It is advisable to identify which nearby local or federal agencies have such animals and whether, in an emergency, they would be available for use in the private sector. References include FEMA 426 (Table 1-22 and Section 12.26) and Williams (2012).
12	7	Facility has a CCTV security system monitoring all entrances and exits.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs and WMDs. CCTV coverage of entrances and exits can assist the security force in identifying the situation and determining response requirements. The CCTV systems at entrances and exits should be used primarily for alarm assessment and access control automation purposes. The use of the CCTV system for general surveillance should be discouraged, with the occasional exception of automated video guard tours or monitoring certain areas such as a childcare center or childcare center play yard. For deterrence and to aid postincident investigations, activity at all entrances should be video recorded. The use of digital video systems should be considered by the designer. Operational capabilities, such as pan, tilt, and zoom, can be used to enhance the effectiveness of CCTV monitoring. References include ISC (2004).

Discipline	Count	Countermeasure	Guidance
12	8	Facility has an operation control center (OCC) with adequate environmental controls (e.g., A/C, lighting, heating, air circulation, backup power) for engineering/maintenance personnel.	The OCC is where operations personnel monitor operational information, signals, and alarms from the mechanical and electrical systems installed in the building. The OCC can be used for remote operation of the equipment in these systems. The OCC supervisor can dispatch operations personnel for maintenance and repair. It serves as a central location for decisions and actions that are required in emergency situations. For example, the HVAC system can be operated in various modes from the OCC to mitigate a terrorist CBR attack or hazardous material incident by removing smoke and airborne contaminants. The OCC should have redundant capability for voice and data transmission and mass communication. A backup power source should be provided. An area in the OCC should be designated where the following building documents will be readily available: • Emergency instructions, • OEP manuals, • Building plans, and • Maintenance and repair manuals and records. Colocation with the fire command center and security control center, if feasible, can enhance the ability to communicate in emergency situations. References include FEMA 426 (Table 1-22 and Section 10.16), ISC (2004), and Williams (2012).
12	9	The security force has access to a computerized guard tour system.	Patrolling the facility is a prime function of a guard force. A method is required to ensure that tours are performed properly. A computerized guard tour management system comprises software, handheld computers, and bar codes to monitor all tour and inspection activities. Preprogrammed bar codes that identify each item or site are placed on the equipment or location requiring inspection. Officers use portable data collection devices to scan the bar codes of all security checkpoints visited during their rounds. The device records each scan, providing proof that the item or location was inspected. To further ensure the site was visited, the handheld device documents the time, date, and location of the inspection. The system's tracking capabilities provide a method for monitoring productivity and analyzing trends. Prior to beginning a tour, a route is downloaded from a desktop computer to the handheld computer. The application then directs officers to the checkpoints in a set order, ensuring that no area is missed. Additionally, the program provides a feature that enables officers to complete the inspections in any order they wish while in the roam mode. Within minutes after completing their rounds, the officers download data stored on the device to a desktop computer. The computer database is then updated, allowing officers to print out accurate, tamper-proof reports that outline daily security operations. Officers also have the ability to document incidents in the field, such as vandalism, a broken window, or an exit light that is out. References include FEMA 426 (Table 1-22 and Section 12.37).
12	10	Duress button at control center(s) is connected to police or backup monitoring location.	Terrorists or militants wanting to gain control over a facility to inflict the maximum damage might attempt forced entry into one or more of the control centers. This would place life safety (fire alarm and suppression, HVAC, communications) and security systems (access control, intrusion detection) in jeopardy. Therefore, it is expedient to have a means of notifying the police or a backup monitoring location (e.g., commercial central station) when such a situation occurs. This can be accomplished by the use of a duress alarm system (also known as a panic alarm or hold-up alarm). Duress alarms should be located in the OCC, FCC, and SCC. Duress alarm systems may be either hardwired or portable, using a radio frequency or microwave transmission. It is useful, when possible, to have CCTV coverage of the command centers so that law enforcement, security, and building management personnel can appraise the situation that necessitated the alarm and direct security or law enforcement responders. Some CCTV systems now can be monitored by off-site security personnel via the Internet. References include FEMA 426 (Table 1-22 and Section 12.4), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
12	11	CCTV system is used primarily for alarm assessment and access control automation purposes rather than for general surveillance.	CCTV can be a valuable tool for deterring terrorists, criminals, and militants from attacking a facility or identifying an intrusion or potential attack (i.e., alarm assessment). CCTV systems are also useful for automating access control and monitoring egress through emergency exits. The CCTV systems should be primarily for alarm assessment and access control automation purposes. The use of the CCTV system for general surveillance should be discouraged, with the occasional exception of automated video guard tours or monitoring certain areas of the childcare center or childcare center play yard. One reason is that the efficiency of monitoring multiple screens decreases as the number of screens increases. Also, fatigue becomes a factor when monitoring personnel must maintain general surveillance. They become more likely to miss an incident or event. References include ISC (2004).
12	12	CCTV cameras are monitored and/or recorded 24 hours/7 days a week by security personnel.	CCTV can be a valuable tool for deterring terrorists, criminals, and militants from attacking a facility or identifying an intrusion or potential attack (i.e., alarm assessment). CCTV systems are also useful for automating access control and monitoring egress through emergency exits. The CCTV systems should be primarily for alarm assessment and access control automation purposes. The use of the CCTV system for general surveillance should be discouraged, with the occasional exception of automated video guard tours or monitoring certain areas of the childcare center or childcare center play yard. One reason is that the efficiency of monitoring multiple screens decreases as the number of screens increases. Also, fatigue becomes a factor when monitoring personnel must maintain general surveillance. They become more likely to miss an incident or event.
12	13	Duress buttons are located at all guard posts.	A potential for violence exists anywhere there is contact between the security force and the public. Therefore, it is expedient to have a means of notifying the security control center when a situation appears to get out of control and requires backup forces. This can be accomplished by the use of a duress alarm system (also known as a panic alarm or hold-up alarm). Duress alarms should be located at all guard posts. Duress alarm systems may be either hardwired or portable, using a radio frequency or microwave transmission to alert the security control center or local law enforcement. The first level of monitoring for guard post duress alarms can be provided at an on-site, proprietary security control center. To mitigate staffing requirements and annual operating costs, commercial central stations are sometimes used for after-hours monitoring or to supplement on-site monitoring. They should notify the police and appropriate off-site security supervisors or managers. This situation might be appropriate for facilities with no public contact after normal business hours. For facilities that might have public contact at all hours, the alarms can be monitored by an on-site, 24-hour proprietary security control center, which could call in law enforcement backup. It is useful, when possible, to have CCTV coverage of the guard posts where duress buttons are located so that security control room personnel can appraise the situation that necessitated the alarm and direct security or law enforcement responders. Some CCTV systems now can be monitored by on-site and off-site security personnel via the Internet. References include FEMA 426 (Table 1-22 and Section 12.4), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
12	14	Accessible windows (below 18 ft (5.5 m) or adjacent to climbing assistance) have glass break sensors.	Windows at scalable heights or that are adjacent to climbing assistance, can be used by an intruder to gain entry. Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs. Windows below the second story of a building (18 ft (5.5 m) or lower) are considered to be accessible to a potential intruder. Windows higher on the building that are close to climbing aids (e.g., ladder to the roof, fire escape, or vegetation) are also considered accessible. Security alarms can be used to counter these threats by deterring a potential adversary or detecting an entry attempt through the building envelope. As opposed to indoor motion detectors, glass break sensors offer the advantage of sounding an alarm while an intruder is still outside. Breaking glass produces unique sound wave frequencies (3-5 kilohertz, or kHz) that glass break sensors “hear,” and seismic shock frequencies (200 hertz, or Hz) that they “feel.” Built-in microprocessors enable the devices to react to these sounds and ignore others that cause false alarms. References include FEMA 426 (Table 1-22 and Section 12.10), U.S. General Services Administration (2005), ISC (2004), and Williams (2012).
12	15	Redundant security system communication routes or paths are employed.	In the event of an attack or other emergency, adequate communication systems are vital to the response by staff and off-site responders. A single point failure should not be allowed to disrupt security communications. Multiple distribution runs, separated as much as possible and not located near high-risk areas, should be used for hardwired communications such as telephones and public address systems. The wiring and conduits should be controlled preferably by routing them through separate and secure closets. The communication systems should be connected to an emergency power source. Wireless data transmission minimizes the risk of communications breakdowns due to wiring damage. Radio telemetry can be used for nonsecure data that support the life safety system and other critical operations. For the greatest protection, distributed antennas could be located throughout the facility if required for emergency communication through wireless transmission of data. Other communications systems such as a second telephone system, intercom, portable radio, pager, cell phone, walkie-talkie, and personal data assistants (PDAs) should be considered. Messengers can be used as a last resort. References include FEMA 426 (Table 1-22 and Section 12.35) and ISC (2004).
12	16	Security equipment selection criteria are defined.	Security equipment plays a vital role in the modern security program. Barriers and other traffic control devices, access control, intrusion detection, duress alarms, and communication and CCTV systems provide warning and defense against terrorists, militants, and criminals intent on causing harm to the facility and its occupants. The risk assessment will determine the threats to a facility and countermeasures to address the threats and lower risk. Security hardware and software help to implement these countermeasures. Because of the rapid development of new security technology, a security consultant should be used to define selection criteria for new and replacement security equipment, which should be a part of the security planning process. References include FEMA 426 (Table 1-22 and Section 12.41).

Discipline	Count	Countermeasure	Guidance
12	17	Security plan includes security system design and drawing standards for future system implementation.	Security equipment plays a vital role in the modern security program. Barriers and other traffic control devices, access control, intrusion detection, duress alarms, and communication and CCTV systems provide warning and defense against terrorists, militants, and criminals intent on causing harm to the facility and its occupants. The risk assessment will determine the threats to a facility and countermeasures to address the threats and reduce risk. Security hardware and software help to implement these countermeasures. Because of the rapid development of new security technology, a security consultant should be used to define selection criteria for new and replacement security equipment, which should be a part of the security planning process. In light of this technological development, the security plan should provide security system design and drawing standards for use in implementing future security system changes. References include FEMA 426 (Table 1-22 and Section 12.41) and Williams (2012).
12	18	Guard force is employed at the facility.	A security force can work directly for the enterprise (in house or proprietary) or for an independent contractor. It is generally accepted that to staff a guard post with a single guard 24 hours a day, 7 days a week, requires 4 to 5 full-time employees. The basic functions of a security force are usually • Control of entrances and movement of pedestrian and vehicle traffic, • Patrol of buildings and perimeters, • Escort of material and personnel, • Inspection of security and fire exposures, and • Special assignments. In 2012, the Private Sector Liaison Committee (PSLC) of the International Association of Chiefs of Police (IACP) published guidelines for the selection, training, and licensing of private security guards (officers). While not specified in IACP/PSLC (2012), the essential personal attributes for an officer are considered to be • Good character, • Proper attitude and ability to handle people, • Neat appearance, • Circumspect deportment, • Knowledge of the job, and • Adequate training and ongoing education. IACP/PLSC (2012) also includes minimum criteria for private security officer training. Many states have adopted legislation requiring that armed officers be licensed by the state and mandate minimum qualifying standards for the issue of licenses or permits to carry firearms. Officers must be thoroughly proficient in the use of arms before they are allowed to carry them. Training includes proper handling of firearms and live range firing for qualification. The efficiency of the security force depends on the adequacy and skill of its supervisors. Unless officers are properly trained and closely supervised, they may not provide the protection required. Officers are frequently dispersed over a large area, which requires a supervisory style that is different from that used with clustered workers. Security officer supervisory personnel should be selected on the basis of their knowledge of the job plus demonstrated administrative and leadership abilities. They should be given special training so that they can keep current with new developments and methods. Some organizations prefer to rotate the assignments of supervisors to prevent the development of cliques and to ensure familiarity with all phases of security officer duties. In some instances, deputation as a peace officer may be necessary to the performance of the job—such as in the handling of traffic on adjacent streets. When officers are deputized, limiting the scope of their authority to the actual security officer duties is customary and prudent. Because officers may at any time be required to detain someone, it is essential that they be thoroughly familiar with the law regarding arrest, search, and seizure.

Discipline	Count	Countermeasure	Guidance
			The facility OEP manual that covers all locations in the facility should be used by security guards and employees. Guards and employees should receive emergency training in the proper reporting and response to fires and other emergencies and in the use of portable and built-in protection systems, including training in system maintenance. References include FEMA 426 (Table 1-22 and Section 2.7), ISC (2004), and Williams (2012).
			13—Security master plan
13	1	Facility has an occupant emergency plan (OEP) manual establishing emergency plans, policies, and procedures that cover all locations in the facility. The OEP should include plans for evacuation and sheltering in place.	Criminal, terrorist, or militant attacks such as bombing, arson, and CBR agent release can cause confusion, panic, injury, and death. This is also true for accidental emergencies such as fire, gas leaks, and natural disasters. At a minimum, an occupant emergency plan (OEP) can support evacuations and shelter-in-place and building system control. An OEP generally covers response actions for specific events. These events usually include fire, bomb threat, suspicious package, and weather-related emergencies typical for the geographical region (i.e., tornadoes, hurricanes, winter weather, etc.). In certain seismic zones, the OEP may include response procedures for earthquakes. OEPs provide a detailed procedure for safeguarding building occupants during an emergency. OEPs include evacuation plans and routes, exterior assembly areas, shelter-in-place locations, and detailed lists of responsibilities for staff members who perform important functions during an emergency. Regardless of a facility's size or mission, some level of planning is necessary. Reasons for planning include • Mitigating the impact of the event; • Preparing staff, visitors, and assets; • Accelerating recovery of facilities and finance and administrative operations; • Allowing an agency or institution to continue its mission, business, or operation; • Enhancing image with staff, customers, and community; and • Fulfilling moral responsibility. Organizations must consider a more comprehensive and holistic approach to disaster management planning (DMP) beyond OEPs that support their facility's preparedness, response, and recovery from a major emergency or disaster. All employees and some visitors require some form of training. This includes periodic employee discussion sessions to review policies, technical training in equipment use for professional emergency response crews, evacuation drills, and full-scale exercises. Consider the training and information needs of persons regularly on the premises, including employees, contractors, visitors, managers, and emergency response crews. Training can include • Orientation and education sessions, including regularly scheduled discussions to provide information, answer questions, and identify needs and concerns; • Tabletop exercises, in which members of the emergency management group meet in a conference room setting to discuss their responsibilities and how they would react to an emergency scenario; • Walk-through drills, in which the emergency management group and response teams perform their emergency response functions; • Functional drills, such as tests of specific functions including warning and communication procedures and equipment, medical response, or emergency notifications; • Evacuation drills, in which personnel walk the evacuation route to designated areas where procedures to account for all personnel are tested and participants note potential hazards such as stairwell congestion; • Full-scale exercises, in which an emergency situation is simulated as closely as possible, include company personnel and community response organizations. References include FEMA 426 (Table 1-22 and Section 2.22), ISC (2004), and U.S. General Services Administration (2005).

Discipline	Count	Countermeasure	Guidance
13	2	The security plan has been benchmarked or compared against related organizations and operational entities.	Physical security is a system of tangible countermeasures, designed to protect the organization's physical and operational assets from identified threats. A plan for the physical security component of a comprehensive security program usually comprises • Policies and procedures: statements of security goals and the required means of achieving them; • Personnel: people to monitor, administer, and implement the system; • Barriers: access control devices or structures; • Equipment: detection, alarm, and communication and control systems (includes both hardware and software); and • Records: past and incident reports, access records, and transaction logs. Each of these areas should be compared against the security plans of organizations and operational entities (e.g., office buildings, hotels, and medical facilities) similar to those of the facility. This can be facilitated by a rapport developed from close contact between security professionals. Security industry organizations such as ASIS International can promote this contact. References include FEMA 426 (Table 1-22 and Section 13.3) and Williams (2012).
13	3	The security plan has been tested and evaluated from a cost-benefit and operational efficiency and effectiveness perspective.	Physical security is a system of tangible countermeasures designed to protect the organization's physical and operational assets from identified threats. A plan for the physical security component of a comprehensive security program usually comprises • Policies and procedures: statements of security goals and the required means of achieving them; • Personnel: people to monitor, administer, and implement the system • Barriers: access control devices or structures; • Equipment: detection, alarm, and communication and control systems (includes both hardware and software); and • Records: past and incident reports, access records, and transaction logs. The security professional must insist on being part of the facility planning and design process and, if necessary, should hire staff or consultants who speak the language of architecture and construction to ensure that effective security is incorporated into the architect's vision and layout. In addition, the cost-effective implementation of security technology requires early coordination with the facility design team. For example, coordination is required with the architect to allocate sufficient space for monitoring stations and equipment closets (and uniformed security staff locker room facilities) and with the electrical engineer for power and conduit requirements. The security plan should be evaluated and tested to determine if it provides an acceptable cost-benefit ratio. For example, the cost of countermeasures should relate to the level of risk. The plan should be evaluated to determine if a satisfactory level of operational efficiency and security efficiency is provided in accomplishing the goals of the plan. Tests of the operating program are also essential in the implementation of the security system. Tests should result in the following: • Risks or hazards still existing are identified and system deficiencies are revealed. • System changes required to accommodate facility or organization revisions become apparent. References include FEMA 426 (Table 1-22 and Section 13.4) and Williams (2012).
13	4	The security plan defines mission, vision, and short- and long-term security program goals and objectives.	The security plan must define the mission of the security program, which is generally the protection of assets (i.e., people, facilities, equipment, product, and accounts receivable). A vision should be defined to provide both security and nonsecurity personnel with an idea of what the security program hopes to achieve. Short- and long-term security goals should be defined so that the security organization can see in what direction it is heading. For example, the security department might want to obtain the latest and future technology for surveillance, access control, etc. References include FEMA 426 (Table 1-22 and Section 13.5).

Discipline	Count	Countermeasure	Guidance
13	5	Designated chain of command is specified for decision making during emergencies.	Emergency situations can cause uncertainty and confusion. Planning for specific courses of action, such as with an OEP or disaster management plan, can help to structure the response to the emergency. A building may have the following control centers: • Operation control center (OCC), • Fire command center (FCC), • Security control center (SCC), and • Backup control center (BCC). Centralizing control center information can improve the reliability and effectiveness of life safety systems, security systems, and building functions. It may be advisable to colocate the OCC, FCC, and SCC. (This does not require the addition of an OCC, FCC, or SCC if one does not exist.) If the control centers are colocated, operational requirements must be specified, especially a predetermined chain of command to ensure that the most qualified leadership is in control for specific types of events. References include ISC (2004).

APPENDIX G

Countermeasure Commentary for Level 4, Gold

Discipline	Count	Countermeasure	Guidance
1—Site			
1	1	Design, site layout, or speed control measures prohibit a vehicle from approaching at significant speed.	Blast loads decrease rapidly with distance from the explosion. Therefore, setback is one of the first considerations when designing for blast loads. The setback distance is the range between the explosive threat location and the nearest structural element requiring protection. The term standoff is synonymous with setback, and the two terms may be used interchangeably. The term standoff is often used when discussing the distance between a facility and the threat location. Each foot of setback can be of critical importance in reducing or limiting damage, injury, and death. If a vehicle can be driven through the facility's perimeter or into the building, this will nullify the setback. Vehicle bombs are especially dangerous because of the size of the explosive load that can be carried. The energy of a moving vehicle increases with the square of its velocity; therefore, minimizing a vehicle's speed allows vehicle barriers to be lighter and less expensive. To facilitate reductions in vehicle speeds, ensure there are no unobstructed vehicle approaches perpendicular to inhabited buildings at the required parking and roadway standoff distances. If such approaches already exist, using obstacles and barriers can create a serpentine (curving) approach route to slow approaching vehicles. Speed bumps can also reduce a vehicle's speed. References include FEMA 426 (Table 1-22 and Section 1.13) (2003a), U.S. General Services Administration (2005), and ISC (2004).
1	2	Closed-circuit television (CCTV) surveillance system with recording capability is used to view activity within 50 ft (15.2 m) of the perimeter of the building.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs. A distance of 50 ft (15.2 m) is recommended to limit opportunities for concealment, detect the approach of unauthorized personnel, and provide sufficient standoff for a self-carried explosive device. In urban situations, it may only be possible to view activity much closer to the building. Still, the presence of CCTV will act as a deterrent to potential intruders. The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. Alarm-activated CCTV coverage of the area surrounding the facility can assist the security force in identifying the situation and determining response requirements.

Discipline	Count	Countermeasure	Guidance
			Cameras should be on real-time and time-lapsed video recorders. For deterrence and to aid postincident investigations, assistance stations should be video recorded. The use of digital video systems should be considered by the designer. A distance of 50 ft (15.2 m) is recommended to limit opportunities for concealment, detect the approach of unauthorized personnel, and provide sufficient standoff for a self-carried explosive device. However, 50 ft (15.2 m) may not be available or required for all facilities. The reviewer must determine that an adequate clear zone exists for proper surveillance and to limit places of concealment. References include FEMA 426 (Table 1-22 and Section 12.2).
1	3	System of fencing, grilles, doors, etc., to completely close down access to the entire site in unattended hours, or in some cases, all hours exists.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs and weapons of mass destruction (WMDs). A perimeter barrier system, either at some distance from the building (e.g., a fence) or, in some cases, the building envelope itself (e.g., grilles, doors), should deter or delay attackers from gaining access to the facility. The perimeter barrier should be designed to completely close down access to the entire facility in unattended hours, or in some cases, all hours. Ground-level pedestrian exits that open into nonsecure areas should be emergency exits only and fitted with panic bar hardware for exiting movement only. References include FEMA 426 (Table 1-22 and Section 1.4), U.S. General Services Administration (2005), and ISC (2004).
1	4	Vehicles are inspected at perimeter.	As discussed in Gold Countermeasure Discipline 1 Countermeasure 1, a vehicle bomb can be a major terrorist or criminal threat to a facility. This applies to stationary and moving vehicles containing explosives. If a perimeter barrier is employed, providing points of access through the perimeter for building users (i.e., employees, visitors, and service providers) is necessary. An entry control point or guard building serves well as the designated point of entry for site access. It provides a point for implementation of desired or required levels of screening and access control. The objective of the entry control point is to prevent unauthorized access while maximizing the rate of authorized access by foot or vehicle. Vehicle access control and inspection should occur as far from facilities as possible (preferably at the site perimeter) with the ability to regulate the flow vehicles one at a time. Space should be provided for inspection at the curb line or outside the protected perimeter for gross amounts of explosives. The location should be separated from the building as much as practical. If screening space cannot be provided, other features such as hardening, or other operational procedures such as finding alternative space for inspection, may be required. The vehicle checkpoint is a location where the identity and contents of inbound and outbound vehicles can be determined before they are permitted to proceed. An effective checkpoint presumes a means to prevent the vehicle from further movement until released. In highly sensitive facilities or in those exposed to credible threats of attempted barrier breach, the barrier must be substantial. A fully hardened checkpoint includes the ability to perform a complete inspection of the vehicle, including a view of the undercarriage with inspection mirrors. Explosives detectors, based upon vapor trace analysis, can also be utilized at the checkpoint. An adequate checkpoint design will permit future options, such as simple vehicle and driver identification checks, to a comprehensive inspection. Active barriers for entrance checkpoints include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. The barrier system should impede both inbound and outbound traffic. The system should include traffic control features to deter inbound vehicles from using outbound lanes for unauthorized access. Barrier devices that traverse both roadways should be used. References include FEMA 426 (Table 1-22 and Section 1.7), FEMA 386-7 (2002), ISC (2004), and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
1	5	Pull-over lanes are available at checkpoints to inspect vehicles.	As discussed in Gold Countermeasure Discipline 1 Countermeasure 1, a vehicle bomb can be a major terrorist or criminal threat to a facility. This applies to stationary and moving vehicles containing explosives. If a perimeter barrier is employed, providing points of access through the perimeter for building users (i.e., employees, visitors, and service providers) is necessary. An entry control point or guard building serves well as the designated point of entry for site access. It provides a point for implementation of desired or required levels of screening and access control. The objective of the entry control point is to prevent unauthorized access while maximizing the rate of authorized access by foot or vehicle. Pull-over lanes facilitate vehicle inspection when required while allowing authorized vehicles to proceed. Authorized vehicles can be identified by using bumper or window stickers, placards, hanging tags, or electronic means such as radio frequency readers or video-based recognition systems. References include FEMA 426 (Table 1-22 and Section 1.8), U.S. General Services Administration (2005), and ISC (2004).
1	6	Vehicle control measures (sally port, etc.) are available to prevent tailgating.	As discussed in Gold Countermeasure Discipline 1 Countermeasure 1, a vehicle bomb can be a major terrorist or criminal threat to a facility. This applies to stationary and moving vehicles containing explosives. As discussed in Gold Countermeasure Discipline 1 Countermeasure 4, vehicle inspection points can be used to screen vehicles for gross amounts of explosives before they are allowed through a protected perimeter onto the facility's property. To prevent an unauthorized vehicle from following an authorized vehicle through an entry point, a sally port is often used. This system requires two operable vehicle barriers. A vehicle approaches a first barrier, enters, stops in front of the second barrier and the first barrier closes behind the vehicle. Once the vehicle is authorized to enter the site, the second barrier in front of the vehicle opens while the closed first barrier behind the vehicle prevents unauthorized vehicles from following. References include FEMA 426 (Table 1-22 and Section 1.8), U.S. General Services Administration (2005), and ISC (2004).
1	7	Garage or service entrances that are not otherwise protected by site perimeter (crash) barriers are provided vehicle-arresting devices.	As discussed in Gold Countermeasure Discipline 1 Countermeasure 1, a vehicle bomb can be a major terrorist or criminal threat to a facility. If the perimeter inspection described in Gold Countermeasure Discipline 1 Countermeasure 4 is not performed, barriers should be provided at parking garage and service entrances. The antiram device must be capable of arresting a vehicle of the designated threat size at the speed attainable at the location. Active antiram barriers (arresting devices) include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. Control internal building parking, underground parking garages, and access to service areas and loading docks in this manner with proper access control, or eliminate parking altogether. To meet impact requirements, any barrier system proposed must be tested or otherwise certified by an independent testing lab or firm to meet or exceed the required vehicle size and impact velocity. Without proper site-specific design, there is no assurance that such barriers will perform as required. References include FEMA 426 (Table 1-22 and Section 1.18), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
1	8	Emergency vehicle routes have vehicle barriers capable of allowing passage of large fire apparatus.	A terrorist bomb attack in which an explosive-laden vehicle is driven through a perimeter or into a building could result in catastrophic structural damage, injury, and death. Vehicle barriers of various types are designed to stop a vehicle before it can penetrate the defended setback. The stopping power or rating is based on the weight of the vehicle and the maximum speed it can attain prior to striking the barrier. The desired barrier rating for a particular facility is based on the required level of protection identified in the risk assessment. Active barriers for entrances include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. The active barrier at entrances for emergency vehicles, including large fire apparatus, should be wide enough to allow passage of the vehicle in either direction. Fire departments and other emergency responders can provide information about the width of their vehicles. Barriers should also operate quickly in case an unexpected emergency vehicle appears. References include FEMA 426 (Table 1-22 and Section 1.2), U.S. Army (1987), and U.S. General Services Administration (2005).
1	9	The uninterruptable power supply (UPS) is located in a secure area.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. For example, electric power systems can suffer significant damage when subjected to the shock of an explosion. Electrical power may be critical for safely evacuating people from the building. Destruction of critical electrical components could cause damage that is disproportionate to other building damage resulting from an explosion. Uninterruptible power systems can provide a source of electrical power in the event that normal supply is lost. They can also provide power to cover the lag time before a backup generator comes on line. In small buildings, a UPS may be the only source of emergency power. Therefore, protecting this alternate source of power is necessary for emergency situations. Do not locate a UPS near high-risk areas such as building entrances, lobbies, loading docks, mailrooms, and hazardous materials storage rooms. Rooms or areas containing a UPS should have access control and intrusion-detection sensors. References include ISC (2004).
2—Architectural			
2	1	Vehicle standoff (based on blast assessment) is available for unscreened vehicles, defended by rated crash barrier systems.	A vehicle bomb can be a major terrorist or criminal threat to a facility. This applies to stationary and moving vehicles containing explosives. A vehicle bomb can be more devastating to a facility because of the much larger weight of explosive material that can be carried. This is especially true for van and truck bombs. These vehicles do not have to be as close to the building as a hand-carried bomb. Blast loads decrease rapidly with distance from the explosion. Therefore, setback is one of the first considerations when designing for blast loads. The setback distance is the range between the explosive threat location and the nearest structural element requiring protection. The term standoff is synonymous with setback, and the two terms may be used interchangeably. The term standoff is often used when discussing the distance between a facility and the threat location. Each foot of setback can be of critical importance in reducing or limiting damage, injury, and death. The facility blast analysis (see Silver Countermeasure Discipline 3 Countermeasure 4) will determine the required setback distance to protect against the threats identified in the risk assessment (see Silver Countermeasure Discipline 4 Countermeasure 4).

Discipline	Count	Countermeasure	Guidance
			Where those distances are not available, analysis of the structure by an engineer experienced in blast-resistant design is required. In addition, hardening will be applied as necessary (in those cases that permit structure hardening) to mitigate the effects of the explosives indicated in the facility risk assessment at the achievable standoff distance for the required level of protection. Vehicle barriers of various types are designed to stop a vehicle before it can penetrate the defended setback. The stopping power or rating is based on the weight of the vehicle and the maximum speed it can attain prior to striking the barrier. The desired barrier rating for a particular facility is based on the required level of protection identified in the risk assessment. Active barriers for entrance checkpoints include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. Passive barriers include fixed bollards, concrete planters, freestanding walls, and terrace walls. To meet impact requirements, any barrier system proposed must be tested or otherwise certified by an independent testing lab or firm to meet or exceed the required vehicle size and impact velocity. Without proper site-specific design, there is no assurance that such barriers will perform as required. References include FEMA 426 (Table 1-22 and Section 1.10), U.S. General Services Administration (2005), and ISC (2004).
2	2	Trash receptacles are placed at the perimeter of the facility, or they are hardened or removed from around the facility.	Hand-carried explosives placed near buildings can cause significant localized damage, potentially resulting in injuries or fatalities. It is assumed that aggressors will not attempt to place explosive devices in areas near buildings where those devices could be visually detected by building occupants casually observing the area. It is also assumed that sufficient controls will preclude bombs being brought into buildings. An explosive device equivalent to that indicated by the risk assessment and blast analysis is assumed to be placed by hand either in trash containers or in the immediate vicinity of buildings. That quantity of explosives is further assumed to be built into a bomb 150 mm (6 in.) or greater in height. Measure the standoff distance from the nearest point of the trash container or trash container enclosure to the closest point on the building exterior or inhabited portion of the building. Where the standoff distance is not available, harden trash enclosures to mitigate the direct blast effects and secondary fragment effects of the explosive on the building if the applicable level of protection can be proven by analysis. If trash enclosures are secured to preclude introduction of objects into the enclosures by unauthorized personnel, they may be located closer to the building as long as they do not violate unobstructed space provisions. Openings in screening materials and gaps between the ground and screens or walls making up an enclosure must not be greater than 150 mm (6 in.). DoD (2002) considers 33 ft (10 m) to be a sufficient standoff distance for trash receptacles, while USAF (1997) considers 30 ft (9.1 m) as the minimum acceptable standoff. Fifty ft (15.2 m) is a more conservative standoff between a hand-placed bomb concealed in or behind an obstruction and the building perimeter. However, 50 ft (15.2 m) may not be available or required for all facilities. The reviewer must determine that an adequate clear zone exists for proper surveillance and to limit places of concealment. References include FEMA 426 (Table 1-22 and Section 2.4).

Discipline	Count	Countermeasure	Guidance
2	3	Potential hiding places are avoided or closed off.	Landscape and structural features can provide concealment for covert activity by a terrorist, criminal, or militant intent on causing harm. Hiding places also can be used to conceal hand-carried bombs and WMDs. Vegetation such as ground cover and shrubs should not be placed close to buildings or else should be cut or trimmed to remove places of concealment. Shrubs should be cut to within 2 ft (0.6 m) of the ground. The lower branches of existing trees should be no lower than 10 ft (3 m) from the ground. Nooks and crannies in the building's structure and areas beneath outdoor stairwells should be eliminated or closed off. References include FEMA 426 (Table 1-22 and Section 2.1), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004).
2	4	Foyers have reinforced concrete walls, and interior and exterior doors are offset from each other.	A vehicle or hand-carried bomb detonated at the building entrance could result in injury and damage in controlled areas behind the entrance. In buildings where a foyer separates the entrance or screening area from the controlled area, reinforced concrete walls should separate the foyer from the controlled area to protect against blast. Reinforced concrete walls offer considerable protection against the effects of blast. Exterior and interior doors of the foyer should be offset from each other so when an exterior door fails due to a blast, the door and any fragmentation associated with it will be caught by the interior foyer wall. This may limit injury and damage to the building occupants or assets. The interior foyer door should be equivalent in construction to the exterior door. This protective measure can also be used at other points of staff/public contact. References include FEMA 426 (Table 1-22 and Section 2.1) and U.S. Army (1994).
2	5	Exterior hallways are not present in inhabited portions of the building to protect personnel from open exposure to large amounts of flying glass and debris.	A terrorist vehicle bomb driven near or into the building or a hand-carried bomb placed close to the building creates secondary debris when detonated. In past explosive events where there was no building collapse, a large number of injuries resulted from flying glass fragments and debris from walls, ceilings, and fixtures (nonstructural features). The glass used in most windows breaks at very low blast pressures, resulting in hazardous, daggerlike shards. Minimizing those hazards through reduction in window numbers and sizes and through enhanced window construction has a major effect on limiting mass casualties. Hazardous fragments may also include secondary debris such as those from barriers and site furnishings. Exterior hallways with windows in the outer wall of the building should not be used in inhabited areas where personnel in the hallway would be exposed to secondary debris from a blast. Likewise, personnel in offices adjacent to the hallway could be affected because external hallways have large numbers of doors that can become hazardous debris during explosive blast events and lead into inhabited areas. If exterior hallways must be used, measures should be taken to reduce secondary debris from a blast, including • Using laminated glazing; • Providing protection with an antishatter (fragment retention) film a minimum of 7-mil (0.18 mm) thick, or specially manufactured 4-mil (0.10 mm) thick film; • Applying structural silicone to glazing systems with a 1/2-in. (12.7-mm) (3/4 in. (19.0 mm) is better) bite; • Ensuring the window system design on the exterior façade is balanced (i.e., glazing, frames, and anchorage to supporting walls) to mitigate the hazardous effects of flying glass following an explosive event; • Using window treatments such as a blast curtain or shield; and • Using doors designed to resist blast effects. References include ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	6	Stairwells required for emergency egress are located away from areas where blast events might occur, such as lobbies, mailrooms, parking, and loading docks.	Stairwells required for emergency egress must be designed to meet applicable codes and must serve as an integral part of the Occupant Emergency Plan (OEP). As such, stairwells should be located as remotely as possible from areas where blast events might occur (e.g., lobbies, mailroom, loading dock, and parking areas). Wherever possible, do not have stairs discharge into lobbies, parking, or loading areas. Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc., out of the stairway. Pressurize exit stairways in accordance with ICC (2012). References include FEMA 426 (Table 1-22 and Section 2.23), U.S. General Services Administration (2005), ISC (2004), and CDC/NIOSH (2002).
2	7	Stairwells required for emergency egress are designed to support the OEP.	Stairwells required for emergency egress must be designed to meet applicable codes and must serve as an integral part of the OEP. As such, stairwells should be located as remotely as possible from areas where blast events might occur (e.g., lobbies, mailroom, loading dock, and parking areas). Wherever possible, do not have stairs discharge into lobbies, parking, or loading areas. For example, if an OEP calls for evacuation down a stairwell, the plan for the building must consider where the stairs will discharge and the need for a source of electrical power that will function in that area if a design-basis event occurs. References include ISC (2004).
2	8	Parking is prohibited underneath or within facility.	A terrorist vehicle bomb attack where the vehicle is driven to a parking area within or under the building could result in catastrophic structural damage, injury, and death. Vehicle barriers of various types are designed to stop a vehicle before it can penetrate the defended setback. The stopping power or rating is based on the weight of the vehicle and the maximum speed it can attain prior to striking the barrier. The desired barrier rating for a particular facility is based on the required level of protection identified in the risk assessment. Active barriers for entrances include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. Passive barriers include fixed bollards, concrete planters, freestanding walls, and terrace walls. To meet impact requirements, any barrier system proposed must be tested or otherwise certified by an independent testing lab or firm to meet or exceed the required vehicle size and impact velocity. Without proper site-specific design, there is no assurance that such barriers will perform as required. References include DoD (2002).
2	9	Public toilets, service spaces, and vertical circulation systems are located in secure areas behind security screening points.	Public restrooms that are located on the public side of screening stations could be used by an attacker to conceal bombs or WMDs. The public should not be allowed access to service spaces such as electrical and mechanical rooms for heating, ventilating, and air conditioning (HVAC). Locating elevators and stairwells on the public side gives aggressors access to multiple floors. Access to HVAC equipment and ductwork provides an opportunity for dispersing chemical, biological, and radiological (CBR) agents. If any of these items is already in place, some form of access control should be in place for stairwell doors, elevator controls, service rooms, and public toilets. This could include key locks, push-button locks, and elevator card readers. References include FEMA 426 (Table 1-22 and Section 6.12), U.S. General Services Administration (2005), ISC (2004), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
2	10	Distance of at least 50 ft (15.2 m) separates main entrance, loading docks, shipping/receiving areas, vehicle circulation, and parking from utility mains, utility rooms, and other critical components and important assets.	Utility systems and other critical assets can suffer significant damage when subjected to the shock of an explosion. Some of these utilities and critical components may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Distribution systems; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms and equipment. Loading docks, shipping/receiving areas, vehicle circulation, and parking areas are among the most susceptible to the delivery of explosive materials. Maintaining a distance of at least 50 ft (15.2 m) between these areas and utilities, critical components, and important assets will reduce their vulnerability to bomb attack. A distance of 50 ft (15.2 m) is the generally accepted margin for a high level of protection found in the source criteria and guidance documents. However, 50 ft may not be available or required for all facilities. The reviewer must determine that a separation exists between utilities, critical components, and important assets and loading docks, shipping/receiving areas, etc. References include FEMA 426 (Table 1-22 and Sections 2.15, 8.3), DoD (2002), ISC (2004).

Discipline	Count	Countermeasure	Guidance
2	11	Distance of at least 50ft (15.2m) separates mailrooms from utility mains, utility rooms, and other critical components and important assets.	Utility systems and other critical assets can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Distribution systems; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms and equipment. Mailrooms and mail-handling areas are among the most susceptible to the delivery of explosive materials. Maintaining a distance of at least 50ft (15.2m) between these areas and utilities, critical components, and important assets will reduce their vulnerability to bomb attack. A distance of 50ft (15.2m) is the generally accepted margin for the highest level of protection found in the source criteria and guidance documents. However, 50ft may not be available or required for all facilities. The reviewer must determine that a separation exists between mailrooms and utility mains, utility rooms, and other critical or important assets. References include FEMA 426 (Table 1-22 and Sections 2.15, 8.3), DoD (2002), and ISC (2004).
2	12	Interior doors to high-risk offices are protected by door contacts.	Staff offices that are not separated from public areas are at greater risk for attacks by criminals, terrorists, or militants because these elements can approach and enter with ease. Threats include assault, assault with a deadly weapon, assassination, kidnapping and hostage taking, robbery, and hand-delivered bombs. Where separation includes doors between staff areas and public areas, the doors should be provided with an intrusion-detection device, usually an electromechanical intrusion sensor, commonly known as a door contact. The sensor can be either a mechanical or magnetic switch. This type of sensor is composed of a two-part electrical contact. One is installed on the opening surface, the other installed on the fixed surface. When the opening surface, typically a door, is in a closed position, the two contacts provide a closed circuit and a continuity of electrical current. When the opening surface is moved, separating the contacts, the circuit is broken and the interruption in current activates an alarm. The switch is usually installed so that it operates when the leading edge of the movable surface is opened. The switches may be either mechanical or magnetic, recessed or surface mounted, wired or wireless. They should always be installed on the protected or secure side. While surface-mounted switches are cheaper to install than those that are recessed, they may be more susceptible to damage and compromise. Surface-mounted switches also may not be aesthetically suitable for office or residential applications. References include FEMA 426 (Table 1-22 and Section 2.8) and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
2	13	Stairways are maintained with positive pressure, or other smoke control systems are present.	Stairwells required for emergency egress must be designed to meet applicable codes and must serve as an integral part of the OEP. As such, stairwells should be located as remotely as possible from areas where blast events might occur (e.g., lobbies, mailroom, loading dock, and parking areas). Wherever possible, do not have stairs discharge into lobbies, parking, or loading areas. Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc., out of the stairway. Pressurize exit stairways in accordance with ICC (2012). If this is not feasible, alternate means of smoke removal should be considered, such as venting the stairwell to the outside with the HVAC system. References include FEMA 426 (Table 1-22 and Section 2.23), U.S. General Services Administration (2005), ISC (2004), and CDC/NIOSH (2002).
3—Structural			
3	1	Surface or structured parking within 25 ft (7.6 m) (or based on risk and blast assessment) of the building is restricted to authorized vehicles.	As discussed in Gold Countermeasures Discipline 1, Countermeasure 1, a vehicle bomb can be a major terrorist or criminal threat to a facility. This applies to stationary and moving vehicles containing explosives. Each bit of setback can be of critical importance in reducing or limiting damage, injury, and death. The facility blast vulnerability analysis (see Silver Countermeasures Discipline 2 Countermeasure 1) will determine the required setback distance to protect against the threats identified in the risk assessment (see Silver Countermeasures Discipline 1 Countermeasure 1). Unauthorized vehicles, as determined by facility access control policies and procedures, should be prevented from parking within the required setback by access control. Security patrols and vehicle towing arrangements should be considered if access control is not fully adequate. The references (U.S. General Services Administration 2005, ISC 2004) recommend a standoff distance of 25 ft (7.6 m) as adequate to provide a medium level of protection. A higher level of protection can be achieved by providing a standoff distance greater than 25 ft (7.6 m). However, 25 feet (7.6 m) may not be available or required for all facilities. The reviewer must determine that a separation exists between public parking and critical/important assets. References include FEMA 426 (Table 1-22 and Section 1.11), U.S. General Services Administration (2005), and ISC (2004).
3	2	Unrestricted vehicle and pedestrian access is not permitted under building overhangs.	A terrorist bomb attack in which an explosive-laden vehicle is driven under a building overhang could result in catastrophic structural damage, injury, and death. Likewise, a hand-delivered bomb could cause significant damage and casualties, particularly in the confined space created by the overhang. If the overhang is supported by exposed columns, the detrimental effects of the device could increase. Pedestrian barriers and/or access control can be used to prevent access to this area. Barriers could include anticlimb fencing, screens, and grilles. Signs should be posted describing the prohibition of pedestrians and vehicles beneath the overhanging portion(s) of the building. Vehicle barriers of various types are designed to stop a vehicle before it can penetrate the defended setback. The stopping power or rating is based on the weight of the vehicle and the maximum speed it can attain prior to striking the barrier. The desired barrier rating for a particular facility is based on the required level of protection identified in the risk assessment. Active barriers for entrances include retractable bollards, swing gates, sliding gates, beam/cable barrier systems, and hydraulic wedge systems. Passive barriers include fixed bollards, concrete planters, freestanding walls, and terrace walls. To meet impact requirements, any barrier system proposed must be tested or otherwise certified by an independent testing lab or firm to meet or exceed the required vehicle size and impact velocity. Without proper site-specific design, there is no assurance that such barriers will perform as required. References include DoD (2002).

Discipline	Count	Countermeasure	Guidance
3	3	Ceiling and lighting systems are designed to remain in place during hazard events.	When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and nonstructural building components under loads not considered in standard building codes. It has been shown that connection criteria for these systems in high seismic activity areas resulted in much less falling debris that could injure building occupants. Ceilings and all overhead utilities and other fixtures weighing 14 kg (31 lb) or more should be constructed and mounted to minimize the likelihood that they will fall and injure building occupants. Equipment mountings should be designed to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This does not preclude the need to design equipment mountings for forces required by other criteria, such as seismic standards. References include FEMA 426 (Table 1-22 and Section 2.23) and DoD (2002).
3	4	All columns in the garage area are designed for an unbraced length equal to two floors, or three floors where there are two levels of parking.	Design of the columns for unbraced lengths longer than the actual as-built unbraced lengths allows for the potential loss of lateral support provided by a floor level or two due to a blast in the garage. Since the loss of lateral support was already considered in the design, this reduces the potential of progressive collapse. Refer to Silver Countermeasures Discipline 4 Countermeasure 8 for definitions and causes of progressive collapse. References include FEMA 426 (Table 1-22 and Section 3.6), U.S. General Services Administration (2005), and ISC (2004).
3	5	If primary construction is unreinforced masonry, precast concrete frame, concrete frames with unreinforced masonry infill walls, steel frames with unreinforced masonry infill walls, or tilt-up, blast or progressive collapse analysis should be performed. The threat and acceptance limits should both be consistent with the levels that were used in defining the classification of the building.	The primary type of construction influences the capability of the structure to respond to abnormal loading, including loads in directions contrary to conventional design loads. Different construction types inherently provide different levels of ductility (energy absorption) and potential redundancy for abnormal loadings such as blast. The ratings (points) for each construction type indicate potential capacity for sustaining abnormal and reversing loads. References include FEMA 426 (Table 1-22 and Section 3.1), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
3	6	If primary construction is braced steel frame, concrete shear wall, or reinforced masonry, then adequate ductile detailing away from the bracing system, shear wall, or reinforced masonry should be in place, as needed by the postulated threat.	These systems offer large global lateral resisting mechanisms. For locally applied hazards, care must be given to protecting the steel bracings and the concrete shear walls, because the loss of either might result in system-wide instability. Well-distributed lateral load systems within the plan of the building offer greater redundancy and better distribution of the load-resisting mechanisms. References include FEMA 426 (Table 1-22 and Section 3.1), U.S. General Services Administration (2005), and ISC (2004).
3	7	If primary construction is steel or concrete, moment-resisting frames or steel frames with cast-in-place concrete shear walls, then ductile detailing of all structural components should be constructed.	Moment frames offer good redundant systems. The load paths are numerous. To achieve this redundancy potential, connections must be designed so as to offer a large degree of ductility. A balance of moment-resisting connections and ductile components (columns and beams) must be achieved. References include FEMA 426 (Table 1-22 and Section 3.1), U.S. General Services Administration (2005), and ISC (2004).
3	8	If primary construction is wood framing or light metal, then adequate ductile detailing should be constructed.	Direct blast effects on these light systems can result in significant damage. Increased setbacks can mitigate such large damage effects. Special attention must be given to both redundancy (additional and adequate load paths) and hardening (resiliency in case of direct blast events). References include FEMA 426 (Table 1-22 and Section 3.1), U.S. General Services Administration (2005), and ISC (2004).
3	9	Symmetric steel reinforcement (positive and negative faces) exists in all floor slabs, roof slabs, walls, beams, and girders that may be subjected to rebound, uplift, and suction pressures (ONLY applies to reinforced concrete structures).	Subjected to an explosive detonation, components might act in directions for which they are not normally designed. This is due to the engulfment of structural members by blast, negative phase loading, upward loading of elements, and dynamic rebound of members. In a reinforced concrete structure, symmetric steel reinforcement increases the potential for structural capacity for load reversals. References include FEMA 426 (Table 1-22 and Section 3.6), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
3	10	Lap splices fully develop the capacity of the reinforcement (ONLY applies to reinforced concrete structures).	In a reinforced concrete structure, fully continuous tensile capacity provided by reinforcing steel is required to resist load reversals. Lap splices must be adequate to provide this continuity. References include FEMA 426 (Table 1-22 and Section 3.2).
3	11	Lap splices and other discontinuities are staggered (ONLY applies to reinforced concrete structures).	In a reinforced concrete structure, fully continuous tensile capacity provided by reinforcing steel is required to resist load reversals. Discontinuities must be minimized by staggering to provide this continuity. References include FEMA 426 (Table 1-22 and Section 3.2), U.S. General Services Administration (2005), and ISC (2004).
3	12	Special shear reinforcement, including ties and stirrups, is available to allow large postelastic behavior (ONLY applies to reinforced concrete structures).	Large postelastic behavior is required to absorb the significant energy delivered by abnormal loading events like blast loads. References include FEMA 426 (Table 1-22 and Section 3.2), U.S. General Services Administration (2005), and ISC (2004).
3	13	Connections possess ductile details.	Ductile connections are required to develop postelastic capacity of the connected members. References include FEMA 426 (Table 1-22 and Section 3.2), U.S. General Services Administration (2005), and ISC (2004).
3	14	Moment connections are used (ONLY applies to steel-frame structures).	In steel-framed structures, moment connections are required to develop the postelastic capacity of the connected members. References include FEMA 426 (Table 1-22 and Section 3.3), U.S. General Services Administration (2005), and ISC (2004).
3	15	Column spacing is not greater than 30 ft (9.1 m) for a reinforced concrete-framed or steel-framed structure.	Excessive column spacing will not permit reasonable structural designs, especially considering the requirements imposed by progressive collapse considerations, i.e., potential loss of a vertical load-carrying member like a column (doubled span). References include FEMA 426 (Table 1-22 and Section 3.3), U.S. General Services Administration (2005), and ISC (2004).
3	16	Floor heights are not greater than 16 ft (4.9 m) for a reinforced concrete-frame or steel-frame structure.	Excessive floor heights will not permit reasonable structural designs, especially considering the requirements imposed by progressive collapse considerations, i.e., potential loss of support for a vertical load-carrying member like a column (doubled column height). References include FEMA 426 (Table 1-22 and Section 3.3), U.S. General Services Administration (2005), ISC (2004), and U.S. General Services Administration (2001).

Discipline	Count	Countermeasure	Guidance
3	17	If exterior masonry walls are present, they are grouted and reinforced with at least 0.05% steel with spacing no less than 48 in. (1.2 m).	Avoid unreinforced masonry walls to increase capacity for abnormal loading and reduce hazardous debris potential. U.S. General Services Administration (2005) and ISC (2004) recommend fully grouted and reinforced concrete masonry unit (CMU) construction where CMU is selected. DoD (2002) states, “unreinforced masonry walls are prohibited for the exterior walls of new buildings. A minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1200 mm (48 in.) will be provided. For existing buildings, implement mitigating measures to provide an equivalent level of protection.” (This is light reinforcement and based upon the recommended standoff distance for the situation.) References include FEMA 426 (Table 1-22 and Section 3.9).
3	18	Facility is designed to prevent progressive collapse.	Refer to Silver Countermeasures Discipline 4 Countermeasure 8 for definitions and causes of progressive collapse. Progressive collapse may be a significant risk for buildings of three or more stories. Basements are considered stories if they have one or more exposed walls. For all buildings of three stories or more, the superstructure should be designed to sustain local damage with the structural system as a whole remaining stable and not being damaged to an extent disproportionate to the original local damage. This should be achieved through an arrangement of the structural elements that provides stability to the entire structural system by transferring loads from any locally damaged region to adjacent regions capable of resisting those loads without collapse. This may be accomplished by providing sufficient continuity, redundancy, or energy-dissipating capacity (ductility, damping, hardness, etc.), or a combination thereof, in the members and connections of the structure. In addition, the following measures should apply to all buildings of three or more stories. All exterior vertical load-carrying columns and walls should be able to sustain a loss of lateral support at any of the floor levels by adding one story height to the nominal unsupported length. While this standard is based on the assumption of an external threat, this provision also applies to internal vertical load-carrying columns and walls where parking beneath buildings is unavoidable. The structure should be analyzed to ensure that it can withstand removal of one primary exterior vertical or horizontal load-carrying element (i.e., a column or a beam) without inducing progressive collapse. All floors should have capacity to withstand load reversals due to explosive effects by designing them to withstand a net uplift equal to the dead load plus one-half the design live load. At a minimum, facilities should be designed for the loss of a column for one floor above grade at the building perimeter without progressive collapse. This design and analysis requirement for progressive collapse is not part of a blast analysis. It is intended to ensure adequate redundant load paths in the structure should damage occur for whatever reason. Designers may apply static and/or dynamic methods of analysis to meet this requirement. Ultimate load capacities may be assumed in the analyses. In recognition that a design-basis event may cause a partial collapse of the structure, new facilities with a defined threat should be designed with a reasonable probability that, if local damage occurs, the structure will not collapse or be damaged to an extent disproportionate to the original cause of the damage. The design should prevent progressive collapse due to the loss of one primary column, or it must be shown that the proposed design precludes such a loss. That is, if columns are sized, reinforced, or protected so that the design-basis event will not cause the column to be critically damaged, then progressive collapse calculations are not required for the internal event.

Discipline	Count	Countermeasure	Guidance
			As an example, if an event causes the local failure of one column and major collapse within one structural bay, a design mitigating progressive collapse would preclude the additional loss of primary structural members beyond this localized damage zone (i.e., the loss of additional columns, main girders, etc.). This does not preclude the additional loss of secondary structural or nonstructural elements outside the initial zone of localized damage, provided the loss of such members is acceptable for that performance level and the loss does not precipitate the onset of progressive collapse. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-02 (2003). For additional information concerning progressive collapse design, refer to Section 8 of U.S. General Services Administration (2005). References include U.S. General Services Administration (2005) and DoD (2005).
3	19	Where lobby retail exists, shared partitions are hardened against blast.	Permitting retail activities in nonsecured areas such as the building lobby is not advisable because it gives access to the public. Terrorists could use this advantage to plant a hand-carried bomb. However, the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting buildings. Retail and mixed uses may be accommodated, as required, through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures such as guard patrols. Hardening can be accomplished using blast-resistant materials for walls, floors, and ceilings. References include ISC (2004).
			4—Building envelope
4	1	Windows are designed to resist actual blast loads based on risk and blast assessments.	A terrorist vehicle bomb driven near or into the building or a hand-carried bomb placed close to the building creates secondary debris when detonated. In past explosive events where there was no building collapse, a large number of injuries resulted from flying glass fragments and debris from walls, ceilings, and fixtures (nonstructural features). The glass used in most windows breaks at very low blast pressures, resulting in hazardous, dagger-like shards. Minimizing those hazards by reducing window numbers and sizes and enhancing window construction has a major effect on limiting mass casualties. Windows should be designed to resist blast up to the specified load as directed by the facility's risk assessment. Window systems design (glazing, frames, anchorage to supporting walls, etc.) on the exterior façade should be balanced to mitigate the hazardous effects of flying glass following an explosive event. The walls, anchorage, and window framing should fully develop the capacity of the glass material selected. A combination of methods should be used. These include government-produced and -sponsored computer programs (see http://www.gsa.gov), coupled with test data and recognized dynamic structural analysis techniques, to show either that the window system survives the specified threats or that the postdamage performance protects the occupants. When using such methods to calculate reactions on frames and anchorage, a breakage probability no higher than 750 breaks per 1,000 trials should be used. All glazing hazard reduction products for these protection levels require product-specific test results. In addition, they require engineering analyses performed by qualified independent agents demonstrating the performance of the product under the specified blast loads and stating that it meets or exceeds the minimum performance-required load as specified by the facility's risk assessment. Preferred glazing systems include • Thermally tempered glass with a security film installed on the interior surface and attached to the frame; • Laminated—thermally tempered, laminated—heat strengthened, or laminated—annealed glass; and • Blast curtains.

Discipline	Count	Countermeasure	Guidance
			Acceptable systems include monolithic thermally tempered glass with or without film if the pane is designed to withstand the full design-basis threat. Unacceptable systems include untreated monolithic annealed or heat-strengthened glass and wire glass. In general, thicker antishatter security films provide higher levels of hazard mitigation than thinner films. Film that is 0.18 mm (7 mil) thick, or specially manufactured 0.1 mm (4 mil) thick film, is the minimum necessary to provide hazard mitigation from blast. References include FEMA 426 (Table 1-22 and Section 4.2), U.S. General Services Administration (2005), and ISC (2004).
4	2	All exterior doors in inhabited areas open outward to ensure seating in door frames.	If a terrorist bomb placed or driven near an entrance with a swinging door is detonated, the door might be propelled by the blast into the interior of the building, causing injury or death. If all exterior swinging doors into inhabited areas are installed so that they open outward, the doors will seat into the door frames in response to an explosive blast, increasing the likelihood that the doors will not enter the buildings as hazardous debris. If a door opens outward so that it seats against the inward frame, the hinges are on the nonsecure side of the door, which might facilitate unauthorized access. If the hinge pins are removed, the door can be opened whether or not it is locked. This situation can be addressed by preventing removal of the hinge pins. Methods to ensure that hinge pins are secured include • Providing concealed hinges, • Peening (i.e., hammering to mushroom the end of the pin), • Installing a hinge with a nonremovable pin, • Inserting a pin or set screw through the hinge pin on the inside of the hinge leaves, and • Installing a safety stud hinge. References include DoD (2002) and USAF (1997).
4	3	Enclosures for emergency egress are hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees.	Evacuees could be exposed to debris from an explosion that would impede safe passage. Stairwells required for emergency egress must be designed to meet applicable codes and must serve as an integral part of the OEP. As such, stairwells should be located as remotely as possible from areas where blast events might occur (e.g., lobbies, mailroom, loading dock, and parking areas). Wherever possible, do not have stairs discharge into lobbies, parking, or loading areas. However, if stairwells and other egress pathways do adjoin any of these areas, these egress pathways should be hardened against the effects of blast. Hardened stairwells allow egress of occupants after any blast event and permit more rapid response for first responders. References include FEMA 426 (Table 1-22 and Section 2.24) and FEMA 386-7 (2002).
4	4	Facility structure and exterior walls are designed to resist actual blast loads based on risk and blast assessments.	Terrorist groups that use bombs frequently seek international media coverage. Widespread coverage is more likely if the bombs are actually detonated rather than threatened. The hallmark of the terrorist bomb is not the threat in advance but the attribution or claim of responsibility after its detonation, which is usually accompanied by property damage, personal injuries, and deaths. Vehicle bombs are especially dangerous because the size of the explosive load that might be carried can cause extensive structural damage to the building, including progressive collapse. Facility structure and exterior walls should be designed to resist blast up to the specified load as directed by the facility's risk assessment.

Discipline	Count	Countermeasure	Guidance
			To address blast, the relative importance of a structural or nonstructural element should be considered in the following order: 1. Primary structural elements: the essential parts of the building's resistance to catastrophic blast loads and progressive collapse, including columns, girders, roof beams, and the main lateral resistance system; 2. Secondary structural elements: all other load-bearing members, such as floor beams, slabs, etc.; 3. Primary nonstructural elements: elements (including their attachments) that are essential for life safety systems, or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units; 4. Secondary nonstructural elements: all elements not covered in primary nonstructural elements, such as partitions, furniture, and light fixtures. Priority should be given to the critical elements that are essential to mitigating progressive collapse. Designs for secondary structural elements should minimize injury and damage. Consideration should also be given to reducing damage and injury from primary and secondary nonstructural elements. Structures should be designed to resist blast loads. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads. The design should use ultimate strengths with dynamic enhancements based on strain rates. Allowable responses are generally postelastic. Data on material properties and performance may be found in U.S. Army (1990) and Krauthammer et al. (1999). Also ensure that the walls are capable of withstanding the dynamic reactions from the windows. Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls must be considered primary structures. Design exterior shear walls to resist the actual blast loads predicted from the threats specified in the risk assessment. Where exterior walls are not designed for the full design loads, give special consideration to construction types that reduce the potential for injury. Where childcare centers are on the building exterior, the exterior childcare center walls should be designed to resist the actual blast loads predicted from the threats specified for the facility in the risk assessment to reduce the potential for child injury. References include FEMA 426 (Table 1-22 and Section 3.5), DoD (2002), and ISC (2004).
4	5	There is less than a 40% fenestration opening per structural bay.	Glazing is a major source of hazard for blast. Less glass produces fewer hazards. References include FEMA 426 (Table 1-22 and Section 4.2), U.S. General Services Administration (2005), and ISC (2004).
4	6	Nonbearing masonry walls are reinforced.	Avoid unreinforced masonry walls to increase capacity for abnormal loading and reduce hazardous debris potential. References include FEMA 426 (Table 1-22 and Section 4.2), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
4	7	Nonwindow openings have been designed to the level of protection required for exterior walls.	If a bomb detonates outside the building, nonwindow openings, such as mechanical vents and exposed plenums, can subject the structure to infilling of blast overpressures. Nonwindow openings should provide the level of protection required for exterior walls. Infilling of blast overpressures must be considered through nonwindow openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures. Nonwindow openings should provide as much protection as the rest of the building envelope against forced entry. References include FEMA 426 (Table 1-22 and Section 4.5), U.S. General Services Administration (2005), and ISC (2004).
4	8	Security glazing meets the requirements of ASTM F1233 (1998) or UL 972 (2002).	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs and WMDs. In addition to alarm sensors to detect attempted entry through windows, windows can be made more resistant to entry with security glazing. In these cases, the glazing material should meet the requirements of ASTM F1233 or UL 972. Glass-clad polycarbonate and laminated polycarbonate are two types of acceptable glazing material for this application. If windows are upgraded to bullet resistant, burglar resistant, or forced entry resistant, ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern. Fire safety is an important consideration in blast-resistant window design. A fire protection engineer should evaluate the performance requirements for all security glazing materials proposed for a facility. Normal tools carried by firefighters, such as a pick head axe, halligan tool, or similar device, may not readily overcome ordinary glazing barriers. If the use of more specialized tools, such as a rabbit tool, a k-tool, circular saws, rams, or similar devices are necessary to break through the glazing barrier or if the glazing itself is hardened so that high pressures may not blow out the windows, alternative methods or systems to ensure that smoke from an incident is not trapped inside the building must be implemented. References include FEMA 426 (Table 1-22 and Section 4.4), U.S. General Services Administration (2005), and ISC (2004).
5—Utilities			
5	1	Emergency generator is access controlled.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to life safety and security systems. Emergency power must be provided to essential building services, especially those required for life safety, evacuation, and shelter in place, providing lighting and surveillance to deter and detect criminal activities and providing emergency communication. If the emergency generator is installed outdoors at grade, it should be protected by perimeter walls (barriers) and locked entrances. When barriers are installed outdoors, clear zones should be established on both sides to provide an unobstructed view of the barrier and adjacent terrain. Clear zones should be kept free of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to breach the barrier. References include FEMA 426 (Table 1-22 and Section 1.18), U.S. General Services Administration (2005), ISC (2004), and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
5	2	Emergency generator system is protected by intrusion-detection devices.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power must be provided to life safety and security systems. Emergency power must be provided to essential building services, especially those required for life safety, evacuation, and shelter in place, providing lighting and surveillance to deter and detect criminal activities and providing emergency communication. Intrusion-detection devices (sensors) are the basic ingredients of an alarm system. They detect the condition or event indicating a security problem. All logical discrimination, transmission, processing, display, and recording activities that occur subsequent to initial detection have meaning because of what sensors see, hear, feel, or otherwise sense with optical, electronic, electromechanical, or mechanical capabilities. The types of intrusion devices appropriate for outdoor use are classed as “point of entry” sensors and include the following. Passive infrared sensors, commonly referred to simply as PIRs, are the most widely used intrusion detectors today and are highly versatile. PIRs “see” the invisible, bold colors of thermal or infrared (IR) energy. Because there is no beam, they are called passive. This energy, like heat from the sun, has no visible color or light. Just as a camera takes in light, a PIR sees warm, infrared images against a cooler background. The microwave sensor operates on generally the same principle as the ultrasonic sensor. The difference lies in the type of wave or signal used. The ultrasonic sensor uses a high-frequency sound wave, whereas the microwave sensor utilizes much higher frequency electromagnetic energy. The microwave transmitter sends a signal that is reflected back to an antenna. A comparison circuit compares the transmitted and reflected signals. If there is no movement in the area, the waveform remains constant. When the signal is reflected from a moving object, the waveform changes, initiating an alarm. Microwave sensors may be utilized in outdoor and indoor applications, because they are not generally affected by heavy fog, rain, snow, sleet, air turbulence, drafts, noise, temperature extremes, or atmospheric disturbances. Photoelectric sensors operate based on modification of a light level or interruption of a light beam protecting an area. In the first application, an ambient light threshold is established in a protected area. When an intrusion alters this light level, the sensor initiates an alarm. If the light beam is visible, it can be avoided. For this reason, infrared filters are usually placed over the light source so only invisible light is transmitted. Because photoelectric cells are sensitive to infrared, no modification to the receiver is necessary. A balanced pressure sensor has been developed for outdoor applications. This sensor consists of liquid-filled hoses spaced about 4 ft (1.2 m) apart. A differential pressure sensor is connected at one end of each hose or tube. Intruders are detected by sensing slight changes in differential pressure on soil as intruders walk or crawl over ground where hoses are buried. When a momentary pressure differential is sensed, an alarm is generated. The hoses can be buried to conform to the contour of the ground along fence lines or across open spaces. Closed-circuit television use as a motion alarm sensor has grown in recent years. Measurement of a change in the scene under CCTV surveillance is the basis for this technology. The scene is stored and compared to the real-time signal during the next frame. Such systems are capable of detecting and comparing motion on multiple video signals, generating hardware or software alarms. Parameters of motion-detection algorithms—such as for the sensitivity of detection—are under user control. While these devices prove useful in many applications, the generation of a video alarm alone cannot determine whether the “intruder” appearing in the image is a “good guy” or a “bad guy.” With digitized imagery it is possible to develop TV motion detection even further in that any number of screen “bits” can be selected for change (movement) monitoring. Irregular patterns of a screen display can thus be studied without being affected by status changes elsewhere in the scene being viewed.

Discipline	Count	Countermeasure	Guidance
			The level of monitoring and the agency performing this duty vary with the level of protection, size, assets, complexity, and occupancy of the facility. At the low end of the scale, monitoring can be provided by a commercial central station or, in special circumstances, an on-site security central control center can be provided during normal business hours. A more advanced measure of safety and security can be provided by monitoring at an on-site, proprietary security control center. To mitigate staffing requirements and annual operating costs, commercial central stations are sometimes used for after-hours monitoring or to supplement on-site monitoring. At the high end of the protection scale, security systems should be monitored by an on-site, 24-hour proprietary security control center. References include FEMA 426 (Table 1-22 and Section 1.18), U.S. General Services Administration (2005), ISC (2004), and ASIS (2012).
5	3	Utilities have redundant and separated paths for entering facility.	Gas, water, steam, and electric power supplies could be disrupted by a terrorist, criminal, or militant attack, greatly affecting or shutting down the facility. Water should be available from two or more pumping stations. Supply piping should be separated as much as possible. Two or more gas supply pipelines should enter the facility at separate locations. Feeders from two or more electrical substations should enter the property at different points, separated as much as possible. References include FEMA 426 (Table 1-22 and Section 5.15).
5	4	Incoming utility systems have blast protection, including burial or proper encasement.	Protecting utility systems, locating them away from vulnerable areas, and restricting access help ensure that services will facilitate life safety and operations support after an event such as a terrorist attack or other emergency. Overhead electrical transmission lines should be avoided. Within building and property lines, conceal incoming utility systems (e.g., water, electricity, or steam) and give them blast protection, including burial or proper encasement (e.g., ducts, conduits, and guard pipes), wherever possible. References include FEMA 426 (Table 1-22 and Section 5.19).
5	5	Facility has a backup control center (BCC) for off-site monitoring of alarm, fire, and building maintenance systems.	A terrorist or criminal attack could degrade the communications and monitoring ability of the operations, fire, and security control centers. A backup control center provides redundancy in case the primary center is disabled. A fully redundant BCC should be installed at an off-site location. The BCC should have equivalent capability for voice, data, mass notification, emergency operations, security, fire alarms, and building automation. The BCC should have access to backup systems, including emergency power. References include FEMA 426 (Table 1-22 and Section 10.16), U.S. General Services Administration (2005), and ISC (2004).
5	6	There are alternate water supplies for fire suppression.	The concern is that the fire suppression water supply should be adequate to fight the worst-case situation according to the fire codes. A terrorist bomb attack against a single source of supply could result in an inadequate supply of water. The fire suppression system water may be supplied from the domestic water, or it may have a separate source, separate storage, or nonpotable alternate sources. Whatever the source of fire suppression water (e.g., local utility company lines, storage tanks with utility company backup, lake, or river), there should always be alternate supplies. This will prevent a single-point failure leaving the facility without enough water for fire suppression. References include FEMA 426 (Table 1-22 and Section 5.2) and FEMA 386-7 (2002).

Discipline	Count	Countermeasure	Guidance
5	7	The sprinkler and standpipe connections are adequate and redundant.	The concern is that the fire sprinkler/standpipe system should be adequate to fight the worst-case situation according to the fire codes. A terrorist bomb attack against a single point in a nonredundant system could result in inadequate fire suppression capability. Sprinkler and standpipe connections should be adequate as determined by the site fire protection analysis. There should be redundancy to prevent a single-point failure leaving the facility without adequate fire suppression capability. References include FEMA 426 (Table 1-22 and Section 5.7) and U.S. General Services Administration (2005).
5	8	Fire hydrant and water supply connections are near the sprinkler/standpipe connections.	The concern is that the fire sprinkler/standpipe system should be adequate to fight the worst-case situation according to the fire codes. A terrorist bomb attack against a single point in the water supply to the fire suppression system could result in failure to suppress the fire. Placing water supply connections near sprinkler standpipe connections could provide an alternate supply of water if temporary connections were made between the two. A nearby fire hydrant could be connected by hose to supply water to the fire suppression system. References include FEMA 426 (Table 1-22 and Section 5.7) and U.S. General Services Administration (2005).
5	9	Fire water pumps are redundant (e.g., one electric, one diesel).	The concern is that the fire sprinkler/standpipe system should be adequate to fight the worst-case situation according to the fire codes. If a single pump provided pressurized water to the fire suppression system, loss of the pump would result in loss of fire suppression capability. With two pumps, the normal source to drive the pump, which is usually electrical power, could be disrupted. The second pump, normally driven by a diesel engine, would then start to take over the duty of supplying fire-suppression water. There should be an adequate supply of fuel for the diesel-driven pump as determined by the site fire protection analysis. References include FEMA 426 (Table 1-22 and Section 5.7) and U.S. General Services Administration (2005).
5	10	The water pumps are located apart from one another.	The concern is that the fire sprinkler/standpipe system should be adequate to fight the worst-case situation according to the fire codes. Colocating fire water pumps puts them at risk for a single incident to disable the fire-suppression system. With two pumps, the normal source to drive the pump, which is usually electrical power, could be disrupted. The second pump, normally driven by a diesel engine, would then start to take over the duty of supplying fire-suppression water. The pumps should be separated, preferably in blast-resistant enclosures. References include FEMA 426 (Table 1-22 and Section 5.7), FEMA 386-7 (2002), and U.S. General Services Administration (2005).
5	11	Access to security system, emergency communication system, and associated systems' wiring and conduits is controlled, preferably by routing them through separate and secure closets.	In the event of an attack or other emergency, adequate communication systems are vital to the response by staff and off-site responders. A single-point failure should not be allowed to disrupt security systems, emergency communication systems, and associated systems. Multiple distribution runs, separated as much as possible and not located near high-risk areas, should be used for hardwired communications such as telephones, public address systems, and data transmission systems. The wiring and conduits should be controlled preferably by routing them through separate and secure closets. Closets should be access controlled and equipped with intrusion-detection devices. References include FEMA 426 (Table 1-22 and Section 5.20) and ISC (2004).

Discipline	Count	Countermeasure	Guidance
6—Mechanical			
6	1	Automated access control system is provided to monitor access to mechanical, electrical, and telecommunication rooms.	Mechanical areas may exist at one or more locations within a building. These areas provide access to centralized mechanical systems (HVAC, elevator, water, etc.), including filters, air-handling units, and exhaust systems. Such equipment is susceptible to tampering and may subsequently be used in a CBR attack. Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. For example, electric power systems can suffer significant damage when subjected to the shock of an explosion from a bomb placed in an electrical room. Electrical power may be critical for safely evacuating people from the building. Destruction of critical electrical components could cause damage that is disproportionate to other building damage resulting from an explosion. Damage from an attack on telecommunications rooms could leave the facility without adequate communications with off-site authorities and first responders and could hinder on-site communications with security and safety personnel. Access to mechanical, electrical, and telecommunications rooms can be safeguarded by automated access controls. The system would monitor access by authorized personnel and delay access by an attacker. Refer to Gold Countermeasure Discipline 2 Countermeasure 6 for a discussion of automated access control systems. Authorized facility operations, maintenance, and management personnel can be granted unescorted access to equipment and utility rooms. To deter tampering by outside maintenance personnel, a building staff member can escort these individuals throughout their service visit and visually inspect their work before final acceptance of the service. Alternatively, building owners and managers can ensure the reliability of prescreened service personnel from a trusted contractor. References include FEMA 426 (Table 1-22 and Section 6.2), CDC/NIOSH (2002), Lawrence Berkeley National Laboratory (2003), U.S. General Services Administration (2005), and ISC (2004).
6	2	Fire dampers are installed at all fire barriers.	Fire can be one of the most destructive events, whether accidental or the result of a terrorist arson or bomb attack. Fire dampers should be installed at all fire barriers to retard the spread of smoke and flame through the barriers. All dampers (fire, smoke, outdoor air, return air, and bypass) must be functional for proper protection within the building during an incident. Rapid acting dampers should be used when feasible. References include FEMA 426 (Table 1-22 and Section 6.18) and CDC/NIOSH (2002).
6	3	HVAC systems are isolated in lobbies, mailrooms, loading docks, and other locations where the significant risk of CBR contamination exists.	Terrorist, militant, or criminal groups may attack a facility with CBR agents. Lobbies, mailrooms, loading docks, and other entry and storage areas are the most susceptible to the introduction of bulk quantities of CBR agents. Isolating these areas from other areas of the building will reduce the potential for wider dissemination of hazardous agents. These areas should not share a return air system or return pathway (e.g., ceiling plenum) with other areas of the building. To limit migration into buildings of airborne chemical, biological, and radiological agents introduced into lobbies, mailrooms, loading docks, and other locations where significant risk of CBR contamination exists, ensure that these areas are well sealed between their envelopes and other portions of the buildings in which they are located. Ensure that the walls fully extend and are sealed to the undersides of the roofs, to the undersides of any floors above them, or to hard ceilings (i.e., gypsum wallboard ceiling). Sealing should include visible cracks, the interface joints between walls and ceilings/roofs, and all wall and ceiling/roof penetrations. Doors should have weather stripping on all four edges. References include FEMA 426 (Table 1-22 and Section 6.8), DoD (2002), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
6	4	Lobbies, mailrooms, and loading docks maintain negative pressure relative to the rest of the facility.	Terrorist, militant, or criminal groups may attack a facility with CBR agents. Lobbies, mailrooms, loading docks, and other entry and storage areas are the most susceptible to the introduction of bulk quantities of CBR agents. These areas should not share a return air system or return pathway (e.g., ceiling plenum) with other areas of the building. Applying HVAC zones that isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building's HVAC zones and maintaining negative pressure within these areas will contain CBR releases. Identify common return systems that service more than one zone, effectively making a large single zone. Conversely, emergency egress routes should receive positive pressurization to ensure that contamination does not hinder egress. Consider filtering of the pressurization air. References include FEMA 426 (Table 1-22 and Section 6.8) and CDC/NIOSH (2002).
6	5	Gas adsorption filters are used on recirculated air and on outside air intakes.	Terrorist, militant, or criminal groups may attack a facility with a gaseous chemical agent. There could also be a release of gas from a hazardous material accident. These incidents can be exterior to or within the facility. Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern are the airflow patterns and dynamics in buildings, specifically in building heating, ventilating, and air conditioning (HVAC) systems. These systems can become an entry point and a distribution system for hazardous contaminants, particularly CBR agents. It is important to note that particulate air filters are used for biological and radiological particles and are not effective for gases and vapors typical of chemical attacks. These types of compounds require adsorbent filters (i.e., activated carbon or other sorbent-type media) and result in substantial initial and recurring costs. Adsorbent filters should be used on recirculated air and that from the air intakes. References include FEMA 426 (Table 1-22 and Section 6.4), ISC (2004), and CDC/NIOSH (2002).
6	6	Ventilation system is connected to an emergency power system.	Terrorists may release a CBR agent inside or outside a building or may direct a large-scale attack in the area. They may also strike using a bomb or incendiary to cause a fire. Following notification of a CBR release or fire, HVAC equipment will be used in one or more modes to mitigate the consequences. Depending on whether the agent is released inside or outside the building, the air intake may need to be shut down. In the case of an interior release, certain parts of the building may need to be isolated. If the HVAC system is also the smoke removal system, it will have to operate in that mode. The HVAC system can be vital to supporting an evacuation or shelter-in-place situation. It may be the only system offering collective protection for chemical, biological, and radiological contamination designed into the building. If a fire or explosion disrupts the normal electrical power supply, emergency power should be available to ensure that the HVAC system can be shut down or operated in the proper mode. References include FEMA 426 (Table 1-22 and Section 6.4), ISC (2004), and CDC/NIOSH (2002).

Discipline	Count	Countermeasure	Guidance
6	7	CBR analysis has been performed using air-plume models to determine threat to facility.	Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern is the intentional (e.g., terrorist or militant group) or accidental release of chemical or biological agents at some point outside the building under consideration. The obvious concern is that airborne contamination will reach the building and enter through air intakes or infiltration through the envelope of the building. Rapid determination of a contaminated area's location, size, and toxicity is imperative for prompt situational assessment of a chemical or biological incident. The fastest method of predicting a contaminated area's characteristics is by simulating the path of the toxic plume using fluid flow analysis in conjunction with the forecasted weather conditions. The timeliness of this information is critical to the selection of a plan of action to be taken in response to such an incident. The simulations that solve the partial differential equations describing the fluid flow of the chemical or biological contaminants are a function of the weather, the terrain, and the scale of the area of interest. Modeling and simulation software packages can provide very good simulations. A geographic information system (GIS) is a computerized database management system used for the capture, storage, retrieval, analysis, and display of spatial (i.e., defined by location) data. A GIS can be used to analyze the extent of a chemical attack using a plume-analysis application. By taking into account, for example, wind direction and topographic and demographic data, the extent of spread of the chemical plume can be better understood. References include Ferketic (2002) and Holzhauer et al. (2000).
7—Plumbing and gas			
7	1	Exterior water mains are looped and sectionalized to prevent disruption from damage.	A terrorist or militant attack could be directed at the facility's supply of water for fire suppression and facility operation. This could compound the results of a bomb or arson attack. An adequate water supply is essential for support of fire suppression and facility operations. Protecting the water supply and/or locating it away from vulnerable areas help ensure that services will provide life safety and operations support after an event. The water system should be protected from single-point failure. The incoming line should be encased, buried, or located 15 m (50 ft) from high-threat areas. The exterior mains should be looped and sectionalized. Looping of piping and use of section valves provides redundancies in the event sections of the system are damaged. References include FEMA 426 (Table 1-22 and Section 7.3) and ISC (2004).
7	2	Water supply has backflow preventers.	If the facility is part of a campus, terrorists might try to contaminate the surrounding buildings with a chemical or biological agent by introducing the agent into the water supply at one building. Normally the contaminated fluid would pass to the waste collection system. Unfortunately the water sometimes reverses direction back through the water meter. This reversal of direction is called backflow. The most common type of backflow is backsiphonage. Backsiphonage is caused by a sudden loss of pressure in the public water mains. This loss of pressure can be caused by a broken water main, a nearby fire that causes the fire department to use large quantities of water, or simply a fire hydrant opened for testing. Any buildings near the break or the fire hydrant being used will experience a lowering of the water pressure. This is when backsiphonage occurs. Terrorists may deliberately disrupt the water supply at a public main outside the facility's perimeter. The subsequent backflow could spread contamination to other buildings when water service is restored. Backflow preventers keep contaminants that may be introduced into the water system inside the property or building from backflowing into the supply lines if pressure in the delivery system is lost. References include American Backflow Prevention Association (ABPA 2014) and ISC (2004).

Discipline	Count	Countermeasure	Guidance
7	3	Water supply is protected from single-point failure, or redundant supply is provided.	Terrorists or militants may attack the incoming water supply to disrupt the facility's mission. They may either cut off the supply or attempt to contaminate it. Domestic water is critical for continued building operation. Although bottled water can satisfy requirements for drinking water and minimal sanitation, domestic water meets many other needs—flushing toilets, building heating and cooling system operation, cooling of emergency generators, humidification, etc. Exterior sources of water for fire suppression are vital to the security and safety of the facility and its occupants in the event of criminal, terrorist, or militant attack by bombs or incendiaries. If the building or site has only one source of water entering at one location, the entry point should be secure. For the greatest protection within building and property lines, conceal incoming utility systems by means including burial or proper encasement, wherever possible. Incoming water piping systems should be located away from loading docks, entrances, and parking. Underground service is preferred. Consideration should be given to obtaining a backup water supply to the facility from a separate pumping station. References include FEMA 426 (Table 1-22 and Section 5.2), FEMA 386-7 (2002), U.S. General Services Administration (2005), and ISC (2004). 9—Fire
9	1	For enclosures, an automatic fire door or rolling fire shutter with an access door is employed so that the area is wide open during normal use.	Terrorist, criminal, or militant groups may use arson, bomb, or CBR agent attacks to accomplish their goal of harming a facility and its staff. The principal means of passive fire protection in structures is by completely enclosing areas with fire barriers. Fire barriers include fire doors, walls, ceilings, and floors. Fire barriers play an integral role in managing a fire by interrupting the spread of smoke, other toxic gases, and the fire itself from one fire zone into another. Fire doors are fundamental to the integrity of fire barriers because any time an access portal (such as a doorway) leads to a compartment, a fire barrier is broken temporarily. To minimize the break in protection, fire doors must be self-closing and have proper latching devices to provide as much resistance as possible to the spread of fire, smoke, and toxic gases. Fire exit doors are often held open for the convenience of employees and visitors, creating a significant fire hazard for all building occupants because of the break created in the fire barrier. Doors that are designed to be fire exit doors can be held open, but only if they automatically release when building fire alarms are activated. Occupational Health and Safety Administration (OSHA) regulations require that fire doors not be held open unless equipped with a device that releases the door upon activation of the fire alarm [29 CFR §1910.36 (a)(3)]. When fire doors are needed: • Where a door has an EXIT sign on or around it, • Where a door leads to exit stairwells and horizontal exits, • Where a door leads to a hazardous area such as flammable storage, and • In general, where a door leads to a hallway or from one fully enclosed room to another. An important consideration for sheltering in place (e.g., during an exterior CBR release) is that stairwells must be isolated by closed fire doors. The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal, by zone ducting, fire walls, fire stops, and fire doors) provides energy conservation benefits and functional benefits during a CBR incident. Hazards to avoid with fire doors: Fire doors should never be tied open or held open by unapproved devices, such as door wedges and blocks. Fire doors can only be held open by a device that automatically releases when the fire alarm is activated (such as an electromagnetic hold open device). Even when closed, fire doors should never have their latch taped over; during a fire, hot gases can easily build up enough pressure to cause fire doors to blow open. References include FEMA 426 (Table 1-22 and Section 6.19) and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
9	2	Automated access control system is provided to monitor access to command and control center(s).	Terrorists or militants wanting to gain control over a facility to inflict the maximum damage might attempt forced entry into one or more of the control centers. This would place life safety (fire alarm and suppression, HVAC, and communications) and security systems (access control and intrusion detection) in jeopardy. Access to command and control centers can be safeguarded by automated access controls. The system would monitor access by authorized personnel and delay access by an attacker. Refer to Silver Countermeasure Discipline 2 Countermeasure 14 for a discussion of automated access control systems. References include FEMA 426 (Table 1-22 and Section 9.2).
9	3	Doors and shutters are closed by a smoke detector when needed instead of a fire-rated door that remains closed all the time.	Terrorist, criminal, or militant groups may use arson, bomb, or CBR agent attacks to accomplish their goal of harming a facility and its staff. The principal means of passive fire protection in structures is by completely enclosing areas with fire barriers. Fire barriers include fire doors, walls, ceilings, and floors. Fire barriers play an integral role in managing a fire by interrupting the spread of smoke, other toxic gases, and the fire itself from one fire zone into another. Fire doors are fundamental to the integrity of fire barriers because any time an access portal (such as a doorway) leads to a compartment, a fire barrier is broken temporarily. To minimize the break in protection, fire doors must be self-closing and have proper latching devices to provide as much resistance as possible to the spread of fire, smoke, and toxic gases. Fire exit doors are often held open for the convenience of employees and visitors, creating a significant fire hazard for all building occupants because of the break created in the fire barrier. Doors that are designed to be fire exit doors can be held open, but only if they automatically release when building fire alarms are activated. OSHA regulations require that fire doors not be held open unless equipped with a device that releases the door upon activation of the fire alarm [29 CFR §1910.36 (a)(3)]. When fire doors are needed: • Where a door has an EXIT sign on or around it, • Where a door leads to exit stairwells and horizontal exits, • Where a door leads to a hazardous area such as flammable storage, and • In general, where a door leads to a hallway or from one fully enclosed room to another. An important consideration for sheltering in place (e.g., during an exterior CBR release) is that stairwells must be isolated by closed fire doors. The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal, by zone ducting, fire walls, fire stops, and fire doors) provides energy conservation benefits and functional benefits during a CBR incident. Hazards to avoid with fire doors: Fire doors should never be tied open or held open by unapproved devices, such as door wedges and blocks. Fire doors can only be held open by a device that automatically releases when the fire alarm is activated (such as an electromagnetic hold open device). Even when closed, fire doors should never have their latch taped over; during a fire, hot gases can easily build up enough pressure to cause fire doors to blow open. References include FEMA 426 (Table 1-22 and Section 6.19) and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
9	4	Alternate methods, such as painting handrails, stair treads, signs, and doors with phosphorescent paint, are used to illuminate or delineate stairwells and emergency exits.	Visibility of exit pathways is vital to life safety in the event of an emergency that requires evacuation of the facility, such as a terrorist bomb attack. Visibility can be provided by using emergency powered or self-contained battery lights in stairwells and for exit signs. As an alternative to battery-powered lighting, handrails, stair treads, signs, and doors can be painted with phosphorescent paint. References include FEMA 426 (Table 1-22 and Section 11.8), FEMA 386-7 (2002), and ISC (2004).
9	5	Facility has an area designated as the emergency command center (ECC), where building documents such as emergency instructions, OEP manuals, and building plans are readily available.	A terrorist attack or natural disaster could result in a large-scale emergency situation. An emergency command center, sometimes known as an emergency operations center (EOC), is a location in the facility, preferably in the operations control center (with alternate locations), where a team can assemble to deal with emergency or disaster situations beyond what security and safety personnel can handle. The ECC commander should be given the responsibility of assessing the situation and determining whether an event is a disaster. If a disaster occurs, the ECC commander may activate the ECC. Assisted by the ECC team members, he or she will make decisions and move forward to respond to the disaster. The ECC team should include the following: ECC commander; security chief; and ECC support (e.g., technical assistants, event recorder, messengers, and reporters). Where applicable, members of the team should also include representatives from • Safety and environmental management; • Facility management; • Engineering; • Operations; • Human resources; • Information technology; • Public information; and • Planning, management, and budget. The responsibilities of the ECC team should include • Resource management; • Direction, control, and coordination; • Communications and warning; • Operations and procedures; and • Crisis communications, public education, and information. The critical information that should be readily available to the ECC team (i.e., prepositioned) includes emergency instructions, call lists, facility OEP manuals and building plans, and maps and drawings. Specific functions of the ECC should include • Coordinating the response to an event; • Gathering and disseminating information to aid response activities and assist employees, visitors, and their families during an event; • Communicating with emergency responders to provide necessary information to facilitate rescue and/or disaster mitigation efforts; • Facilitating the allocation of resources, as necessary, to respond to disasters; • Shifting guards and/or other manpower to facilitate evacuation and securing the facility; and • Directing emergency responders and providing maps and/or site plans of facilities. References include FEMA 426 (Table 1-22 and Section 9.1), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
10—Communications and IT			
10	1	Perimeter cameras are supported by an uninterruptible power supply, battery, or building emergency power.	CCTV can be a valuable tool for deterring terrorists, criminals, and militants from attacking a facility or identifying an intrusion or potential attack (i.e., alarm assessment) at the site perimeter. Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. In the event of a disruption, electrical power should be provided to security systems including the perimeter CCTV cameras. Various sources of emergency power can be UPS systems, batteries, power conditioners, and emergency generators. References include FEMA 426 (Table 1-22 and Section 12.9).
10	2	Facility has a base radio communication system with antenna installed in the stairwell and portable sets distributed on floors.	Emergencies created by terrorist, criminal, or militant attack may cause the building to be evacuated. Communication is essential in any situation that requires evacuation of the building. Floor monitors (fire wardens) should be equipped with portable radios that will give them contact with the base radio station. The base station should be located in the security control center or colocated command and control centers, which can provide situation reports to the monitors. Additionally, the radio system will facilitate communication and coordination between the floors of a building during the evacuation. Installing antennas or repeaters in the stairwell will ensure that floor monitors evacuating their people will remain in communication during the evacuation. Locating antennas in the stairwell could also serve to isolate them from the damaged parts of the building because stairwells are usually more robust than other parts of the structure. References include FEMA 426 (Table 1-22 and Section 12.35) and ISC (2004).
10	3	A UPS is connected to the emergency power system for life safety and security systems.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. For example, electric power systems can suffer significant damage when subjected to the shock of an explosion. Electrical power may be critical for safely evacuating people from the building. Destruction of critical electrical components could cause damage that is disproportionate to other building damage resulting from an explosion. Such systems can include • Access control, • Alarms, • Building control centers, • Communications, • Elevators, • Emergency lighting, • Fire suppression, and • HVAC (smoke removal). Normally these emergency services are provided with an emergency generator or a tertiary power source. Some types of electronic security system equipment, such as processors with solid state memory, cannot tolerate short interruptions of power, which will occur during switchover from the normal power source to an engine-driven emergency power source. This volatile electronic equipment must be provided with an uninterruptible power supply to bridge the gap between the event and activation of the main emergency power source. A UPS consists of a rectifier, batteries, and inverter. References include FEMA 426 (Table 1-22 and Section 8.6), U.S. General Services Administration (2005), ISC (2004), and U.S. Army (1994).

Discipline	Count	Countermeasure	Guidance
10	4	Redundant communications system is provided.	In the event of an attack or other emergency, adequate communication systems are vital to the response by staff and off-site responders. A single-point failure of one method of communication should not be allowed to disrupt communications. Where applicable, the communication systems should be connected to an emergency power source. Wireless data transmission minimizes the risk of communications breakdowns due to wiring damage. Radio telemetry can be used for nonsecure data that support the life safety system and other critical operations. For the greatest protection, distributed antennas could be located throughout the facility if required for emergency communication through wireless transmission of data. Other communications systems such as a second telephone system, intercom, portable radio, pager, cell phone, walkie-talkie, and personal data assistants (PDAs) should be considered. Messengers can be used as a last resort. References include FEMA 426 (Table 1-22 and Section 5.20) and ISC (2004). 11—Equipment operations and maintenance
11	1	A computerized security incident reporting system is used to prepare reports and track security incident trends and patterns.	In the past, law enforcement organizations used a “blotter” to track various incidents (e.g., crime, detentions, arrests, accidents, bomb and CBR threats, and attacks) and to provide a record of actions taken and the disposition of a case. Computerized systems can now facilitate this record keeping. Databases can be compiled to track security incident trends and patterns at the facility. The main station for the automated reporting system is usually located in the SCC at the security console. The advantage of the computerized system lies in the ability of other security personnel to enter reports into the blotter system. References include FEMA 426 (Table 1-22 and Section 12.36).
11	2	Critical air systems have been rebalanced at least once a year.	Critical HVAC systems must be fully operational to ensure that they function as intended to mitigate the consequences of an attack or other emergency situation. Although the systems may function, critical HVAC systems should be tested and rebalanced at least once a year to ascertain their capability to perform as intended. They should be tested and rebalanced after any changes to the system (e.g., bigger blowers or additional or new filters). Annual testing is to be conducted in addition to required periodic system testing. Although the system may function, it must be tested periodically to ensure it is performing as designed. Balancing is also critical after initial construction to set equipment to proper performance per the design. Rebalancing may only occur during renovation. References include FEMA 426 (Table 1-22 and Section 11.2) and CDC/NIOSH (2002).
11	3	Backup power systems are tested monthly under load.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. For example, electric power systems can suffer significant damage when subjected to the shock of an explosion. Electrical power may be critical for safely evacuating people from the building. Destruction of critical electrical components could cause damage that is disproportionate to other building damage resulting from an explosion. In the event of a disruption, emergency power must be provided to essential building services, especially those required for life safety, evacuation, and shelter in place, providing lighting and surveillance to deter and detect criminal activities, and providing emergency communication. Usually backup power is provided by a diesel-driven emergency generator. The backup system should be tested monthly under load. Loading should be at or above maximum connected load to ensure available capacity, and automatic sensors should be tested at least once per year. Periodically (once a year as a minimum) check the duration of capacity of backup systems by running them for the expected emergency duration or estimating operational duration through fuel consumption, water consumption, or voltage loss. References include FEMA 426 (Table 1-22 and Section 11.7) and FEMA 386-7 (2002).

Discipline	Count	Countermeasure	Guidance
12—Security systems			
12	1	Assistance stations within parking facilities or other remote areas have broadcast capability for emergency notification.	To reduce both the real exposure and the perceived risk of drivers and passengers to personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants, alarm devices and intercoms can be installed at selected lot and garage locations. In addition to duress alarm buttons, assistance stations can be provided with a separate or integrated intercom system to permit conversation between the person requesting assistance and the monitoring station. The intercom system would be useful for identifying the emergency so that the proper forces could respond (e.g., EMTs for a medical emergency, fire department, police, or driver assistance). The intercom system can also be used as a part of the mass communications system, which can be used to provide emergency information to persons within the parking facilities or in other remote areas of the facility. References include FEMA 426 (Table 1-22 and Section 12.4).
12	2	Cameras are oriented to record license plates of entering and departing vehicles and to record pedestrians exiting or entering via vehicle ramps.	The risk of personal attack (assault, robbery, rape, carjacking, or kidnapping); exposure of vehicles and their contents to larceny; and violent acts by terrorists or militants increases when access to parking facilities is uncontrolled. The use of CCTV with video-recording capability may reduce the risk associated with these threats. Points of prime concern are the entry and exit locations. Cameras should be oriented to record license plates of entering and departing traffic. If remote-controlled entry is planned, in which a security or other service person operates the gate or barrier, the TV is essential for safety. If TV cameras are to be used at entries or exits consider the camera orientation in relation to the sun at various times of day and artificial illumination at or near the camera. Older vidicon cameras are adversely affected by strong artificial light or direct sunlight falling on the tube face—modern CCD cameras less so. Arranging the camera so that it does not receive direct incident light avoids this problem in either case. With remote pan-tilt controls, the operator must remain aware in maneuvering a tube-type camera not to expose the picture tube to such light. CCD cameras are not susceptible to this problem but can encounter what is known as transfer smear. This occurs when the focus moves from a brightly lit to a low or unlit object, as could happen while panning. Transfer smear obscures a usable image until it subsides. Selected interior monitoring will enhance the personal safety and protection capability of the facility operator. Remote pan-tilt cameras, used in conjunction with entry and exit, may also serve a general monitoring function. Other cameras could provide surveillance of ramps, turns, and parking stall areas. The objective is not to monitor every location in the facility. The monitoring should capture all inbound and outbound vehicular movements and, in addition, as much aisle and interlevel activity as possible. A camera installed on any particular level other than entrance or exit levels should be able to track vehicles moving to or from that level via aisles and turning aprons. By ensuring longitudinal aisle views, both vehicles and pedestrians will be seen as they enter and leave individual parking stalls. In enclosed parking structures, the relatively low ceiling heights and the density of the parked vehicles pretty much preclude any useful extensive monitoring into or across the parking stalls. The key to successful use of CCTV is in the monitoring. Adequate monitoring and timely response by personnel are needed to ensure corrective action when off-normal situations are picked up on the cameras. References include ISC (2004) and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
12	3	Automated access control requires two inputs to verify identification (ID) (i.e., proximity card and personal identification number (PIN)).	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs and WMDs. Automated access control systems are a means of preventing aggressors from gaining access to the facility through entrances. Electronic access control has supplanted conventional keys for access control in applications that involve large numbers of people, demand real-time records of entry, or require instant access denial capability. Electronic access control systems use readers for • Magnetic coding, • Proximity/contact, • Resonant circuits, • Radio frequency, • Biometric technology, • Optical character, and • Smart card technology. The optimum value of these systems will be ensured only if all the following are observed: • The coding system is not easily decoded and duplicated. For example, on magnetic strip cards the magnetic coding is susceptible to transfer to another magnetic strip and later decoding or duplication. Low-coercivity cards (the typical credit and debit cards) are particularly vulnerable. • The system can be modified from a remote location, quickly and at any time, even during heavy system use, to delete (or add) a user. • All the access level features are used. For systems that permit portal control by individual name, day of the week (or year), and clock hours (or shift), such features should be incorporated into the selection of the appropriate access level for each user. And these parameters should be updated immediately when that user's status changes. • Each protected portal in very secure applications requires not only that the correct card be used but that a remembered value (PIN) be keyed in as well. Alternatively, biometric readers may be used. These require more elaborate readers at higher unit cost, but for truly secure applications, they will ensure that a lost or purloined card cannot be used before its loss has been discovered and reported. References include FEMA 426 (Table 1-22 and Section 12.20) and ASIS (2012).
12	4	Screening equipment, such as metal detectors, explosive detection equipment, or canines, is used at public entrances to supplement visual inspections.	Screening visitors to the facility for weapons and explosives is important. At increased levels of risk, staff should also be screened. This reduces the vulnerability to actions that accompany violent terrorist or criminal activity and acts related to domestic disputes. Without screening, facilities might be vulnerable to such threats as assault, assault with a deadly weapon, and hand-delivered bombs or weapons of mass destruction (WMDs). Equipment that can be used in the screening process, in addition to visual inspection and baggage search, includes walk-through and handheld metal detectors, X-ray inspection machines, explosives detectors, and, if the level of threat warrants, radiation detectors and chemical or biological agent detectors. If the nature of the threat warrants, canines can be brought in to assist the inspectors. Most metropolitan police departments have canine units that include explosives detection animals. BATFE, the U.S. Customs Service, and various military departments of the federal government also have explosives detection dogs. Airport law enforcement agencies in major gateway cities also use them. It is advisable to identify which nearby local or federal agencies have such animals and whether, in an emergency, they would be available for use in the private sector. References include ASIS (2012).

Discipline	Count	Countermeasure	Guidance
12	5	Screening of packages and deliveries (for weapons, explosives, and CBR material) is performed at loading docks and shipping/receiving areas.	Screening packages and deliveries entering the facility via commercial transport or package delivery services for weapons and explosives is important. This reduces the vulnerability to actions that accompany violent terrorist or criminal activity. Without screening, facilities might be vulnerable to assault with a deadly weapon, assassination, mail or package bomb, or CBR agent release. Equipment that can be used in the screening process includes metal detectors, X-ray inspection machines, explosives detectors, and, if the level of threat warrants, radiation detectors and chemical or biological agent detectors. In the event explosives are found, explosive disposal containers may be needed. If the nature of the threat warrants, canines can be brought in to assist the inspectors. Most metropolitan police departments have canine units that include explosives detection animals. BATFE, the U.S. Customs Service, and various military departments of the federal government also have explosives detection dogs. Airport law enforcement agencies in major gateway cities also use them. It is advisable to identify which nearby local or federal agencies have such animals and whether, in an emergency, they would be available for use in the private sector. Written procedures should be available to loading dock or shipping/receiving personnel to explain the required actions in the event weapons, explosives, or CBR materials are discovered. References include FEMA 426 (Table 1-22 and Section 12.26).
12	6	Backup motion detection sensors are located at all entrances/exits and accessible windows.	If intrusion-detection equipment at doors and accessible windows should fail, having a backup sensor is necessary. The following motion-sensing intrusion-detection devices would be applicable for indoor use. Passive infrared sensors, commonly referred to simply as PIRs, are the most widely used intrusion detectors today and are highly versatile. PIRs “see” the invisible, bold colors of thermal or infrared (IR) energy. Because there is no beam, they are called passive. This energy, like heat from the sun, has no visible color or light. Just as a camera takes in light, a PIR sees warm, infrared images against a cooler background. The operation of ultrasonic sensors is much like that of more technologically advanced and popular passive infrared detectors. Based on the Doppler effect, microwaves or sound waves are disturbed when movement changes signal frequency between transmission and receipt. As long as the return pattern being received is the same as that being transmitted, a stable condition exists. When a distortion of the wave pattern caused by movement is detected, an alarm is initiated. The microwave sensor operates on generally the same principle as the ultrasonic sensor. The difference lies in the type of wave or signal used. The ultrasonic sensor uses a high-frequency sound wave, whereas the microwave sensor utilizes much higher frequency electromagnetic energy. The microwave transmitter sends a signal that is reflected back to an antenna. A comparison circuit compares the transmitted and reflected signals. If there is no movement in the area, the waveform remains constant. When the signal is reflected from a moving object, the waveform changes, initiating an alarm. Microwave sensors may be utilized in outdoor and indoor applications, because they are not generally affected by heavy fog, rain, snow, sleet, air turbulence, drafts, noise, temperature extremes, or atmospheric disturbances. References include FEMA 426 (Table 1-22 and Section 12.10), U.S. General Services Administration (2005), ISC (2004), and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
12	7	Delayed egress hardware is provided at egress doors, if permitted by governing code authorities.	The installation of exit devices requires a balance between life safety and physical security. An exit device, also known as a panic bar or crash bar, is commonly used on doors in the path of egress. Exit devices can be electrified to permit remotely controlled reentry via a push button or card reader/keypad. A special application of this type of hardware is the delayed egress locking system. This system was developed as a compromise between safety and security; it is usually applied to doors intended to be used only for emergency fire egress. Rather than allowing immediate egress when pushed, the bar starts a 15- or 30-second delay after which the door unlocks. The system will sound a local alarm and report that alarm condition to a central monitoring location. A CCTV camera mounted near the exit can be used to identify the intruder and any articles being carried and to record the incident. Special signage can be used to inform users of the delay. Life safety is maintained by connecting the system to the fire alarm system and preventing the delay occurring in the event of a fire or other life safety emergency. The delayed egress system is controversial; a special code variance may be required, and some communities have banned them completely. References include FEMA 426 (Table 1-22 and Section 12.29).
12	8	Escort procedures have been implemented for visitors within staff areas.	High-risk facilities are at greater risk for attacks by criminals, terrorists, or militants if these elements can approach and enter with ease. Threats include assault, assault with a deadly weapon, assassination, kidnapping and hostage taking, robbery, and hand-delivered bombs. Access control procedures should include a provision for escorting visitors, vendors, and service personnel while they are in staff areas of the facility. Escort procedures should include contacting the facility staff member who will be responsible for the visitor. Escort can be provided by security personnel or facility staff. Entrance procedures should include a register or log with the particulars of the visitor and the name of the escort. References include ISC (2004).
12	9	Guards and employees receive emergency training in the proper reporting and response to fires and other emergencies and in the use of portable and built-in protection systems, including training in system maintenance.	Especially during nonbusiness hours, the guard force may be the first line of defense against aggressor attack involving bombs and incendiaries. The guard force must receive training to handle emergency situations generated by attack or accident. In addition to training in regulations of the guard force, requirements of particular assignments (post orders), and rules of the enterprise, training should include: • Emergency communication and reporting procedures; • Layout of facilities and offices; • Facility security procedures; • Safety and fire regulations; • Firefighting procedures; • Vulnerable points such as sensitive areas, transformer stations, and primary switchgear, oil and gas supply points, and areas containing hazardous materials; • Locations of all departments and key personnel; • Locations of all telephones, fire alarm stations, and fire and emergency exits; • Locations of all stairways and doors; • Storage locations of stocks of materials; • Location of all firefighting equipment and system maintenance requirements; • Locations of light switches; • Locations of elevator control switches; • Locations of heating, air conditioning, and ventilating controls; • Locations of all sprinkler system valves; • Locations of control devices for machinery and operations within the facility; and • Shutdown procedures for equipment.

Discipline	Count	Countermeasure	Guidance
			An initial period of general security instruction should be given as soon as the officer reports for duty. Special instruction for specific duties is given as the duties are assigned. Follow-up instruction—an essential—may range from classroom courses in complex topics to a brief discourse at lineup time when the officers report for duty each day. Training may be accomplished in a variety of venues using a number of training tools. They include • Classroom courses, • Videotapes or discs, • Interactive computer-based programs, • Home study, • On-the-job training, • Written instructions, • Guard manuals and post orders, and • Lineup time. References include FEMA 426 (Table 1-22 and Section 5.6), FEMA 386-7 (2002), ISC (2004), and ASIS (2012).
12	10	The security plan addresses standardized security system construction specification documents.	Before a facility can be protected, the professional security practitioner should apply a logical process in evaluating the risk and applying countermeasures. The process requires the development of a plan that starts with an analysis of the needs for security and ends with the implementation of effective and applicable solutions. The risk assessment (see Silver Countermeasure Discipline 4 Countermeasure 4) will determine the threats, vulnerability, and impact for the particular facility. After all of the assessments have been completed, security objectives have been developed, and the role of physical security in achieving those objectives has been identified, the final step is to develop countermeasures. Countermeasures should conform to acceptable security industry standards and codes. After required equipment to implement countermeasures and its likely configuration have been determined, a technical specification should be prepared. Such specifications can be either of the “prescriptive” or “performance” type. The former identifies specifically with the actual equipment required while the latter describes the function or performance demanded. Performance specifications give suppliers latitude to propose items that may not have been considered by the specifying organization, but that will accomplish the required function. They generally encourage innovative approaches. The specification will be included in a request for proposal (RFP) or invitation to bid (ITB), which will also include instructions to bidders on how to make submittals; the requirements for stating equipment, installation, and unit costs; and the criteria used to award the contract. Site familiarization and inspection tours of the facility may be organized for the bidders if the project is large or complex enough. Once the planning phase has been completed and reviewed and the design concepts and budgetary cost estimates approved, the project moves into the design and documentation phase. In the construction design industry this may be split into two separate phases, typically referred to as the design development and construction documents. Alternatively, it may be considered as a single phase called construction documents, or CD, with the completion of the design development work being referred to as 30% or 35% CD. The security plan should contain all standardized security system construction specification documents developed from the planning phase. The word “system” in the security context can be defined as a combination of equipment, personnel, and procedures design, coordinated in such a way as to ensure optimum achievement of the system’s stated security objectives. References include FEMA 426 (Table 1-22 and Section 12.43) and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
13—Security master plan			
13	1	The security plan includes security implementation schedules established to address recommended security solutions.	Before a facility can be protected, the professional security practitioner should apply a logical process in evaluating the risk and applying countermeasures. The process requires the development of a plan that starts with an analysis of the needs for security and ends with the implementation of effective and applicable solutions. The risk assessment (see Silver Countermeasure Discipline 4 Countermeasure 4) will determine the threats, vulnerability, and impact for the particular facility. After all assessments have been completed, security objectives have been developed, and the role of physical security in achieving those objectives has been identified, the final step is to develop countermeasures. Countermeasures should conform to acceptable security industry standards and codes. Implementation schedules should be developed for all phases involved in design, procurement, construction, installation, testing, and acceptance of systems and equipment required to implement the recommended security solutions. References include FEMA 426 (Table 1-22 and Section 13.7) and ASIS (2012).
13	2	The security plan addresses security operating and capital budgets.	A budget is usually prepared in two major sections, one dealing with capital costs, the other with operational costs. Capital costs are incurred in the acquisition of assets that • Will be used in the ongoing business of the organization; • Will have useful lives generally longer than one year; and • Exceed some minimum acquisition cost, which varies among organizations as a matter of policy. Operations costs, however, do not result in the acquisition of a lasting or permanent asset. They are typically generated for services or for physical items with a useful life of less than one year, or that will be consumed in the activity of the business (office supplies, fuel, etc.). Salaries and wages and the costs of services procured from contractors or nonemployees are treated as operational cost items. Budgets must be approved and supported by management of the organization. References include FEMA 426 (Table 1-22 and Section 13.8).
13	3	Regulatory or industry guidelines or standards were followed in the preparation of the security plan.	Before a facility can be protected, the professional security practitioner should apply a logical process in evaluating the risk and applying countermeasures. The process requires the development of a plan that starts with an analysis of the needs for security and ends with the implementation of effective and applicable solutions. The risk assessment (see Silver Countermeasure Discipline 4 Countermeasure 4) will determine the threats, vulnerability, and impact for the particular facility. After all assessments have been completed, security objectives have been developed, and the role of physical security in achieving those objectives has been identified, the final step is to develop countermeasures. Countermeasures should conform to requirements and guidance including, but not limited to, • National, state, and local building (construction) codes and standards; • Equipment and material standards; • Federal regulations and guidelines; and • Security industry guidelines and standards. References include FEMA 426 (Table 1-22 and Section 13.9) and ASIS (2012).

Discipline	Count	Countermeasure	Guidance
13	4	The security plan addresses the following major components: access control, surveillance, response, building hardening, and protection against CBR and cyber-network attacks.	To implement the physical security concepts of deter, detect and annunciate, delay, deny access, and apprehend, the security plan must address the necessary components, including • Providing visual and electronic surveillance to discourage intruders; • Using visual and electronic means (e.g., CCTV, guard patrol, and intrusion detectors) to detect attempts to illegally gain access; • Delaying an intruder with forced-entry-resistant doors, windows, walls, floor, and roof; • Denying access with protection in depth (layered concept) with barriers and access control systems; and • Providing a response to unauthorized access with guard force or local law enforcement to apprehend the intruder. In addition to controlling access, a physical security program is designed to prevent the interruption of operations. Interruptions can occur as a result of natural catastrophes like hurricanes and floods; environmental disasters like nuclear meltdown or toxic pollutant release; industrial accidents like fires or explosions; and intentional acts such as vandalism, malicious mischief, bombing, arson, and release of CBR agents. Cyber-network attacks can also adversely affect operations. Such measures as building hardening, emergency and disaster management plans, and cyber security can address these issues. The personal safety of employees is an aspect of the overall security program—this requires ensuring that employees are reasonably free from preventable security risks to life or person. These risks are beyond the normal risks of accidental injury in any workplace and are typically a concern of the safety program. Protection against extraordinary risks is achieved through key employee security measures and by minimizing the opportunity for theft of property or personal assault while at work. The physical security program embraces these objectives and that of protecting the employer's property interests by • Allocating protected employee entrances, exits, and parking lots; • Providing safeguards for employee property left in lockers; • Ensuring that nonemployees who gain entry to the facility are authorized to be there and are nonthreatening to the workforce; and • Providing assistance to employees involved in dangerous workplace situations. References include FEMA 426 (Table 1-22 and Section 13.12) and ASIS (2012).
13	5	The security plan addresses qualifications for security consultants, system designers and engineers, installation vendors, and contractors.	Before a facility can be protected, the professional security practitioner should apply a logical process in evaluating the risk and applying countermeasures. The process requires the development of a plan that starts with analysis of the needs for security and ends with implementation of effective and applicable solutions. The security plan should contain qualifications for all persons involved in the planning, design, procurement, construction, installation, testing, and acceptance of systems and equipment required to implement protective countermeasures. The word "system" in the security context can be defined as a combination of equipment, personnel, and procedures design, coordinated in such a way as to ensure optimum achievement of the system's stated security objectives. References include FEMA 426 (Table 1-22 and Section 12.45) and ASIS (2012).

APPENDIX H

Countermeasure Commentary for Level 5, Platinum

Discipline	Count	Countermeasure	Guidance
1—Site			
1	1	Facilities with similar threat levels have been clustered (if on campus).	Depending on the site characteristics, the occupancy requirements, and other factors, buildings on a campus may be clustered tightly in one area or dispersed across the site. Grouping high-risk activities, concentrations of personnel, and critical functions into a cluster can help maximize standoff from the perimeter and create “defensible space.” This also helps to reduce the number of access and surveillance points and minimize the size of the perimeter needed to protect the facilities. However, the practical benefits of clustering facilities must be balanced with the survivability benefits of resource dispersal in the event of an attack. To the extent that site, economics, and other factors allow, buildings that are functionally compatible and have similar threat levels should be consolidated (clustered) on campus. For example, visitor screening areas, receiving/loading areas, and mailrooms constitute the innermost line of defense because they may be the first places where people and materials are closely inspected before being introduced into the facility. Logically, they should be physically separated from the key assets such as main operational areas and concentrations of people. Locating potential target buildings away from lower risk areas is desirable to minimize collateral damage should an attack occur. References include USAF (1997).
1	2	Culverts, sewers, storm drains, concrete trenches, duct systems, and pipelines (that enter or go under the facility) have intrusion detection to detect unauthorized access.	Unprotected utility tunnels, pipelines, manholes, stormwater runoff culverts, sewers, and concrete trenches can provide covert access and weapon concealment opportunities. This increases the facility’s vulnerability to terrorist or criminal attack. Access to a building might be obtained through floor openings such as openings for shafts and ducts; utility tunnels or chases for heat, gas, water, electric power, and telephone; sewers and other types of drains; and other small service openings. Intrusion-detection devices should be used to protect against unauthorized access via these routes. Intrusion-detection devices (sensors) are the basic ingredients of an alarm system. They detect the condition or event indicating a security problem. All logical discrimination, transmission, processing, display, and recording activities that occur subsequent to initial detection have meaning because of what sensors see, hear, feel, or otherwise sense with optical, electronic, electromechanical, or mechanical capabilities.

Discipline	Count	Countermeasure	Guidance
			The types of intrusion devices appropriate for outdoor use are classed as “point of entry” sensors and include • Passive infrared sensors (PIRs), • Microwave sensors, • Photoelectric sensors, • Balanced pressure sensors, and • Closed-circuit television. Refer to FEMA 426 (2003a) for a description of these sensors. References include FEMA 426 (Table 1-22 and Section 1.9) and USAF (1997).
1	3	Access to site is controlled by performing identification (ID) check and/or screening pedestrians entering the site.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs and weapons of mass destruction (WMDs). Vehicle and pedestrian access control and inspection should occur as far from facilities as possible (preferably at the site perimeter) with the ability to regulate the flow of people one at a time. Refer to paragraph 4.1 of this document for a discussion of access control ID systems. References include FEMA 426 (Table 1-22 and Section 2.7).
2—Architectural			
2	1	Screening of mail, packages, and deliveries (for weapons, explosives, and chemical, biological, and radiological (CBR) material) is performed off site.	Mailrooms and mail-handling areas are vulnerable to the threat of a mail or package bomb sent by criminals, terrorists, or militants. Explosives in packages delivered through the mail can cause significant localized damage, injuries, and fatalities if they detonate inside a building. Off-site screening stations or a separate on-site delivery-processing building may be cost-effective, particularly if several buildings share one mailroom. A separate delivery-processing building reduces risk and simplifies protection measures. Equipment that can be used in the screening process includes metal detectors, X-ray inspection machines, explosives detectors, and, if the level of threat warrants, radiation detectors and chemical or biological agent detectors. In the event that explosives are found, explosive disposal containers may be needed. If the nature of the threat warrants, canines can be brought in to assist the inspectors. Most metropolitan police departments have canine units that include explosives detection animals. BATFE, the U.S. Customs Service, and various military departments of the federal government also have explosives detection dogs. Airport law enforcement agencies in major gateway cities also use them. It is advisable to identify which nearby local or federal agencies have such animals and whether, in an emergency, they would be available for use in the private sector. Written procedures should be available to off-site screening personnel to explain the required actions in the event that weapons, explosives, or CBR materials are discovered. References include FEMA 426 (Table 1-22 and Section 12.31).

Discipline	Count	Countermeasure	Guidance
3—Structural			
3	1	Adjacent buildings are spaced far enough away to prevent severe collateral damage.	Buildings that are functionally compatible and have similar threat levels should be consolidated on campus, although the practical benefits of clustering facilities must be balanced with the survivability benefits of resource dispersal in the event of an attack. Clustered buildings should not be so close as to risk severe collateral damage from an attack on an adjacent building. A risk assessment and blast analysis can assist in determining building locations. References include USAF (1997).
3	2	Additional standoff distances for the facility have been created (based on risk and blast assessments) by eliminating street parking and/or closing streets.	In the United States, there is a trend in which terrorists are making fewer attacks but the individual attacks are becoming more deadly. The spectacular media coverage of demolished buildings, the dead and injured, and interviews with survivors brings the horror of a bombing directly into people's homes. Bombs are a primary weapon of international terrorism and are the principle concern of government agencies and major corporations. Bombs are also used by criminal extortionists, employees, and others with real or imagined grievances. Terrorist groups that use bombs frequently seek international media coverage. Widespread coverage is more likely if the bombs are actually detonated rather than threatened. The hallmark of the terrorist bomb is not the threat in advance but the attribution or claim of responsibility after its detonation, which is usually accompanied by property damage, personal injuries, and deaths. Blast loads decrease rapidly with distance from the explosion. Therefore, setback is one of the first considerations when designing for blast loads. The setback distance is the range between the explosive threat location and the nearest structural element requiring protection. The term "standoff" is synonymous with "setback," and the two terms may be used interchangeably. The term "standoff" is often used when discussing the distance between a facility and the threat location. Each foot of setback can be of critical importance in reducing or limiting damage, injury, and death. If a vehicle can be driven through the facility's perimeter or into the building itself, this will nullify the setback. Vehicle bombs are especially dangerous because of the size of the explosive load that can be carried. Parking is often permitted in curb lanes, with a sidewalk between the lane and the building. Where distance from the building to the nearest curb provides insufficient setback and compensating design measures do not sufficiently protect the building from the assessed threat, adjacent street parking should be eliminated or the street should be closed off. References include FEMA 426 (Table 1-22 and Section 1.11), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
3	3	Utility rooms, utility mains, and service entrances within 50 ft (15.25 m) of loading docks and shipping/receiving areas are hardened for blast.	Utility systems and other critical assets can suffer significant damage when subjected to the shock of an explosion. Some of these utilities and critical components may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generators including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Distribution systems; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • Uninterrupted power supply (UPS) systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Mechanical rooms containing heating, ventilating, and air conditioning (HVAC) equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Water treatment plants and storage; and • Computer/IT rooms and equipment. Evacuation and rescue require emergency systems to remain operational during a disaster, and they should be located away from potential attack locations. Primary and backup systems should be separated to reduce the risk of both being affected by a single incident if colocated. Utility systems should be located at least 50 ft (15.24 m) from loading docks, front entrances, and parking areas. Loading docks and shipping/receiving areas are among the most susceptible to the delivery of explosive materials. Maintaining a distance of at least 50 ft (15.24 m) between these areas and utilities, critical components, and important assets will reduce their vulnerability to bomb attack. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. A distance of 50 ft (15.24 m) is the generally accepted margin for the highest level of protection found in the source criteria and guidance documents. However, 50 ft (15.24 m) may not be available or required for all facilities. The reviewer must determine if an adequate separation exists. References include FEMA 426 (Table 1-22 and Sections 2.15, 8.3), DoD (2002), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
3	4	Building is structurally independent from any adjacent buildings.	A building may be at risk for collateral damage if it is not structurally independent from adjacent buildings that might be the target of terrorist or militant attack. A building should be structurally independent from adjacent buildings and any additions to the existing building. This will minimize the possibility that collapse of an adjacent building or addition will affect the stability of the building. References include DoD (2002).
3	5	Architectural or structural features that provide a minimum standoff of 150 mm (6 in.) from exposed primary load-bearing members have been implemented.	A terrorist bomb placed against an exposed primary load-bearing member could cause localized failure and possibly progressive collapse. Implement architectural or structural features such as embedment or encasement that deny contact with exposed primary vertical load members in these areas. A minimum standoff of at least 150 mm (6 in.) from these members is required. Avoid having exposed structural elements such as columns on the exterior of the facility. References include FEMA 426 (Table 1-22 and Section 3.6), U.S. General Services Administration (2005), and ISC (2004).
3	6	Mailrooms and unscreened retail spaces are designed to mitigate the effects of a blast on primary vertical or lateral bracing members.	Mailrooms and mail-handling areas are vulnerable to the threat of a mail or package bomb sent by criminals, terrorists, or militants. Unscreened retail spaces could be the target of a hand-carried explosive device. Explosives, if delivered through the mail or carried into an unscreened retail space, can cause significant localized damage, injuries, and fatalities if they detonate inside the building. If the blast weakens primary vertical or lateral bracing members, the damage could be intensified, affecting adjacent or overhead areas. Mailrooms and mail-handling areas, where packages are received and opened for inspection, and unscreened retail spaces must be designed to mitigate the effects of a blast on primary vertical or lateral bracing members. The following should be considered: • Redundancy: The use of redundant lateral and vertical force-resisting systems. Redundancy tends to promote a more robust structure and helps to ensure that alternate load paths are available in the case of a structural element(s) failure. Additionally, redundancy provides multiple occasions for yielding to occur, which increases the probability that damage will be constrained. • Ductile structural elements and detailing: It is critical that both the primary and secondary structural elements be capable of deforming well beyond the elastic limit without experiencing structural collapse. Ductile construction materials, (i.e., steel, cast-in-place reinforced concrete, etc.) should be used. • Capacity for resisting load reversals: Both the primary and secondary structural elements should resist load reversals in case of a structural element(s) failure. • Capacity for resisting shear failure: Primary structural elements should maintain sufficient strength and ductility under an abnormal loading event to preclude a shear failure. If the shear capacity is reached before the flexural capacity, the sudden, nonductile failure of the element could potentially lead to a progressive collapse of the structure. References include ISC (2004).

Discipline	Count	Countermeasure	Guidance
3	7	Mailroom design contains provision for interior pressure relief or is hardened sufficiently to protect adjacent occupied space.	Mailrooms and mail-handling areas are vulnerable to the threat of a mail or package bomb sent by criminals, terrorists, or militants. Explosives in packages delivered through the mail can cause significant localized damage, injuries, and fatalities if they detonate inside a building. The following measures address the location of rooms to which mail is delivered or in which mail is handled. The measures involve limiting collateral damage and injuries and facilitating future upgrades to enhance protection should they become necessary. The mailroom should be located on the perimeter of the building away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets. The mailroom should have an outside wall or window designed for pressure relief so that explosive forces and gases from the interior spaces are vented to the outside of the structure. Methods include the use of blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside. However, if these rooms are located in occupied areas (or adjacent to critical utilities), walls, ceilings, and floors should be blast and fragment resistant. Consider wire mesh in plaster to reduce the incidence of flying fragments. Avoid the use of masonry when blast is a threat. Masonry walls break up readily and become secondary fragments during blasts. The use of multiple barrier materials and construction techniques can sometimes accomplish the same goal with less expense than a single material or technique. Significant structural damage to the walls, ceilings, and floors of the mailroom is acceptable. However, the areas adjacent to the mailroom should not experience severe damage or collapse. References include FEMA 426 (Table 1-22 and Section 3.11), U.S. General Services Administration (2005), and ISC (2004).
3	8	Queuing area is enclosed in blast-resistant construction within the building footprint.	If there is sufficient space inside the entrance, queuing will occur within the building footprint. There could be large numbers of people at certain times such as the start of business, lunchtime, and close of business. A terrorist vehicle bomb detonated outside the entrance could result in significant casualties. The queuing area should be enclosed in blast-resistant construction. Material for windows and glazed doors should be selected to provide protection against glass fragments entering the queuing area, or they can be retrofitted with fragment retention film and catching devices. References include U.S. General Services Administration (2005) and ISC (2004).

Discipline	Count	Countermeasure	Guidance
3	9	Structural members and all mechanical system mountings and attachments will resist blast overpressures from infilling through nonwindow openings.	If a bomb detonates outside the building, nonwindow openings, such as mechanical vents and exposed plenums, can subject the structure to potential infilling of blast overpressures. Methods are available for predicting infill pressures through such openings given the area of the opening and the volume of the interior space affected. Designs should account for potential infilling of blast overpressures through such openings. The design of structural members and all mechanical system mountings and attachments should resist these interior fill pressures. All overhead utilities and other fixtures weighing 14 kg (31 lb) or more should be mounted to minimize the likelihood that they will fall and injure building occupants. Equipment mountings should be designed to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This does not preclude the need to design equipment mountings for forces required by other criteria, such as seismic standards. Mechanical vents and exposed plenums are generally located in unoccupied areas of the facility. However, potentially hazardous debris is possible and should be considered in the design of these systems in occupied areas. References include ISC (2004) and DoD (2002). 4—Building envelope
4	1	Lobby doors and partitions are ballistic resistant.	Where screening and access control are performed, an adversary may bring a weapon into the prescreening area, possibly resulting in a ballistic attack against building occupants. To mitigate this threat, make doors and walls along the line of security screening ballistic resistant per UL 752 (2000). For a moderate level of protection, UL Rating Level 3 should be used. For a higher level of protection, UL Rating Level 8 should be used. These UL rating levels are consistent with the guidance of ISC (2004). References include U.S. General Services Administration (2005).
4	2	Ballistic windows are used in the building for high-risk areas.	An adversary may bring a weapon into the building's public areas possibly resulting in a ballistic attack against building occupants in high-risk areas with interior windows. To mitigate this threat, make windows between public and high-risk areas ballistic resistant per the requirements of UL 752 (2000) (level to be determined by the threat level identified in the risk assessment). Glass-clad polycarbonate and laminated polycarbonate are two types of acceptable glazing material. Special consideration should be given to frames, anchorages, and substrates for ballistic-resistant windows because their inherent resistance to attack may impart large reaction loads to the supporting walls.

Discipline	Count	Countermeasure	Guidance
			Fire safety is an important consideration in blast-resistant window design. A fire protection engineer should evaluate the performance requirements for all security glazing materials proposed for a facility. Normal tools carried by firefighters, such as a pick head axe, halligan tool, or similar device, may not readily overcome ordinary glazing barriers. If the use of more specialized tools, such as a rabbit tool, a k-tool, circular saws, rams, or similar devices is necessary to break through the glazing barrier or if the glazing itself is hardened so that high pressures may not blow out the windows, alternative methods or systems to ensure that smoke from an incident is not trapped inside the building must be implemented. To complement ballistic-glazed windows, make doors, ceilings, floors, and walls between public and high-risk areas ballistic resistant per UL 752. For a moderate level of protection, UL Rating Level 3 should be used. For a higher level of protection, UL Rating Level 8 should be used. These UL rating levels are consistent with the guidance of ISC (2004). References include FEMA 426 (Table 1-22 and Section 4.4) and U.S. General Services Administration (2005).
4	3	Ballistic glazing meets the requirements of UL 752 (2000).	An adversary may bring a weapon into the building's public areas possibly resulting in a ballistic attack against building occupants in high-risk areas with interior windows. To mitigate this threat, make windows between public and high-risk areas ballistic resistant per the requirements of UL 752 (level to be determined by the threat level identified in the risk assessment). Glass-clad polycarbonate and laminated polycarbonate are two types of acceptable glazing material. Special consideration should be given to frames, anchorages, and substrates for ballistic-resistant windows because their inherent resistance to attack may impart large reaction loads to the supporting walls. Fire safety is an important consideration in blast- and ballistic-resistant window design. A fire protection engineer should evaluate the performance requirements for all security glazing materials proposed for the project. Normal tools carried by firefighters, such as a pick head axe, halligan tool, or similar device, can readily overcome glazing barriers. More specialized tools, such as a rabbit tool, a k-tool, circular saws, rams, or similar devices may be necessary to break through the glazing barrier if it is blast or ballistic resistant. References include FEMA 426 (Table 1-22 and Section 4.4), U.S. General Services Administration (2005), and ISC (2004).
4	4	Methods such as blow-out panels and window system designs that provide protection from blast pressure applied to the outside but that readily fail and vent if exposed to blast pressure on the inside are used to facilitate the venting of explosive forces and gases from interior spaces, including lobby, mailroom, and loading dock, to the outside of the structure.	Mailrooms, loading docks, and lobbies are vulnerable to the threat of a mail, package, or hand-delivered bomb by criminals, terrorists, or militants. Explosives in these areas can cause significant localized damage, injuries, and fatalities if they detonate. These areas should be designed for pressure relief so that explosive forces and gases from the interior spaces are vented to the outside of the structure. Methods include the use of blow-out panels and window system designs that provide protection from blast pressure applied to the outside but that readily fail and vent if exposed to blast pressure on the inside. If the area below a loading dock is occupied or contains critical utilities, the floor of the loading dock should be blast resistant. References include FEMA 426 (Table 1-22 and Section 3.10), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
5—Utilities			
5	1	Building airtightness is enhanced to prevent exterior CBR contamination.	Terrorists may release a CBR agent outside a building or may direct a large-scale attack in the area. Significant quantities of air can enter a building by means of infiltration through unintentional leakage paths in the building envelope. Such leakage is of more concern for an exterior CBR release at some distance from a building, such as a large-scale attack, than for a directed terrorist act. To limit this infiltration, the building should be “weatherized” by sealing cracks around doors and windows. Sealing these gaps can reduce the amount of flow between the building and the outside, thus improving energy efficiency and slowing the rate at which contamination enters the building from the outdoors. In large buildings subject to very cold weather, reducing the leakiness of the upper floors can greatly reduce flows caused by the stack effect; such reduction is desirable because such flows can transport contamination rapidly through the building and can contaminate stairwells that are needed for evacuation. Many large buildings have a small exterior-surface-to-volume ratio. In such buildings, weatherization is unlikely to have a large effect on reducing casualties from an outdoor chemical or biological release. However, this improvement might pay for itself in a few years through reduced energy cost and improve occupant comfort (especially in the offices on the perimeter of the building), in addition to potentially improving safety for a chemical or biological attack. References include FEMA 426 (Table 1-22 and Section 6.11), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).
5	2	Water supply has a central building water filtration and treatment system.	Terrorists or militants may attack the incoming water supply to disrupt the facility’s mission. They may either cut off the supply or attempt to contaminate it. Operational facilities require reliance on an adequate domestic water supply. The use of point-of-entry filters and a central building filtration, treatment, and storage system can overcome a short-term disruption or contamination. Water trucks could be brought in to replenish the supply to the central system. The filtration and treatment system should produce domestic water that meets or exceeds the applicable local, state, and federal standards. References include FEMA 426 (Table 1-22 and Section 5.4) and ISC (2004).
5	3	Connections for a tertiary power source are provided.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. For example, electric power systems can suffer significant damage when subjected to the shock of an explosion. Electrical power may be critical for safely evacuating people from the building. Destruction of critical electrical components could cause damage that is disproportionate to other building damage resulting from an explosion. In the event of a disruption, emergency power must be provided to essential building services, especially those required for life safety, evacuation, and shelter in place, providing lighting and surveillance to deter and detect criminal activities and providing emergency communication. Usually a backup is provided by an emergency generator or UPS. Because a terrorist attack could also disable these components, another source of power is required. A tertiary power source is intended for buildings where operational continuity is critical. Conduit and line can be installed with “quick connects” outside to allow a trailer-mounted generator to connect to the building’s electrical system; if this option is used, an operations plan for it must be in place. Other tertiary power methods include generators and feeders from alternative substations. References include FEMA 426 (Table 1-22 and Section 6.11), U.S. General Services Administration (2005), and ISC (2004).

Discipline	Count	Countermeasure	Guidance
5	4	The sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation.	Terrorist, criminal, or militant groups may use arson or bomb attacks to accomplish their goal of harming a facility and its staff. In the event of a blast or event-related fires, the fire-suppression system is an essential life safety component. The fire-suppression system must be adequate, code compliant, and protected. Standpipes, water-supply control valves, and other system components should be protected. Central shaft locations for sprinkler/standpipe interior controls (risers) are more vulnerable than multiple riser locations. To address risks associated with a single-point failure of the combination standpipe/sprinkler risers, they should have fire- and blast-resistant separation. References include FEMA 426 (Table 1-22 and Section 7.1).
6—Mechanical			
6	1	Results of analyses using air-plume models related to CBR clouds have been incorporated into the placement of intakes.	One of the most important steps in protecting a building's indoor environment is the security of the outdoor air intakes. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system. Introducing CBR agents into the outdoor air intakes allows a terrorist to use the HVAC system as a means of dispersing the agent throughout a building. Publicly accessible outdoor air intakes located at or below ground level are at most risk—due partly to their accessibility (which also makes visual or audible identification easier) and partly because most CBR agent releases near a building will be close to the ground and may remain there. Securing the outdoor air intakes is a critical line of defense in limiting an external CBR attack on a building. Some buildings have air intakes that are difficult to access (e.g., on the roof or high on the building), but many others have intakes that are easily accessible and thus vulnerable. Physically inaccessible outdoor air intakes are the preferred protection strategy. When outdoor air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective alternative. Iron fencing or similar see-through barriers that will not obscure visual detection of terrorist activities or a deposited CBR source are preferred. The restricted area can also include an open buffer zone between the public areas and the intake louvers. Thus, individuals attempting to enter these protected areas will be more conspicuous to security personnel and the public. Monitoring the buffer zone by physical security, closed-circuit television (CCTV), security lighting, or intrusion-detection sensors will enhance this protective approach. Although elevating outdoor intakes to make them inaccessible to the public is a means of providing security, effectively elevating intakes has practical limits. A plume or cloud of hazardous materials can reach intakes, particularly if the source is large and distant. For low-rise buildings (i.e., those having a width more than twice the height), a plume originating at ground level near the building will travel over the building rather than around it; thus, the wind will convey contaminants to the top of the building, with some dilution occurring. Therefore, it is important that results of analyses using air-plume models related to CBR clouds be incorporated into the placement of intakes. References include FEMA 426 (Table 1-22 and Section 6.1), CDC/NIOSH (2002), Lawrence Berkeley National Laboratory (2003), U.S. General Services Administration (2005), ISC (2004), and DoD (2002).

Discipline	Count	Countermeasure	Guidance
6	2	Low-leakage, fast-acting dampers are installed on the air intakes.	Terrorists may release a CBR agent inside or outside a building or may direct a large-scale attack in the area. Rapid response is essential following notification of a CBR release. How quickly the event can be mitigated depends on operations personnel and HVAC equipment. Response may involve closing various dampers, especially those controlling the flow of outdoor air (in the event of an exterior CBR release). When the HVAC system is turned off, the building pressure compared with outdoors may still be negative, drawing outdoor air into the building via many leakage pathways, including the HVAC system. Consideration should be given to installing low-leakage dampers to minimize this flow pathway. Damper leakage ratings are available as part of the manufacturer's specifications and range from ultra-low to normal categories. Assuming that there is some warning prior to a direct CBR release, the speed with which these dampers respond to a "close" instruction can also be important. From a protective standpoint, dampers that respond quickly are preferred to dampers that might take 30 seconds or more to respond. References include FEMA 426 (Table 1-22 and Section 6.7), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).
6	3	Space and access to air-handling unit (AHU) is provided for future installation of CBR-detection technology and large filter assemblies.	Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern are the airflow patterns and dynamics in buildings, specifically in the building heating, ventilating, and air conditioning (HVAC) systems. These systems can become an entry point and a distribution system for hazardous contaminants, particularly CBR agents. As new technologies emerge for filtration of airborne CBR agents, air-handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. It is important to ensure that there is available space and access to the AHU for emerging CBR-detection technology. References include ISC (2004).
6	4	Smoke evacuation systems are installed.	Terrorist, criminal, or militant groups may use arson or bomb attacks to accomplish their goal of harming a facility and its staff. A major concern in a fire situation is smoke, which can cause casualties through suffocation or toxic action. Smoke evacuation systems with purge capabilities should be installed. These may be stand-alone systems or integrated with the HVAC system in the facility. For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high-risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk during internal events, such as lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants. References include FEMA 426 (Table 1-22 and Section 6.16), U.S. General Services Administration (2005), ISC (2004), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).
6	5	Smoke removal equipment has stand-alone local control panels that can continue to individually function in the event that the control wiring is severed from the main control system.	Terrorist, criminal, or militant groups may use arson or bomb attacks to accomplish their goal of harming a facility and its staff. In addition to removing smoke, a smoke removal system can also be useful in removing chemical (gaseous) contamination from a deliberate or accidental release. Provide smoke removal equipment with stand-alone local control panels that can continue to individually function in the event that the control wiring is severed from the main control system. It may be appropriate to locate the panels with a fire alarm control panel. References include FEMA 426 (Table 1-22 and Section 6.16), U.S. General Services Administration (2005), ISC (2004), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
6	6	HVAC system has emergency shutoff switch to shut down air distribution except where interior pressures and airflow would prevent spread of contaminants.	Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern are the airflow patterns and dynamics in buildings, specifically in the building heating, ventilating, and air conditioning (HVAC) systems. These systems can become an entry point and a distribution system for hazardous contaminants, particularly CBR agents. The HVAC control system should be capable of immediate shutdown of air distribution throughout the building except where interior pressure and airflow control would more efficiently prevent the spread of airborne contaminants and/or ensure the safety of egress pathways. Building personnel should be trained to recognize a terrorist attack quickly and to know when to initiate HVAC shutdown. The emergency shutoff switch (or switches) should be easily accessible by building occupants. Providing such a capability allows the facility manager or building security manager to limit the distribution of airborne contaminants that may be introduced into the building. References include CDC/NIOSH (2002).
6	7	HVAC control options can regulate airflow and pressures within a building on an emergency response basis.	Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern are the airflow patterns and dynamics in buildings, specifically in the building heating, ventilating, and air conditioning (HVAC) systems. These systems can become an entry point and a distribution system for hazardous contaminants, particularly CBR agents. Many central HVAC systems have energy management and control systems that can regulate airflow and pressures within a building on an emergency response basis. Some modern fire alarm systems may also provide useful capabilities during CBR events. In some cases, the best response option (given sufficient warning) might be to shut off the building's HVAC and exhaust system(s), thus avoiding the introduction of a CBR agent from outside. In other cases, interior pressure and airflow control may prevent the spread of a CBR agent released in the building and/or ensure the safety of egress pathways. The decision to install emergency HVAC control options should be made in consultation with a qualified HVAC professional that understands the ramifications of various HVAC operating modes on building operation and safety systems. Depending upon the design and operation of the HVAC system and the nature of the CBR agent release, HVAC control may not be appropriate in all emergency situations. Lobbies, loading docks, and mailrooms might be provided with manually operated exhaust systems, activated by trained personnel to remove contaminants in the event of a known release, exhausting air to an appropriate area. In other instances, manipulation of the HVAC system could minimize the spread of an agent. If an HVAC control plan is pursued, building personnel should be trained to recognize a terrorist attack quickly and to know when to initiate the control measures. For example, emergency egress stairwells should remain pressurized (unless they are known to contain the CBR source). Other areas, such as laboratories, clean rooms, or pressure isolation rooms in hospitals, may need to remain ventilated. All procedures and training associated with the control of the HVAC system should be addressed in the building's Occupant Emergency Plan (OEP) or disaster management plan. References include FEMA 426 (Table 1-22 and Section 6.15) and CDC/NIOSH (2002).

Discipline	Count	Countermeasure	Guidance
6	8	Ducted return air systems are present.	Terrorism events have increased interest in the vulnerability of U.S. workplaces, schools, and other occupied buildings to CBR threats. Of particular concern are the airflow patterns and dynamics in buildings, specifically in the building heating, ventilating, and air conditioning (HVAC) systems. These systems can become an entry point and a distribution system for hazardous contaminants, particularly CBR agents. Ducted returns offer limited access points to introduce a CBR agent. The return vents can be placed in conspicuous locations, reducing the risk of an agent being secretly introduced into the return system. Nonducted return air systems commonly use hallways or spaces above suspended ceilings as a return air path or plenum. CRB agents introduced at any location above the suspended ceiling in a ceiling plenum return system will probably migrate back to the HVAC unit, which will, and, without highly efficient filtration for the particular agent, redistribute it to occupied areas. This issue is closely related to the isolation of lobbies and mailrooms, because shared returns are a common way for contaminants from these areas to disperse into the rest of the building. References include FEMA 426 (Table 1-22 and Section 6.12), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).
6	9	There are redundancies in the air-handling system.	Parts of the HVAC system may be disabled by bombs or incendiary attack. The HVAC system should be evaluated to determine if redundancies are sufficient to mitigate the consequences of failure of part of the HVAC system. Redundancies can include multiple, cross-connected AHUs. All electrically operated HVAC components should be provided with a backup power source. Although all HVAC components should be secure and not accessible by the public, redundancy can reduce the level and complexity of security protection measures required compared with a nonredundant situation. References include FEMA 426 (Table 1-22 and Section 6.10).
6	10	Critical areas can be served from other AHUs if a major system is disabled.	Parts of the HVAC system may be disabled by bombs or incendiary attack. The HVAC system should be evaluated to determine if there are large central air-handling units or multiple units serving separate zones. Independent units can continue to operate if damage occurs to limited areas of the building. Critical areas should be served by cross-connected units with dampers that can be positioned to provide backup air-handling capability. References include FEMA 426 (Table 1-22 and Section 6.9).
6	11	The air-handling system has purge capability.	Terrorist, criminal, or militant groups may use arson, bomb, and CBR attacks to accomplish their goal of harming a facility and its staff. A major concern in a fire situation is smoke, which can cause casualties through suffocation or toxic action. Airborne contamination from chemical or biological agents can also result in casualties. The HVAC system and smoke removal system (if separate) should be evaluated for their ability to remove smoke and/or contaminants. They should have the capability to purge areas of the building affected by fire or CBR release. Check and repair the HVAC system to ensure proper operation, including system balance, and correct operation of the building's economizer mode (if any). Dampers should be checked for proper operation and for leakage and should be replaced or repaired if necessary. In addition to making the building safer in the event of a chemical or biological attack, such repairs could significantly reduce energy costs. References include FEMA 426 (Table 1-22 and Section 6.16), U.S. General Services Administration (2005), ISC (2004), CDC/NIOSH (2002), and Lawrence Berkeley National Laboratory (2003).

Discipline	Count	Countermeasure	Guidance
6	12	Roof-mounted air-handling equipment is located at the center of the roof.	A terrorist attack may involve driving or parking an explosives-laden vehicle near the building. There may also be attempts to tamper with or disable equipment that is mounted on the building roof. HVAC equipment (e.g., self-contained HVAC units and laboratory or bathroom exhausts) may be located on a roof. Also, an emergency generator and day tank could be roof mounted. Roof-mounted equipment should be kept away from the building perimeter. This provides additional setback in the event of a vehicle bomb attack and could reduce damage from blast and fragmentation. In urban areas, if the building is close to another, access could be gained via a window, fire escape, or roof. Equipment located near the center of the roof will provide additional space and time for detection devices to detect or deter an intruder. Also, roof-mounted equipment can be enclosed with fencing on all sides if it is located in the center of the roof. References include FEMA 426 (Table 1-22 and Section 6.17) and U.S. Army (1994).
6	13	HVAC maintenance staff are trained in system operation, maintenance, and procedures for a suspected CBR agent release.	Arson, accidental fire, explosion, CBR contamination, and accidental hazardous material release are threats that could cause an emergency requiring manipulation of the HVAC system. The operation of mechanical system components during emergencies is an essential element of life safety, evacuation, refuge, and operations. Continuity of this protection can be provided by an adequate operations and maintenance (O&M) program. In the event of a blast, fire, CBR attack, or hazardous material release, the ventilation system may be essential to smoke removal, particularly in large, open spaces. Past U.S. experiences with anthrax and similar threats show CBR attack training exercises to be important. If a stairway pressurization system exists it can be used to maintain positive pressure in stairways for occupant refuge, safe evacuation, and access by firefighters. The system can minimize the entry of smoke, hazardous gases, and CBR agents into stairways. Periodic training of HVAC maintenance staff in system maintenance and operation is needed, including the procedures to be followed in the event of a suspected external and internal CBR agent release. It is essential that maintenance staff understand the differences in the best responses to indoor versus outdoor releases and practice the steps they will take in each case. Training to cover health and safety aspects for maintenance personnel and the potential health consequences to occupants of poorly performing systems is important. It is vital for the building operator to confirm that the HVAC operates as expected and to fix any problems with the system that prevent its proper operation. Documents such as current, accurate HVAC diagrams and HVAC system labeling protocols can be addressed in training sessions. These documents can be of great value in the event of a CBR release. If O&M of critical systems is done with in-house personnel, it is important that management know what needs to be done and the workforce has the necessary training to ensure systems reliability. When an in-house facility maintenance workforce does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure that critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel. References include FEMA 426 (Table 1-22 and Section 6.15), ISC (2004), and CDC/NIOSH (2002).

Discipline	Count	Countermeasure	Guidance
7—Plumbing and gas			
7	1	Interior standpipes are cross-connected on each floor.	Terrorist, criminal, or militant groups may use arson or bomb attacks to accomplish their goal of harming a facility and its staff. In the event of a blast or event-related fires, the fire-suppression system is an essential life safety component. The fire-suppression system must be adequate, code compliant, and protected. Standpipes, water supply control valves, and other system components should be secure or supervised. Central shaft locations for standpipes are more vulnerable than multiple riser locations. To address risks associated with a single-point failure of the combination standpipe/sprinkler risers, alternative solutions should be considered to reduce the probability, hazard severity, or a combination of both. Possible solutions include, but are not limited to, cross-connecting the combination standpipe/sprinkler risers at the bottom or top, providing two standpipe/sprinkler risers with connections to each riser on alternate floors, or locating the combination standpipe/sprinkler risers away from exterior walls on floors less than 20 ft (21 m) above grade. References include FEMA 426 (Table 1-22 and Section 7.1).
7	2	Water supply has point-of-use filters.	If terrorists were to introduce chemical or biological contaminants into the water supply from outside or inside the facility, it could result in mass casualties. To address concerns regarding the vulnerability of water distribution systems, EPA's National Homeland Security Research Center (NHSRC) researchers are identifying, testing, and evaluating both point-of-use (POU) and point-of-entry (POE) technologies (EPA/NHSRC 2014). These devices can be used proactively to protect a water system against contamination, and they can be used as a response measure in the event a water system has become contaminated. POU/POE treatment devices can also be used to identify contaminants that may have affected a water system. POU/POE treatment devices are designed to address one or more specific contaminants. They offer a supplemental or alternative method to the more traditional measures, such as system flushing and boil water advisories, currently used when responding to water system contamination. Both POE and POU devices serve as valuable tools that can reduce a water user's risk from acute, chronic, and subchronic exposures. Commonly used POU/POE technologies include reverse osmosis filtration, activated carbon adsorption/filtration, and ultraviolet light disinfection. The most effective POE device is one that combines a variety of available technologies. These types of devices are currently in use in highly vulnerable areas or potentially targeted locations. Emerging POU/POE technologies are using ultrafiltration, nanofiltration, and specialty adsorption media. References include ISC (2004) and EPA/NHSRC (2014).
9—Fire			
9	1	Key fire alarm system components have fire- and blast-resistant separation.	A terrorist vehicle or hand-carried bomb attack could concurrently start a fire and disable portions of the fire alarm system in the affected area. Fire alarm systems must first warn building occupants to evacuate for life safety. Then they must inform the responding agency to dispatch fire equipment and personnel. There should be fire- and blast-resistant separation of key alarm system components so that the intact portions can function as a backup to provide warning and notification of a fire. Fire alarm system components should be located away from high-risk areas such as lobbies, loading docks, and mailrooms. References include FEMA 426 (Table 1-22 and Section 9.1).

Discipline	Count	Countermeasure	Guidance
10—Communications and IT			
10	1	Uninterrupted power supply is provided for critical life safety and security systems until emergency power is activated.	Disruption of the normal electrical power supply can be caused by terrorist acts, accidents, and power outages caused by natural disasters. For example, electric power systems can suffer significant damage when subjected to the shock of an explosion. Electrical power may be critical for safely evacuating people from the building. Destruction of critical electrical components could cause damage that is disproportionate to other building damage resulting from an explosion. Such systems can include • Access control, • Alarms, • Building control centers, • Communications, • Elevators, • Emergency lighting, • Fire suppression, and • HVAC (smoke removal). Normally these services are provided with an emergency generator or a tertiary power source. An uninterrupted power supply should be provided to bridge the gap between the event and activation of the main emergency power source. References include FEMA 426 (Table 1-22 and Section 8.6), U.S. General Services Administration (2005), and ISC (2004).
11—Equipment operations and maintenance			
11	1	The building has a policy or procedure for periodic recommissioning of major mechanical, electrical, and plumbing (M/E/P) systems.	M/E/P systems must be fully operational to ensure that they function as intended to mitigate the consequences of an attack or other emergency situation. Periodic recommissioning involves testing and balancing of systems to ascertain their capability to perform as intended. It is to be conducted in addition to required periodic system testing. The following systems, if present, should be included: • Electrical distribution; • Emergency electrical supply; • Telecommunications; • Mass communications; • Water supply (fire suppression and domestic water); • Wastewater removal; • HVAC; • Smoke removal (if separate from HVAC); • Security (intrusion detection, CCTV, communications, and automated access control); and • Life safety (fire alarm and suppression and emergency lighting). References include FEMA 426 (Table 1-22 and Section 11.14).
11	2	Maintenance and service agreements exist for M/E/P systems.	Maintenance of M/E/P systems is necessary to ensure that they function as required during an attack or other emergency situation. When an in-house facility maintenance workforce does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel. Maintenance service agreements should include requirements for service company and service employee background checks and should be in place for all security systems. References include FEMA 426 (Table 1-22 and Section 13.10).

Discipline	Count	Countermeasure	Guidance
12—Security systems			
12	1	Cameras have video motion-detection capability.	Both indoor and outdoor CCTV systems can act as a deterrent to criminal or terrorist activity or to aid postincident investigations. The CCTV systems should be primarily for alarm assessment and access control automation purposes. The use of the CCTV system for general surveillance should be discouraged, with the occasional exception of automated video guard tours or monitoring certain areas of the childcare center or childcare center play yard. Video motion sensors are available on most digital video recorders used in security applications. They can be programmed to activate alarms, initiate recording, or do any other designated action when motion is detected by a security camera. Some digital video recorders can be programmed to monitor very specific fields of view for specific rates of motion to increase effectiveness and minimize extraneous detections. Video motion sensors can also greatly improve the efficiency of security personnel monitoring security cameras by alerting them when motion is detected (the efficiency of monitoring multiple screens decreases as the number of screens increases). A CCTV system with motion-detection capability and a monitoring screen improves the man–machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. All CCTV cameras should be on real-time and time-lapsed video recorders. For deterrence and to aid postincident investigations, most exterior areas, especially vehicle routes close to the facility, should be video recorded. References include FEMA 426 (Table 1-22 and Section 12.2) and ISC (2004).
12	2	Perimeter intrusion detection is provided to detect unauthorized access onto the site using one or a combination of fence sensors, buried cable, microwave sensors, etc.	Unauthorized access is a gateway threat for assault, assault with a deadly weapon, burglary, arson, kidnap/hostage incident, robbery, vandalism/sabotage, and hand-delivered bombs and WMDs. Intrusion-detection devices (sensors) are the basic ingredients of an alarm system. They detect the condition or event indicating a security problem. All logical discrimination, transmission, processing, display, and recording activities that occur subsequent to initial detection have meaning because of what sensors see, hear, feel, or otherwise sense with optical, electronic, electromechanical, or mechanical capabilities. The types of intrusion devices appropriate for outdoor use are classed as “point of entry” sensors and include • Passive infrared sensors (PIRs), • Microwave sensors, • Photoelectric sensors, • Balanced pressure sensors, and • Closed-circuit television. Refer to 2.1 for a description of these sensors. References include FEMA 426 (Table 1-22 and Section 1.7), FEMA 386-7 (2002), and Williams (2012).

Discipline	Count	Countermeasure	Guidance
12	3	Alarm-actuated CCTV monitoring and recording are installed to monitor critical internal areas of the facility.	Ensuring that only authorized staff, visitors, vendors, and service personnel enter the facility is important to minimize vulnerability to threats associated with unauthorized access such as criminal or terrorist attacks against critical facility components. While some of the high-risk, critical, and sensitive areas will be specific to the business conducted in the facility, others to be considered include, where applicable, • Emergency generators including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power; • Main refrigeration systems, if critical to building operation; • Mechanical rooms containing HVAC equipment; • Critical records storage rooms; • Hazardous material storage rooms; • Radiological material storage rooms; • Childcare centers; • Water treatment plants and storage; and • Computer/IT rooms. The efficiency of monitoring multiple screens decreases as the number of screens increases. Therefore, tying the alarm system to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. Alarm-activated CCTV coverage of assistance stations can assist the security force in assessing the situation and determining response requirements. Cameras should be on real-time and time-lapsed video recorders. For deterrence and to aid postincident investigations, assistance stations should be video recorded. The use of digital video systems should be considered by the designer. References include FEMA 426 (Table 1-22 and Section 12.28).
12	4	Alarm-actuated CCTV monitoring and recording are installed to monitor public/staff separation points within the facility.	Staff offices that are not separated from public areas are at greater risk for attacks by criminals, terrorists, or militants because these elements can approach and enter with ease. Threats include assault, assault with a deadly weapon, assassination, kidnapping and hostage taking, robbery, and hand-delivered bombs. The efficiency of monitoring multiple screens decreases as the number of screens increases. Therefore, tying the alarm system to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by airflow or small animals. Alarm-activated CCTV coverage of public/staff separation points can assist the security force in identifying a potential intruder and determining response requirements. Cameras should be on real-time and time-lapsed video recorders. For deterrence and to aid postincident investigations, assistance stations should be video recorded. The use of digital video systems should be considered by the designer. References include FEMA 426 (Table 1-22 and Section 12.2).

Discipline	Count	Countermeasure	Guidance
13—Security master plan			
13	1	Three-dimensional (3D) evacuation modeling of the facility has been performed to facilitate ingress/egress associated with response to emergency events.	Criminal, terrorist, or militant attacks such as bombing, arson, and CBR agent release can cause confusion, panic, injury, and death. This is also true for accidental emergencies such as fire, gas leaks, and natural disasters. Emergency evacuation plans, including the facility's OEP, must support evacuation of building occupants under a variety of scenarios. A 3D modeling program can aid evacuation planning. Prototype computer programs that simulate the evacuation of people from office buildings and large facilities are being developed. Determining the most effective evacuation plan for a large public facility requires analysis of multiple factors. An evacuation modeling tool provides the computing architecture to handle multiple scenarios, deal with deviations, determine optimum paths, and devise large-scale evacuation plans. Simulation software can be used to construct detailed 2D and 3D models of multistory facilities and simulate large-scale agent egress/ingress events with numerous variables such as agent speed, size, reaction times, and varied environmental events. The automated tool should take an agent-based approach to modeling the behavior of people attempting to evacuate a facility. This provides an intuitive correspondence between the simulation and the real-world situation that is being modeled. Each agent should have properties such as size and speed that allow the modeling of various physical characteristics. The simulation updates agent positions and paths at each time step during the model run. References include U.S. General Services Administration (2005).
13	2	The security plan addresses existing security conditions from administrative, operational, managerial, and technical security systems perspectives.	For a comprehensive security plan to be effective, it must address security-related responsibilities of the administrative, operational, managerial, and technical staff. Each employee position should have specific functions or responsibilities associated with general security or security-related events. The security plan must identify these functions or responsibilities and provide associated employee handbooks or instructions to support the overall security plan. In addition, the plan must define training and exercise requirements to adequately support and implement the security program. Operational manuals for technical security systems should be included in the plan. Operational security measures should also be defined, and any guard post orders should be included. References include FEMA 426 (Table 1-22 and Section 13.10).

This page intentionally left blank

REFERENCES

REFERENCES

- ABPA (American Backflow Prevention Association). (2014). *American Backflow Prevention Association*, <http://www.abpa.org/>, website last accessed 2014.
- ANSI/IESNA (Illuminating Engineering Society of North America). (2000). "Recommended practices—Roadway lighting," *ANSI/IESNA RP-8-00*, New York.
- ASCE. (2003). "Minimum design loads for buildings and other structures," *ASCE 7-02*, Reston, VA.
- ASCE. (2006). "Minimum design loads for buildings and other structures," *ASCE 7-05*, Reston VA.
- ASME. (2011). "Safety code for elevators and escalators," *Standard A17.1*, New York.
- ASTM. (1998). "Standard test method for security glazing materials and systems," *F1233-98*, West Conshohocken, PA.
- ASTM. (2014a). "Horizontal sliding door assemblies," *ASTM F842*, West Conshohocken, PA.
- ASTM. (2014b). "Swinging door assemblies," *ASTM F476*, West Conshohocken, PA.
- CDC (Centers for Disease Control and Prevention)/NIOSH (National Institute for Occupational Safety and Health). (2002). "Guidance for protecting building environments from airborne chemical, biological, or radiological attacks," *Pub 2002-139*, Atlanta.
- EPA (2014). National Homeland Security Research Center (EPA/NHSRC) website, <http://www.epa.gov/nhsrc/pubs.html>, last referenced 2014.
- Ettouney, M., Hansen, E., Hapij, A., Lawver, D., Tang, M., Tennant, D., Vaughan, D., and Xie, M. (2006). "Development of a progressive collapse analysis tool," CTTSO/TSWG, N41756-02-C-4704, Arlington, VA.
- FEMA. (2002). "Integrating human-caused hazards into mitigation planning," FEMA 386-7, Washington, DC.
- FEMA. (2003a). "Reference Manual to mitigate potential terrorist attacks against buildings," FEMA 426, Washington, DC.
- FEMA. (2003b). "Primer for design of commercial buildings to mitigate terrorist attacks," FEMA 427, Washington, DC.
- FEMA. (2005). "A how-to guide to mitigate potential terrorist attacks against buildings," FEMA 452, Washington, DC.
- FEMA. (2009). "Handbook for rapid visual screening of buildings to evaluate terrorism risks," FEMA 455, Washington, DC.
- Ferketic, J. A. (2002). "Applying spatial technology to homeland security—A white paper," James W. Sewall Company, Old Town, ME.
- Holzhauser, D. J., Ramseyer, G., Duncomb, R., Young, D., and Das, D. (2000). "Chemical/biological plume analysis knowledge source (CPAKS)," Air Force Research Laboratory, Rome, New York.
- IACP (International Association of Chiefs of Police)/PSLC (Private-Sector Liaison Committee). (2012). "A law enforcement executive's primer concerning replacement of law enforcement services by private security," Alexandria, VA.
- ICC. (2012). *International building code*, published by International Code Council, Washington, DC.
- IESNA (Illuminating Engineering Society of North America). (1998). "Recommended practices—Lighting for parking facilities," *IESNA RP-20-98*, New York.
- IESNA. (1999). "Recommended practices—Lighting for exterior environments," *IESNA RP-33-99*, New York.
- IESNA. (2014). *Handbook*. New York.
- ISC (Interagency Security Committee). (2004). "ISC security design criteria for new federal office buildings and major modernization projects," Washington, DC.
- Krauthammer, T., Marchand, K. A., Mlakar, P. F., and Conrath, E. J. (1999). *Structural design for physical security: State of the practice*, ASCE, Reston, VA.
- Lawrence Berkeley National Laboratory. (2003). *Protecting buildings from a biological or chemical attack: Actions to take before or during a release*. LBNL Pub 51959, Washington, DC.
- NFPA (National Fire Protection Association). (2000). *SFPE engineering guide to performance-based fire protection: Analysis and design of buildings*, Quincy, MA.
- NFPA. (2012). *NFPA 101, Life safety code*, Quincy, MA.
- UL (Underwriters Laboratories). (2000). "Standard for safety: Bullet-resisting equipment," *UL 752*, Northbrook, IL.
- UL. (2002). "Standard for burglary resisting glazing material," *UL 972*, Northbrook, IL.
- USAF (U.S. Air Force). (1997). *Installation force protection guide*. Air Force Center for Environmental Excellence, San Antonio, TX.
- U.S. Army. (1987). *Design guidelines for physical security of fixed land-based facilities*, MIL-HDBK 1013/1A, Port Hueneme, CA.
- U.S. Army. (1990). "Structures to resist the effects of accidental explosions," TM 5-1300/NAVFAC P-397/AFR 88-22, Washington, DC.
- U.S. Army. (1994). *Security engineering*, TM 5-853, Volumes 1, 2, 3, 4, Washington, DC.

- U.S. DHS (Department of Homeland Security). (2009). *National infrastructure protection plan*, Department of Homeland Security, Washington, DC.
- U.S. DHS. (2011a). *Integrated rapid visual screening of buildings*, Building and Infrastructure Protection Series, Washington, DC.
- U.S. DHS. (2011b). *Integrated rapid visual screening of mass transit stations*, Building and Infrastructure Protection Series, Washington, DC.
- U.S. DHS. (2011c). *Integrated rapid visual screening of tunnels*, Building and Infrastructure Protection Series, Washington, DC.
- U.S. DOC (Department of Commerce)/CIAO (Critical Infrastructure Assurance Office). (1998). Vulnerability assessment framework 1.1, Washington, DC.
- U.S. DOD (Department of Defense). (2002). "Unified facilities criteria: DoD minimum antiterrorism standards for buildings," UFC 4-010-01, Washington, DC.
- U.S. DOD. (2005). "Design of buildings to resist progressive collapse," UFC 4-023-03, Washington, DC.
- U.S. DOS (Department of State). (1997). *Physical security handbook*, 12 FAH-5, Washington, DC.
- U.S. GSA (General Services Administration). (2000). "Progressive collapse analysis and design guidelines for new federal office buildings and major modernization projects," Washington, DC.
- U.S. GSA. (2005). "Facilities standards for the public buildings service," GSA-PBS-P100, Washington, DC.
- U.S. GSA. (2007). *Protective design and security implementation guidelines*, Washington, DC.
- Williams, T. L., Ed. (2012). *Protection of assets manual*. POA Publishing, LLC, Los Angeles.
- ASTM. (1993b). "Standard guide for selecting economic methods for evaluating investments in buildings and building systems," E 1185-93, West Conshohocken, PA.
- ASTM. (1997). "Standard test methods for measuring the forced entry resistance of window assemblies, excluding glazing impact," F 588-97, West Conshohocken, PA.
- ASTM. (1998a). "Standard practice for measuring net benefits for investments in buildings," E 1074-93, West Conshohocken, PA.
- ASTM. (1998b). "Standard practice for applying analytical hierarchy process (AHP) to multiattribute decision analysis of investments related to buildings and building systems." E 1765-98 (now E 1765-02), West Conshohocken, PA.
- Atlas, R. I. (1998). "Designing for crime and terrorism, security and technology design," *Security Technology and Design Magazine*, June.
- Broder, J. F. (1999). *Risk analysis and the security survey*, 2nd edition, Butterworth-Heinemann, Stoneham, MA.
- Building Owners and Managers Association. (1996). *How to design and manage your preventive maintenance program*, Washington, DC.
- CAA (Congressional Accountability Act). (2014). Congressional Accountability Act, <http://www.compliance.gov/publications/caa-overview/>, website last accessed 2014.
- Chrest, A. P., Smith, M. S., and Bhuyan, S. (1996). *Parking structures: Planning, design, construction, maintenance, and repair*, 2nd edition, Kluwer Academic Publishers, New York.
- CIA (Central Intelligence Agency). (1998). *Chemical, biological, radiological incident handbook*, Washington, DC.
- Congressional Office of Compliance Safety and Health. (2008). *FAST FACTS—Fire door safety*, Washington, DC.
- Craighead, G. (2002). *High-rise security and fire life safety*, 2nd edition, Academic Press, Woburn, MA.
- Crowe, T. D. (2000). *Crime prevention through environmental design: Applications of architectural design and space management concepts*, 2nd edition, Butterworth-Heinemann, Boston.
- CTBUH (Council on Tall Buildings and Urban Habitat). (2001). *Task force on tall buildings: "The future,"* Chicago.
- CTBUH. (2002). *Building safety enhancement guidebook*, Chicago.
- EPA. (1991). *Building air quality: A guide for building owners and facility managers*, Washington, DC.
- FBI (Federal Bureau of Investigation). (1999). "Terrorism in the United States, 1999," Counterterrorism Division, Washington, DC.
- Fehr, S. C. (1996). "Parking under siege in D.C.: U.S. anti-terrorism plan threatens 360 spaces," *Washington Post*, July 13, A01.
- FEMA. (1988a). "Seismic considerations: Apartment buildings," Earthquake hazards reduction series 37, FEMA 152, Washington, DC.
- FEMA. (1988b). "Seismic considerations: Office buildings," Earthquake hazards reduction series 38, FEMA 153, Washington, DC.
- FEMA. (1988, 2002). *Rapid visual screening of buildings for seismic hazards: A handbook* (2nd edition), FEMA 154, Washington, DC.
- FEMA. (1996). "The Oklahoma City bombing: Improving building performance through multi-hazard mitigation," FEMA 277, Washington, DC.
- FEMA. (2001a). "Mitigation resources for success," FEMA 372, CD-ROM, Washington, DC.
- FEMA. (2001b). *State and local guide 101, guide for all-hazard emergency operations planning*, Chapter 6, Attachment G, Terrorism, Washington, DC.

ADDITIONAL READING

- ACI (American Concrete Institute). (1965). *Manual of standard practice for detailing reinforced concrete structures*, ACI-315, Detroit, MI.
- ACI. (2014). *Manual of concrete practice*, Farmington Hills, MI.
- AISC. (1969). *Specification for design, fabrication, and erection of structural steel for buildings*, New York.
- Archibald, R. W., Medby, J., Rosen, B., and Schachter, J. (2002). *Security and safety in Los Angeles high-rise buildings after 9/11*, RAND, Santa Monica, CA.
- ASCE. (1998). "Minimum design loads for buildings and other structures," *Standard 7-95*, New York.
- ASHRAE (American Society of Heating, Refrigerating, and Air-Conditioning Engineers). (1989). "Standard 62 basic," Atlanta.
- ASHRAE. (2001). "Ventilation for acceptable indoor air quality," ASHRAE Standard 62-2001, Atlanta.
- ASHRAE. (2002). "Risk management guidance for health and safety under extraordinary incidents," Winter meeting report, January 12, Atlanta.
- ASHRAE. (2003). "Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents on risk management guidance for health, safety, and environmental security under extraordinary incidents," Washington, DC.
- ASIS (American Society for Information Science). (2012). *Protection of assets manual*, ASIS International, Alexandria, VA.
- ASTM. (1993a). "Standard practice for measuring life-cycle costs of buildings and building systems," E 917-93, West Conshohocken, PA.

- FEMA. (2001c). "Understanding your risks, identifying hazards and estimating losses," FEMA 386-2, Washington, DC.
- FEMA. (2002). "World Trade Center building performance study: Data collection, preliminary observations, and recommendations," FEMA 403, Washington, DC.
- Fenelly, L. J. (1997). *Effective physical security*, 2nd edition, Butterworth-Heinemann, Stoneham, MA.
- Fleissner, D., and Heinzelmann, F. (1996). "Crime prevention through environmental design and community policing," National Institute of Justice (NIJ), Washington, DC.
- Garcia, M. L. (2001). *The design and evaluation of physical protection systems*, Butterworth-Heinemann, Stoneham, MA.
- Gonchar, J. (2002). "Building for a secure future: Government facilities underway incorporate already tough standards," *Engineering News-Record*, March 25.
- Gordon, C. L., and Brill, W. (1996). "The expanding role of crime prevention through environmental design in premises liability," National Institute of Justice (NIJ), Washington, DC.
- Greene, R. W. (2002). *Confronting catastrophe: A GIS handbook*, ESRI Press, Redlands, CA.
- Hart, S. (2002). "In the aftermath of September 11, the urban landscape appears vulnerable and random: Architects and consultants focus on risk assessment and security through design," *Architectural Record*, March.
- Interagency Advisory Committee on Security Equipment. (1989). *Terms, definitions, and symbols for security equipment and practices, FED-STD-800*, General Services Administration, Washington, DC.
- Kowalski, W. J. (2002). *Immune building systems technology*, McGraw-Hill Professional, New York.
- Lasley, J. (1998). "'Designing out' gang homicides and street assaults," National Institute of Justice (NIJ), Washington, DC.
- LaVigue, N. G. (1997). "Visibility and vigilance: Metro's situational approach to preventing subway crime," National Institute of Justice (NIJ), Washington, DC.
- Metric Conversion Act of 1975*, Public Law 94-168, as amended by Public Law 100-418, *Omnibus Trade and Competitiveness Act of 1988*.
- Miller, J. D. (2002). "Defensive filtration," *ASHRAE Journal*, 44(12), 18-23.
- NCEL (Naval Civil Engineering Laboratory). (1986). *Terrorist vehicle bomb survivability manual (vehicle barriers)*, Port Hueneme, CA.
- NCPC (National Capital Planning Commission). (2001). "Designing for security in the nation's capital," Washington, DC.
- NCPC. (2002). "The national capital planning urban design and security plan," Washington, DC.
- Newman, O. (1996). "Creating defensible space," U.S. Department of Housing and Urban Development, Washington, DC.
- NFPA (National Fire Protection Association). (2000a). "Recommended practice for smoke-control systems, 2000 edition," NFPA 92A, Quincy, MA.
- NFPA. (2000b). "Guide for smoke management systems in malls, atria, and large areas, 2000 edition," NFPA 92B, Quincy, MA.
- NIBS (National Institute of Building Sciences). (2013). *Whole building design guide: Provide security for building occupants and assets*, Washington, DC.
- NIJ (National Institute of Justice). (1985). "Blast resistant protective materials," NIJ Standard 0108.01, Washington DC. [Subscription required]
- NIJ. (2000). "Guide for the selection of chemical agent and toxic industrial material detection equipment for emergency first responders," NIJ Guide 100-00, Washington, DC.
- NIJ. (2001a). "An introduction to biological agent detection equipment for emergency first responders," NIJ Guide 101-00, Washington, DC.
- NIJ. (2001b). "Guide to the technologies of concealed weapon and contraband imaging and detection," NIJ Guide 602-00, Washington, DC.
- NIJ. (2002). "Guide for the selection of personal protective equipment for emergency first responders," Volumes I-IV, NIJ Guide 102-00, Washington, DC.
- NIOSH (National Institute for Occupational Safety and Health). (2003). "Guidance for filtration and air cleaning systems to protect building environments from airborne chemical, biological, or radiological attacks," Publication No. 2003-136, Cincinnati, OH.
- NRC (National Research Council). (1988). *Protection of federal office buildings against terrorism*, Committee on the Protection of Federal Facilities Against Terrorism, Building Research Board, National Academy Press, Washington, DC.
- NRC. (1995). *Protecting buildings from bomb blast, transfer of blast-effects mitigation technologies from military to civilian applications*, National Academy Press, Washington, DC.
- NRC. (2001). *Protecting buildings and people from terrorism: Technology transfer for blast-effects mitigation*, 2001, National Academy Press, Washington, DC.
- NRC. (2003). "Blast effects on buildings and people: A primer for users of the ISC security design criteria," Washington, DC.
- Omnibus Diplomatic Security and Antiterrorism Act of 1986*, Public Law 99-399.
- Smith, M. (1996). "Crime prevention through environmental design in parking facilities," National Institute of Justice (NIJ), Washington, DC.
- Taylor, R. B., and Harrell, A. V. (1996). "Physical environment and crime," National Institute of Justice (NIJ), Washington, DC.
- TSWG (Technical Support Working Group). (2012). "Terrorist bomb threat stand-off card with explanation of use," Washington, DC.
- USACE (U.S. Army Corps of Engineers). (1986). "Heating, ventilation, and air conditioning of hardened installations," TM 5-855-4, Washington, DC.
- USACE. (1991). "Protective design—Mandatory center of expertise," PDC-TR-91-6, *Blast analysis manual, Part 1-Level of protection assessment guide*, Washington, DC. [For Official Use Only]
- USACE. (1999). "Design of collective protection shelters to resist chemical, biological, and radiological (CBR) agents," ETL 1110-3-498, Washington, DC.
- USACE. (1999a). "Airblast protection retrofit for unreinforced concrete masonry walls," ETL 1110-3-494, Washington, DC. [Restricted Access]
- USACE. (1999b). "Design of collective protection shelters to resist chemical, biological, and radiological (CBR) agents," ETL 1110-3-498, Washington, DC.
- USACE. (1999c). "Estimating damage to structures from terrorist bombs field operations guide," ETL 1110-3-495, Washington, DC. [Restricted Access]
- USACE. (1999d). "Window retrofit using fragment retention film with catcher bar system," ETL 1110-3-501, Washington, DC. [Restricted Access]

- USACE. (2001). *Protecting buildings and their occupants from airborne hazards*, Washington, DC.
- USAF (U.S. Air Force). (1986). *Antiterrorism planning and design guidance*, ETL 86-10, Washington, DC.
- USAF. (1990). "Expedient hardening methods for structures subjected to the effect of nonnuclear munitions," Wright Laboratory Report, Wright-Patterson Air Force Base, OH.
- USAF. (1994). *The Air Force resource protection program*, AFI 31-209, Washington, DC.
- USAF. (1995). *The Air Force antiterrorism (AT) program*, AFI 31-210, Washington, DC.
- USAF. (1996). *The Air Force physical security program*, AFI 31-101, Vol. 1, Washington, DC.
- USAF. (1997). *The Air Force resource protection program*, AFH 31-223, Washington, DC.
- USAF. (1999). "Vehicle bomb mitigation guide, force protection battle lab," Washington, DC. [For Official Use Only]
- USAF. (2002). "Installation entry control facilities design guide," Air Force Center for Environmental Excellence, San Antonio, TX.
- U.S. Army. (1979). *Physical security*, FM 19-30, Washington, DC.
- U.S. Army. (1986). "Fundamentals of protective design for conventional weapons," TM 5-855-1, Washington, DC.
- U.S. Army. (1987). *Terrorism counteraction*, 100-37, Washington, DC.
- U.S. Army. (1992). *Engineer operations short of war*, FM 5-114, Washington, DC.
- U.S. Army. (2001). "Protecting buildings and their occupants from airborne hazards," Technical Instruction 853-01 (Draft), Washington, DC.
- U.S. DAO (Department of Commerce Administrative Orders). (1986). "Occasional use of public areas in public buildings," DAO 206-5, Washington, DC.
- U.S. DAO. (1991). "Security programs," DAO 207-1, amended September 6, Washington, DC.
- U.S. DAO. (2000). "Practices for securing critical information assets," Washington, DC.
- U.S. DHS (Department of Homeland Security). (2002a). "National strategy for homeland security," Washington, DC.
- U.S. DHS. (2002b). "State and local actions for homeland security," Washington, DC.
- U.S. DHS. (2003a). "National strategy to secure cyberspace," Washington, DC.
- U.S. DHS. (2003b). "President's homeland security advisory council—Statewide template initiative," Washington, DC.
- U.S. DHS. (2003c). "The national strategy for the physical protection of critical infrastructures and key assets," Washington, DC.
- U.S. DOD (Department of Defense). (1991). *Physical security program regulation*, DoD 5200.8R, Washington, DC.
- U.S. DOD. (1992). "Fragment retention film for glass," UFGS-O8850, Washington, DC.
- U.S. DOD. (1994). *DoD combating terrorism program procedures*, DoD Instruction 2000.14, Washington, DC.
- U.S. DOD. (1995). "Plastic glazing," UFGS-O8840A, Washington, DC.
- U.S. DOD. (1996). *DoD combating terrorism program*, DoD directive 2000.12, Washington, DC.
- U.S. DOD. (1997a). *DoD combating terrorism program standards*, DoD Instruction 2000.16, Washington, DC.
- U.S. DOD. (1997b). *Planning, design, engineering, and construction of facilities* [draft], DoD Instruction 4270.1 (replaces MIL-HDBK 1190, *Facility planning and design guide*), Washington, DC.
- U.S. DOD. (1997c). "Self-acting blast valves," UFGS-13420A, Washington, DC.
- U.S. DOD. (1999). "Interim antiterrorism/force protection construction standards," Washington, DC.
- U.S. DOD. (2000a). "Bullet-resistant components," UFGS-II035, Washington, DC.
- U.S. DOD. (2000b). "Interim antiterrorism/force protection construction standards—progressive collapse guidance," Washington, DC.
- U.S. DOD. (2001a). "Blast resistant doors," UFGS-08390A, Washington, DC.
- U.S. DOD. (2001b). "Blast resistant tempered glass windows," UFGS-08581, Washington, DC.
- U.S. DOD. (2001c). "Electromagnetic (EM) shielding," UFGS-13095A, Washington, DC.
- U.S. DOD. (2001d). "Forced entry resistant components," UFGS-II025, Washington, DC.
- U.S. DOD. (2001e). "Traffic barriers," UFGS-O2841N, Washington, DC.
- U.S. DOD. (2002a). "Active vehicle barriers," UFGS-O2840A, Washington, DC.
- U.S. DOD. (2002b). "Design and analysis of hardened structures to conventional weapons effects," UFC 3-340-01, Washington, DC. [For Official Use Only] [Formerly Army TM 5-855-1]
- U.S. DOD. (2002c). "DoD minimum antiterrorist standards for buildings," UFC 4-010-01, Washington, DC.
- U.S. DOD. (2002d). "Fencing," UFGS-O2821A, Washington, DC.
- U.S. DOD. (2002e). "Security vault door," UFGS-II020, Washington, DC.
- U.S. DOE. (1992). *Manual for the prediction of blast and fragment loadings on structures*, DOE/TIC 11268, Southwest Research Institute, Albuquerque, NM.
- U.S. DOS (Department of State). (1985). "Specification of vehicle crash test of perimeter barriers and gates," SD-STD-02.01, Washington, DC.
- U.S. DOS. (1987a). "Specification and test criteria for class M modular vault systems," SD-STD-01.05, Revision B, Washington, DC.
- U.S. DOS. (1987b). "Technical security systems standards," DS/ST/SEL, Washington, DC.
- U.S. DOS. (1988). *Physical security standards handbook (limited official use only)*, Bureau of Diplomatic Security, Washington, DC.
- U.S. DOS. (1989). *Perimeter barrier selection guide*, Diplomatic Security Services—Physical Security Division, Washington, DC.
- U.S. DOS. (1991). "Crash barrier analysis program," Diplomatic Security Service, Physical Security Division, Washington, DC.
- U.S. DOS. (1993a). "Certification standard—Forced entry and ballistic resistance of structural systems," SD-STD-01.01, Revision G (Amended), Washington, DC.
- U.S. DOS. (1993b). "Forced entry and ballistic," *Certification standard SD-STD-01.01*, Revision G (amended), Bureau of Diplomatic Security, Washington, DC.

- U.S. DOS. (1993c). "Resistance of structural systems," Amended April 30, Bureau of Diplomatic Security, Washington, DC.
- U.S. DOS. (1995). "Structural engineering guidelines for new embassy office buildings," limited official use only, Bureau of Diplomatic Security, Washington, DC.
- U.S. DOS. (1996). *Physical security programs: Improvised barrier guide*. Bureau of Diplomatic Security, Washington, DC.
- U.S. DOS. (1998). *Architectural engineering design guidelines*, 5 volumes, Bureau of Diplomatic Security, Washington, DC. [For Official Use Only]
- U.S. DOS. (2002a). "Diplomatic telecommunications service installation standards, DTS-IS," *Communications security handbook*, 5 FAH-6. Washington, DC.
- U.S. DOS. (2002b). "Patterns of global terrorism, 2002," Bureau of Diplomatic Security, Washington, DC.
- U.S. Department of the Treasury, BATFE (Bureau of Alcohol, Tobacco, Firearms and Explosives). (1999). "Vehicle bomb explosion hazard and evacuation distance tables," Washington, DC.
- U.S. HUD (Department of Housing and Urban Development). (1975). "The avoidance of progressive collapse, regulatory approaches to the problem," *PB-248 781*, Division of Energy, Building Technology, and Standards, Office of Policy Development and Research, Washington, DC.
- U.S. GSA (General Services Administration). (1983). *Preferred metric units for general use by the federal government*, FED-STD-376A, Washington, DC.
- U.S. GSA. (1999). "Balancing security and openness: A thematic summary of a symposium on security and the design of public buildings," Washington, DC.
- U.S. GSA. (2000). "Progressive collapse analysis and design guidelines for new federal office buildings and major modernization projects," Washington, DC. [Restricted Access]
- U.S. GSA. (2001). *Security reference manual, part 3: Blast design and assessment guidelines*, Washington, DC. [For Official Use Only] [Restricted Access]
- U.S. GSA. (2002). *Mail center managers security guide*, 2nd edition, Washington, DC.
- U.S. Marshals Service. (1995). *Vulnerability assessment of federal facilities*, Washington, DC. [Restricted Access]
- U.S. Navy. (1986a). "Blast resistant structures," NAVFAC DM 2.08, Alexandria, VA.
- U.S. Navy. (1986b). "Commercial intrusion detection systems (IDS)," NAVFAC DM 13.02, Alexandria, VA.
- U.S. Navy. (2003). "Entry control facilities," Interim Technical Guidance (ITG) 03-03, Alexandria, VA.
- U.S. VA (Department of Veterans Affairs). (2002). *Physical security assessment for Veteran Affairs facilities, recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs*, Washington, DC.
- Wright Laboratory. (1990). *Expedient hardening methods for structures subjected to the effect of nonnuclear munitions*, report, Wright-Patterson Air Force Base, OH.

This page intentionally left blank

INDEX

- artificial intelligence, 45
- bonus points, procedure for, 25–26
- bronze rating
 - commentary, 57*t*–76*t* (*see also* countermeasure commentary level 2, bronze)
 - countermeasure checklist, 34*t*–35*t*
 - description, 21, 22*t*, 23
- building classification
 - general approach to, 4–5
 - general methodology of, 3–4, 4*f*
 - impact questions on, 28*t*, 30*t*, 31*t*
 - mathematical evaluation of, 10–11, 10*t*, 11*t*
 - overview of, 3
 - primary hazard classification factors of, 5, 6*t*
 - primary impact/consequence classification factors of, 8–9, 8*t*, 9*t*
 - secondary hazard classification factors of, 5, 7–8, 7*t*, 8*t*
 - secondary impact/consequence classification factors of, 9–10, 9*t*, 10*t*
 - threat questions on, 27*t*–30*t*
- building functions/usage, hazard classification and, 5, 6*t*
- building security ratings
 - bonus points in, 25–26
 - description of, 21–23, 22*f*
 - philosophy of, 23
 - process for, 23–25, 23*t*–25*t*
- building security rating system (BSRS)
 - basis of, 1–2
 - building classification and, 3–11, 4*f*, 6*t*–11*t*
 - countermeasures used in, 2
 - innovations in, 45
 - purpose of, 1
 - references used to develop, 2
- building size factor, 9, 9*t*
- chemical, biological, and radiological (CBR) agents, 2
- child care factor, 9, 9*t*
- city population factor, 7, 7*t*
- Class A facilities, 3
- Class B facilities, 3
- Class C facilities, 3
- Class D facilities, 3
- countermeasure checklist
 - bronze rating, 34*t*–35*t*
 - gold rating, 38*t*–41*t*
 - platinum rating, 41*t*–43*t*
 - rated, 33*t*–34*t*
 - silver rating, 36*t*–38*t*
- countermeasure commentary level 1, rated
 - architectural, 50*t*–52*t*
 - envelope, 53*t*
 - equipment operations and maintenance, 55*t*
 - mechanical, 54*t*–55*t*
 - security master plan, 56*t*
 - security systems, 55*t*–56*t*
 - site, 47*t*–50*t*
 - structural, 52*t*
 - utilities, 53*t*–54*t*
- countermeasure commentary level 2, bronze
 - architectural, 60*t*–66*t*
 - communications and IT, 71*t*
 - envelope, 67*t*–68*t*
 - equipment operations and maintenance, 71*t*–72*t*
 - mechanical, 69*t*–71*f*
 - security master plan, 76*t*
 - security systems, 72*t*–75*t*
 - site, 57*t*–60*t*
 - structural, 66*t*–67*t*
 - utilities, 68*t*
- countermeasure commentary level 3, silver
 - architectural, 78*t*–81*t*
 - communications and IT, 92*t*
 - electrical, 89*t*–90*t*
 - envelope, 84*t*–85*t*
 - equipment operations and maintenance, 92*t*
 - fire, 90*f*–92*f*
 - mechanical, 87*t*–88*t*

- plumbing and gas, 88*t*
- security master plan, 100*f*–102*f*
- security systems, 93*t*–100*t*
- site, 77*t*–78*t*
- structural, 81*t*–84*t*
- utilities, 85*t*–86*t*
- countermeasure commentary level 4, gold
 - architectural, 105*t*–112*t*
 - communications and IT, 130*t*–131*t*
 - envelope, 117*t*–120*t*
 - equipment operations and maintenance, 131*t*
 - fire, 127*t*–129*t*
 - mechanical, 124*t*–126*t*
 - plumbing and gas, 126*t*–127*t*
 - security master plan, 137*t*–138*t*
 - security systems, 132*t*–136*t*
 - site, 103*t*–106*t*
 - structural, 112*t*–117*t*
 - utilities, 120*t*–123*t*
- countermeasure commentary level 5, platinum
 - architectural, 140*t*
 - communications and IT, 154*t*
 - envelope, 145*t*–146*t*
 - equipment operations and maintenance, 154*t*
 - fire, 153*t*
 - mechanical, 148*t*–152*t*
 - plumbing and gas, 153*t*
 - security master plan, 157*t*
 - security systems, 155*t*–156*t*
 - site, 139*t*–140*t*
 - structural, 141*t*–145*t*
 - utilities, 147*t*–148*t*
- countermeasure levels
 - function of, 13
 - layout of, 13–14, 15*t*–19*t*
 - required, 18, 19*t*
 - security ratings and, 24–25, 33*t*–43*t*
- countermeasures
 - evaluation of, 13, 14*f*
 - innovations in, 45
 - interrelationship among, 19
 - non-applicable, 18–19
- crime prevention through environmental design (CPTED)
 - principles, 2, 21
- critical infrastructure association factor, 5, 6*t*
- digital IP (Internet Protocol) video, 45
- distance to hazardous materials/transportation routes factor, 7, 7*t*
- distance to high-profile buildings factor, 7, 7*t*
- factor weight equation, 5*e*
- Federal Emergency Management Agency (FEMA), *Manual to Mitigate Potential Terrorist Attacks against Buildings*, 1–2
- gang activities factor, 7, 8*t*
- gold rating
 - commentary, 130*t*–138*t* (*see also* countermeasure commentary level 4, gold)
 - countermeasure checklist, 38*t*–41*t*
 - description, 22, 22*t*, 23
- hazard classification factors
 - primary, 5, 6*t*
 - secondary, 5, 7–8, 7*t*, 8*t*
- historic status factor, 9–10, 10*t*
- impact/consequence classification factors
 - primary, 8–9, 8*t*, 9*t*
 - secondary, 9–10, 9*t*, 10*t*
- impact questions, 28*t*, 30*t*, 31*t*
- infrastructure or transportation utility factor, 8–9, 9*t*
- LEED system, building security rating system and, 1
- local economic significance factor, 8, 8*t*
- Manual to Mitigate Potential Terrorist Attacks against Buildings* (FEMA 426), 1–2
- national political significance factor, 8, 8*t*
- national symbolism or prominence factor, 8, 8*t*
- occupancy factor, 9, 9*t*
- overall impact factor, 10, 10*t*
- physical design countermeasures, innovation in physical, 45
- platinum rating, 22–23, 22*t*, 41*t*–43*t*
 - commentary, 139*t*–157*t* (*See also* countermeasure commentary level 5, platinum)
 - countermeasure checklist, 41*t*–43*t*
 - description, 22–23, 22*t*
- primary hazard classification factors, 5, 6*t*
- primary impact/consequence classification factors, 8–9, 8*t*–9*t*
- proximity to law enforcement factor, 8, 8*t*
- public visitors factor
 - as secondary hazards classification factor, 7, 7*t*
 - as secondary impact/consequence classification factor, 9, 9*t*
- rated countermeasure
 - commentary, 47*t*–56*t* (*see also* countermeasure commentary level 1, rated)
 - countermeasure checklist, 33*t*–34*t*
 - description, 21, 22*t*, 23
- scaling factors, values of, 10*t*, 11
- secondary hazard classification factors, 5, 7–8, 7*t*, 8*t*
- secondary impact/consequence classification factors, 9–10, 9*t*–10*t*
- security ratings, countermeasure levels and, 24–25, 33*t*–43*t*
- silver rating
 - commentary, 77*t*–102*t* (*see also* countermeasure commentary level 3, silver)
 - countermeasure checklist, 36*t*–38*t*
 - description, 21–23, 22*t*
- threat history factor, 5, 6*t*
- threat questions, 27*t*–30*t*
- threat weights, hazard classification and, 5, 6*t*
- total weight of factors equation, 10*e*
- VIP factor, 5, 7*t*